حملة - المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

دليل الأمان الرقمي

للمدافعين/ات ومؤسسات حقوق الإنسان

أمان رقمي
حملة - المركز العربي
لتطوير الإعلام الاجتماعي

حملـــة - المـركز العـربيّ لتطويـــر الإعـــلام الاجتمـاعيّ

دليل الأمان الرقمي
للمدافعين/ات ومؤسسات حقوق الإنسان

شباط/فبراير 2024

إعداد وتحرير: مجموعة الحماية الشاملة
تصميم الدليل: مجد شربجي
تصميم الرسوم والأيقونات: ستوديو سفر
ترجمة للعربية: رتاج للحلول الإدارية

لمزيد من الموارد زوروا منصتنا لتعلم الأمان الرقمي

نتطلّع لتواصلكن ّ وتواصلكم معنا عبر القنوات التالية:
البريد الإلكتروني: info@7amleh.org
الموقع الإلكتروني: www.7amleh.org
الهاتف: 20670 7740 (0) 972+

تابعونا عبر صفحاتنا على منصات الإعلام الاجتماعي 7amleh

فهرس

مقدمة 5

1| التهديدات الرقمية: المؤشرات والوقاية والاستجابة 6
1.1| المراقبة الرقمية 9
1.2| هجمات التصيد والهندسة الاجتماعية 13
1.3| التحرش والملاحقة عبر الانترنت 16
1.4| تصيد (ترولينغ) 20
1.5| انتهاكات الخصوصية 22

2| أدلة الأمان الرقمي 24
2.1| أمان كلمات المرور والحسابات 25
2.1.1| إنشاء كلمات مرور قوية والحفاظ عليها 25
2.1.2| استخدام مدير كلمات المرور 27
2.1.3| متى يجب تغيير كلمة المرور 30
2.1.4| أين نحن ومن يستطيع أن يرانا 30
2.1.5| تفعيل مصادقة الدخول بمعاملين 30
2.1.6| تجنبوا البصمات وخاصية التعرف على ملامح الوجه (البيومترية) 32
2.1.7| وضع أسئلة استرجاع آمنة 32
2.2| أمان الأجهزة 33
2.2.1| الحواسيب (المكتبية والمحمولة) 33
2.2.2| الهواتف المحمولة 48
2.2.3| الأمان على الإنترنت 57
2.3.1| أمن الشبكات 57
2.3.2| استخدام الشبكات الافتراضية الخاصة VPNs 58
2.3.3| التحايل على الرقابة: طرائق وسبل 58
2.4| أمن الاتصالات 60
2.4.1| التصفح الآمن 62
2.4.2| تطبيقات المراسلة الآمنة 66
2.4.3| مؤتمرات ولقاءات الفيديو الآمنة 67
2.5| حماية البيانات 70
2.5.1| حماية البيانات 70
2.5.2| النسخ الاحتياطية واستعادة البيانات 76
2.5.3| إتلاف البيانات 84

فهرس

3| ادارة مخاطر الأمان الرقمي 90
3.1| تقييم مخاطر التهديدات الرقمية 91
3.1.1| تقييمات مخاطر الأمن السيبراني لمنظمات المجتمع المدني والمؤسسات الإعلامية 101
3.1.2| تقييم مخاطر الأمان السيبراني في الفضاء الرقمي للأفراد (المدافعين/ات عن حقوق الإنسان والصحفيين/ات) 102
3.2| سياسات وإجراءات الأمان الرقمي 108
3.3| الاستجابة للحوادث والطوارئ 110
3.4| متابعة الحوادث: التعافي والرعاية اللاحقة واستقاء الدروس 111
3.5| توثيق الانتهاكات الرقمية 112

4| الحصانة النفسية في مواجهة الاعتداءات الرقمية 116

5| مسرد مصطلحات 118

مقدمة

بادر مركز "حملة"، الذي يقوم منذ سنوات عديدة، ضمن عمله على حماية الحقوق الرقمية الفلسطينيّة بتدريب جمعيّات أهليّة ومنظّمات حقوق إنسان وناشطين/ات في مجال الأمان الرقميّ، إلى إنشاء دليل"الأمان الرقمي للمدافعين/ات ومؤسسات حقوق الإنسان" بهدف ضمان إتاحة هذه المضامين التدريبيّة لكلّ المؤسّسات والناشطين/ات باللغة العربيّة، بأسلوب منهجيّ ، تقني ودائم التحديث، ما يمكّنهم من تقييم وحماية أنفسهم في الفضاء الرقميّ دائم التطوّر والتغييرات ومن صياغة وتنفيذ السياسات والإجراءات لحماية أجهزة المؤسسة ومواردها.

يتضمّن دليل "الأمان الرقمي للمدافعين/ات ومؤسسات حقوق الإنسان" مجموعة من الأدلة التدريبيّة المتقدّمة تشرح خطوة بخطوة عن الإجراءات المطلوبة لضمان حماية الخصوصية واستدامة الأمان الرقميّ للمؤسّسات أو للناشطين، وهي موزّعة على خمسة أبواب:

- **تقييم المخاطر:** تُمكِّن أدلة هذا الباب من إدارة المخاطر في الأمان الرقميّ، بدءًا إجراء تقييم ذاتيّ حول المخاطر، والحصول على توجيهات واضحة لوضع إجراءات وسياسات الأمان الرقميّ، والجهوزيّة لحالات الطوارئ، وتوثيق الانتهاكات.

- **الوقاية الرقمية:** تُمكِّن أدلة هذا الباب من التعرّف بالتفصيل على التهديدات الرقميّة ومؤشّراتها والوقاية منها. تشرح عن المراقبة الرقميّة، والتصيّد، وهجمات الهندسة الاجتماعيّة، والتحرّش، وكلّ أشكال انتهاكات الخصوصيّة، وتوضح خطوة بخطوة سبل الوقاية منها.

- **الحماية الرقمية:** يتضمّن هذا الباب أدلة أمان رقميّ مفصّلة لحماية الأجهزة والشبكة والاتصالات والبيانات والحسابات والكلمات السريّة من المخاطر والتهديدات.

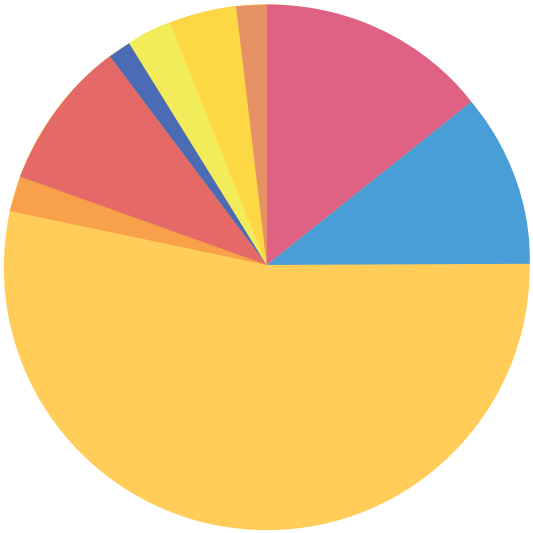
- **الحصانة النفسية:** يتضمّن هذا الباب دليلًا لتعزيز الحصانة النفسيّة من الهجمات الرقميّة.

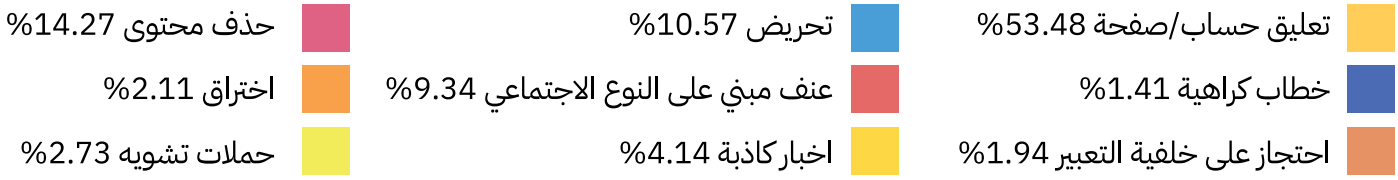
- **مسرد مصطلحات:** قاموس يتضمّن المصطلحات المختلفة المستخدمة في مجال الأمان الرقميّ لتسهيل فهم الأدلة والمعلومات واستخدامها الصحيح.

1| التّهديدات الرّقميّة: المؤشرات والوقاية والاستجابة

مُقدِّمة

في ضوء الانتهاكات الرّقميّة الموثّقة في فلسطين عبر منصّة حُر، يُمكن إجمال أبرز ما يُحدّد البُعد الرّقمي لحياتنا بما يلي:





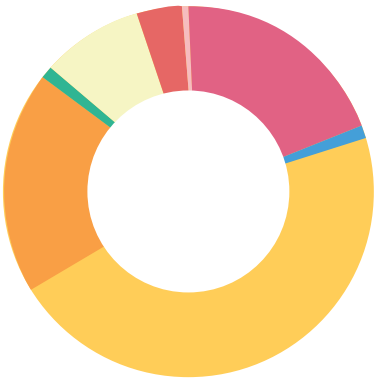
(2022-2023)

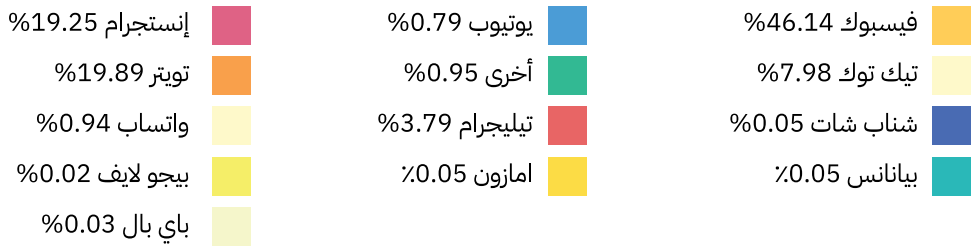
إجمالي الانتهاكات

نوع الانتهاكات؛ نوع الرّقابة؛ صِلة أو انتماء الجهة؛ المنصّة

- تعليق حساب/صفحة: 53.48%
- حذف مُحتوى: 14.27%
- تحريض: 10.57%
- عنف مبني على النّوع الاجتماعي: 9.34%
- أخبار كاذبة: 4.14%
- حملات التّشويه: 2.73%
- اختراق: 2.12%
- احتجاز على خلفيّة التّعبير: 1.94%
- خطاب كراهيّة: 1.41%

تُظهر هذه الأرقام أنّ أكثر من 67% من التّهديدات الموثّقة تدور في فلك غاية واحدة وهو إسكات الجهات المُهدَّدَة، حتّى أنّ الشّكاوى وغيرها من ضروب التّظلّم المشروعة الّتي تُتيحها شركات التّواصل الاجتماعي (مثل ميتا أو تويتر) لحماية حقوق المستخدمين والمستخدمات بات يُساء استخدامه من الخصوم لتعليق الحسابات والصّفحات وحذف المحتوى.
بالمِثل، تُظهر المنصّات المتأثرة بهذه التّهديدات—بمعنى الّتي أضحى فضاؤها مرتعًا لهذه التّهديدات—توجّهات واستنطاقاتٍ أخرى.





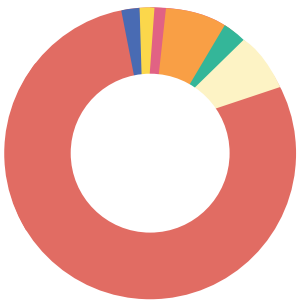
(2022-2023)

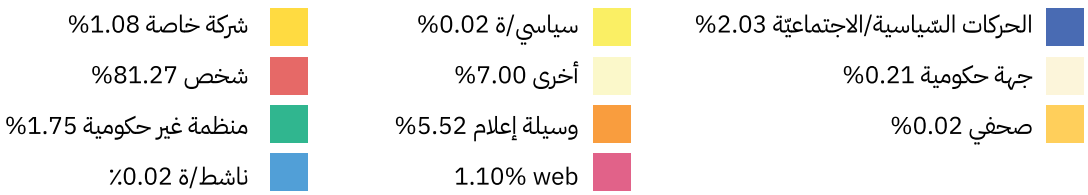
المنصّة

إجمالي الانتهاكات؛ نوع الانتهاكات؛ نوع الرّقابة؛ صِلة أو انتماء الجهة

- فيسبوك: 46.14%
- تويتر: 19.89%
- إنستغرام: 19.25%
- تيك-توك: 7.98%

وبعد ذلك تطبيقات المراسلة!
يُقدّم التّقرير طيفًا من الإضاءات المهمّة، لا سيّما بشأن الفئات المُستهدفة بالتّهديدات. تجدر الإشارة إلى أنّ تصنيف الأفراد (نشطاء، مؤلفين إلخ) يندرج تحت تصنيف (شخص person).





(2022-2023)

الجهات المتأثرة حسب الفئة

1. الشركات الخاصّة 1.45% 1.08%
2. الحركات السّياسية/الاجتماعيّة 2.03%
3. غير ذلك
4. المنظمات الأهليّة 1.75%
5. الصّحفيون والصّحفيات 0.02%
6. المدافعون والمدافعات عن حقوق الإنسان 0.03%
7. النّشطاء 0.02%
8. 0.83%
9. السّاسة 0.02%
10. الأفراد 81.27%
11. جهات رسميّة 0.21%
12. وسائل إعلاميّة 5.52%
13. مؤثّرون ومؤثّرات 0.07%
14. كتّاب وكاتبات
15. كوادر أكاديميّة 0.03%

إدراك أنّ ما نسبته 78.28% من المُستهدفين هم أفراد يُفصح عن حقيقة بالغة الأهمية، وهي الحاجة الماسّة إلى تكوين مجموعات للرعاية الرّقميّة للحؤول دون ترك هذه الفئة عرضة للانتهاكات دون أيّ دعم؛ فمن المهم ألّا يقتصر الاهتمام بالآثار الرّقميّة للانتهاك، ولكن أيضًا بظلاله النّفسية والشّعورية المتعاظمة. في كثير من منظمات المجتمع المدني والحركات الاجتماعية تُعطى الانتصارات والنضالات البارزة وجهًا جماعيًا، أمّا آثارها السّلبيّة فتُترك على أكتاف الأفراد؛ لمواجهة هذا التّرسّبات العاطفيّة للتعدّيات الرّقميّة، عليك بعدَّة الإسعاف الأوّلي الرّقمي (يُمكنك النّفاذ إليها عبر الرّابط.
ولا تفوّت/ي الموارد الإضافيّة الواردة في الرّابط.

يبقى نفير أجهزة المُراقبة الرّقمية الّتي تزرعها سلطات الاحتلال الإسرائيلي في الأرض الفلسطينيّة أحد أبرز وأشمل التّهديدات لخصوصيّة الفلسطينيين، شعبًا وفرادى. ويمتد نطاق هذه المراقبة من كاميرات المراقبة ويتراوح ذلك من الكاميرات المزروعة في الأماكن العامّة والمرتبطة بقواعد قواعد البيانات البوليسيّة الإسرائيليّة، عدا نُظم المراقبة الّتي تعمل بالذّكاء الاصطناعي، وصولًا إلى الجهات المزوّدة لخدمات الإنترنت والهاتف العاملة في الأرض الفلسطينيّة وانتهاكاتها لخصوصيّة الفلسطينيين. وتشمل هذه الخانة نشر الخصوم لبرمجيات وأجهزة التّجسّس. يُذكر في هذا السّياق، ما كُشف عن برنامج التجسس بيغاسوس عام 2021، وما تمخض عن ذلك من زيادة الوعي العام وعرّى حِبال المصالح الواصلة بين الشّركات الخاصّة والدّول القوميّة في الوقوف خلف انتهاكات التّجسس، لمزيد من المعلومات بشأن الانتهاكات المرتبطة ببرنامج بيغاسوس، يُمكن الاطلاع على الرّابط.
إن كان تعرضت أو لديك أي معلومات بشأن انتهاك رقمي في فلسطين، يُمكنك التّبليغ عنه عبر منصّة المرصد الفلسطيني لانتهاكات الحقوق الرّقميّة (حُر).

آلية عملنا

1.1| المراقبة الرّقميّة

أنظمة المراقبة بالفيديو وغيرها من ضروب الرّصد والتّتبع البيومتريّة

زرعت سلطات الاحتلال الإسرائيلي العديد من كاميرات المراقبة بالفيديو في العديد من الأماكن العامّة في الأرض الفلسطينيّة المحتلّة ولا تنفك تستخدمها لخرق خصوصيّة الفلسطينيين. على الرّغم أنّ هناك طيفًا من الأساليب للتحايل على هذه التعديات، مثل إنشاء خرائط تحدّد مواقع هذه الكاميرات، وبالتّالي التّنقل عبر طرقٍ خالية من الكاميرات، في الواقع لا يوجد أي أدوات أو استجابات رقميّة لتجنب الوقوع ضمن نطاق أعين هذه الأجهزة.

من جهة أخرى، لا بدّ من اتخاذ مواقف حازمة حيال البيانات البيومتريّة الّتي نُلقّمها لأجهزتنا والخدمات الرّقميّة المرتبطة بهذه البيانات، فالأمان النّسبي والسّهولة المغرية لاستخدام بصمتي وجوهنا أو أصابع اليد للولوج لأجهزتنا، لفك قفل الشّاشة، مثلًا، لا بدّ ألّا تُنسينا أن هذه البيانات تُخزّن، أقلّه على أجهزتنا، وربما على قاعدة بيانات سحابيّة—يتوقّف ذلك على الجهة المزوّدة لخدمة الاتصالات؛ وبتالي يُمكن أن تُشهر في وجهنا كأدلة علينا وقد يُساء استخدامها لمآرب إجراميّة أو أمور أخرى؛ لذا فإنّنا نشدّد على تجنّب استخدام البيانات البيومتريّة واستبدلاها بكلمات مرور عصيّة وطويلة. (للمزيد بهذا الشّأن، عليك بالقسم 2.1 أمان كلمات المرور والحسابات.)

برمجيّات التّجسّس

منذ الكشف عن توظيفات برنامج التّجسس بيغاسوس التابع لمجموعة "إن إس أو" NSO، والنّشطاء، والإعلاميات والإعلاميون، ومنظّمات المجتمع المدني على وعي بالمخاطر المحيقة بأمانهم بواسطة مدسوسات برمجيات التّجسّس، ورغم التّباين الكبير بين أجهزة التّجسس الّتي تستخدمها الشّركات والحكومات، بالذّات من حيث الخصائص والقدرات، يُمكن الافتراض بأنّ الوصول للبرامج التّالية خاصيّة ممكنة في السّواد الأعظم من برمجيات التّجسّس:

- الرّسائل القصيرة الرسائل النّصية
- رسائل البريد الإلكتروني
- محادثات تطبيق الواتساب
- الصور والفيديوهات
- بيانات نظام التّموضع العالمي
- التّقويم
- تفعيل جهات الاتصال
- تفعيل الميكروفون
- تفعيل الكاميرا
- تسجيل المكالمات الواردة والصادرة!

تعمل برامج التّعقّب—تُسمّى أيضًا ببرامج الأزواج الشّكاكين—على غرار برامج التّجسس، وتضم خصائص مماثلة تُمكّن المتعَقِّب من مراقبة هاتف المُتعَقَّب، وعادةً تُتاح مجانًا لعملاء القطاع الخاص، لكن لا بدّ من اتصالٍ مباشر بالجهاز المُستهدف لتثبيت البرنامج عليه.

مؤشّرات وجود برنامج تجسس على جهازك

- ثمَّ طيف من الأمارات الّتي تُشير إلى أنّ جهازك يخضع لمراقبة رقمية، منها:
- تفاعل الجهاز بطريقة مريبة.
- إعادة توجيهك لمواقع غير محميّة لتثبيت تطبيقات أو تحديثات
- تلقّي رسائل وتنبيهات أمنيّة من خدمات موثوقة.
- وصول معلومات تمّت مشاركتها عبر البريد الإلكتروني أو برنامج المراسلة أو ما شابه ذلك إلى خصوم.
- تسريب معلومات سرية تمت مشاركتها عبر مهاتفات أو رسائل نصيّة قصيرة إلى خصوم (لا سيّما في ظل ظروف حسّاسة).
- العثور على جهاز مريب متصل بالحاسوب أو الشّبكة.
- العثور على جهاز تعقّب على مقربة من شخص.
- ثبوت تعرّض أشخاص مقرّبين منك للمراقبة الرّقمية.

أمّا العوارض الأكيدة للاختراق، فعادة ما تشمل التّالي:

- تكرار إعادة تشغيل الجهاز خلال استخدام أحد تطبيقات الجهاز
- تعطّل الجهاز، لا سيّما عند إدخال بيانات
- تكرار فشل تحديثات نظام التّشغيل وإجراءات الأمان التّصويبيّة أو كلاهما
- ظهور الضّوء الخاص بتشغيل كاميرا الويب رغم عدم استخدامها
- تواتر ظهور شاشة الهلاك الزرقاء أو أحداث الذعر في النواة (kernek panic)
- وميض نوافذ التطبيقات
- تحذيرات مضادات الفيروسات

بعض الأعراض تدلُّ أنّ الجهاز يُبدي سلوكًا غريبًا، لكنه ليس بمدعاة كافية للقلق:

- أصوات طقطقة في الهاتف في أثناء المحادثات
- الاستنزاف السّريع للبطاريّة
- ارتفاع حرارة الجهاز الزّائدة رغم عدم استخدامه
- بطء الجهاز

هذه الأعراض عادةً ما توصف بأنّها دلائل على نشاط مريب للجهاز، إلا أنَّ أيًّا منها لا يُعدُّ مدعاة للقلق ما لم تجتمع.

في حال وجود مؤشرات بأنّ الجهاز به برمجيات تجسس، عليك:

- تسجيل الخروج من كافة الحسابات
- تغيير كلمات المرور لجميع الحسابات
- تفعيل خاصّية التّحقق الثّنائي للولوج إلى الحسابات
- التوقّف عن استخدام الجهاز وفصله عن أي شبكة إنترنت
- التّواصل مع جهة دعم احترافيّة لمعرفة ما إذا كان الجهاز به برامج تجسس فعلًا.

التّحقّق من وجود برنامج تجسس في جهازك: عِدّة من الخطوات والنصائح

لمعرفة ما إذا كان في الجهاز برامج تجسّس، عليك بقسم "جهازي يتصرّف على نحو مريب" ضمن دليل عدَّة الإسعاف الأوّلي الرّقمي.

إذا خَلُص تنخيل المؤشّرات إلى توافر قرائن حقيقيّة على وجود برامج تجسّس في الجهاز، لا بدّ من الاستعانة بدعمٍ متخصّص لمعالجة المسألة: (خانة: الفحص الجنائي). كذلك، يُقدّم كُل من مشروع سِفِل-سْفِير، ومختبر الأمان الرّقمي لمنظمة مراسلون بلا حدود في ألمانيا. خدمات دعم عن بُعد وفحوص عبر الإنترنت للتحقّق من خلو الجهاز أو احتوائه على برمجيّات تجسّس.

تجدر الإشارة أن عدم اكتشاف الفحوص الجنائيّة لأي ما يُثبت وجود برمجيات تجسّس على الجهاز، فإنّ ذلك لا يعني بأنّ الجهاز آمنًا مئة بالمئة، فقد قد يكون مطورو برامج التّجسّس مُعدِّين البرنامج على نحوٍ يجعلها عصيّة على الكشف حتّى بالفحوص الجنائيّة. لذا عليك بالخطوات التّاليّة لحماية جهازك وخصوصيتك.

لحماية جهازك من برامج التّجسّس عليك بالخطوات العامّة التّالية:

- مراجعة وتطبيق إرشادات المحور الثّاني من الفصل الثّاني (2.2 أمان الجهاز).
- إعادة تشغيل الهاتف بوتيرة متكرّرة (مثلاً مرة يوميًا) إلى إزالة بعض إصدارات برامج التجسس (هذه الخطوة أثبتت جدواها للتعامل مع آخر إصدارات من بيغاسوس، تحديدًا على نظام التّشغيل آي-أو-إس (iOS).
- إعادة ضبط الجهاز لإعدادات المصنع من وقتٍ لآخر قد تُسهم بإزالة ما ثُبت على الجهاز، بما في ذلك برامج التّجسّس. لتطبيق هذه الخطوة، عليك مراجعة الخطوات الخاصّة بنظامي التّشغيل أندرويد وآي-أو-إس. ملاحظة: تُسفر إعادة ضبط الجهاز حَسب إعدادات المصنع إلى إزالة كافّة المعلومات المحفوظة على الهاتف، لذا عليك تذكّر الإبقاء على نسخة احتياطيّة صالحة من كافّة تلك المعلومات قبل الإقدام على إعادة الضّبط.

- تحديث أنظمة التّشغيل وكافّة التّطبيقات المستخدمة حال توفّر تحديثات لها (المحور الثّاني من الفصل الثّاني: 2.2 أمان الجهاز).
- الإحجام عن تحميل التّطبيقات من مصادر غير متاجر التّطبيقات الرّسميّة (المحور الثّاني من الفصل الثّاني: 2.2 أمان الجهاز).
- استخدام خاصّية الشّبكات الخاصّة الافتراضيّة (VPN) (القسم الثّاني من المحور الثّالث من الفصل الثّاني: 2.3.2 استخدام شّبكات الخاصّة الافتراضيّة).
- التّحقّق من الرّوابط قبل فتحها (التّصيّد والهندسة الاجتماعيّة للاعتداءات)
- استخدام برامج الحماية من البرمجيات الخبيثة (المحور الثّاني من الفصل الثّاني: 2.2 أمان الجهاز).
- غربلة التّطبيقات غير الضّروريّة وحذفها إن أمكن، وإن لم يكن ممكنًا، فإلغاء تفعيلها (المحور الثّاني من الفصل الثّاني: 2.2 أمان الجهاز).
- استخدام خاصيّة "نمط المنع" (وضع التأمين) الّتي يُتيحها نظام آي-أو-اِس (المحور الثّاني من الفصل الثّاني: 2.2 أمان الجهاز).
- النّظر في استخدام نظام أندرويد بديل (المحور الثّاني من الفصل الثّاني: 2.2 أمان الجهاز).

التّأثير العاطفي

في حمأة كُل هذه الآثار، لا بدّ أن نعي أنّ شبهة اختراق الجهاز الشّخصي أو ثبوت ذلك ينثني على الأرجح على طيفٍ أعمق من الآثار النّفسية.

بهذا الخصوص، عليك بالموارد التالية:

الفصل الرّابع: المَرَانة العاطفيّة في مواجهة الاعتداءات الرّقميّة

قسم العناية بالنّفس من عدَّة الإسعاف الأوّلي الرّقمي.

مزودو خدمات الإنترنت والهاتف والمراقبة المحمولة على ظهر البنى التّحتيّة الرّقمية

- من المعروف—وغالبًا بموجب التزام قانوني—يعمد مزودو خدمات الهاتف والإنترنت إلى جمع معلومات حسّاسة عن مستخدميهم، نحو مكانهم، والخدمات الّتي يستخدمون، وأوقات ومُدد الاستخدام، ومواصفات أجهزتهم المرتبطة بمعلومات تعريف شخصيّة منصوص عليها في وثائق الاشتراك وعقد استخدام خط الهاتف وخدمات الإنترنت.
- في العديد من السّياقات القمعيّة يُضاف لما سبق عنصر البنية التّحتيّة الرّقميّة المشتركة وإساءة استخدام مزودي خدمات الإنترنت والهاتف لمراقبة النّشطاء والكوادر الإعلاميّة. وبما أنه من الصّعب جدًا إثبات حدوث ذلك، والأصعب منعه أو إيقافه، لا يبقى سبيل للوقاية أو المواجهة سوى لتأمين حركتنا على الشّبكة وتجنب استخدام قنوات الاتصال غير الآمنة.
- تتسم مكالمات الهواتف والرّسائل النّصية بسهولة اختراقها واعتراضها، بل وتغدو أكثر انكشافًا إن انخفض جيل الشّبكة من الجيل الخامس إلى الرّابع، أو الثّالث، دنوًا للثّاني؛ لذا حريّ بنا تجنّب إرسال المعلومات الحسّاسة عبر الأقنيّة الّتي تندرج ضمن هذه الأجيال من الويب.

لذا لأغراض التّواصل، ينبغي أن تُعطى الأولويّة لتطبيقات الْمَسِنْجِر (messengers)، وأنظمة المؤتمرات عبر الفيديو، والبريد الإلكتروني، إعطاء الأفضلية للمراسلين ومؤتمرات الفيديو والبريد الإلكتروني عوضًا عن التّطبيقات الّتي تعمل بتقنية التّشفير التّام بين الطّرفين، علمًا أنّ هذه التّقنية، أي التّشفير التّام بين طرفي المراسلة تعني بأنّ كافّة البيانات المُرسلة من المُرسل إلى المستقبل مشفرة

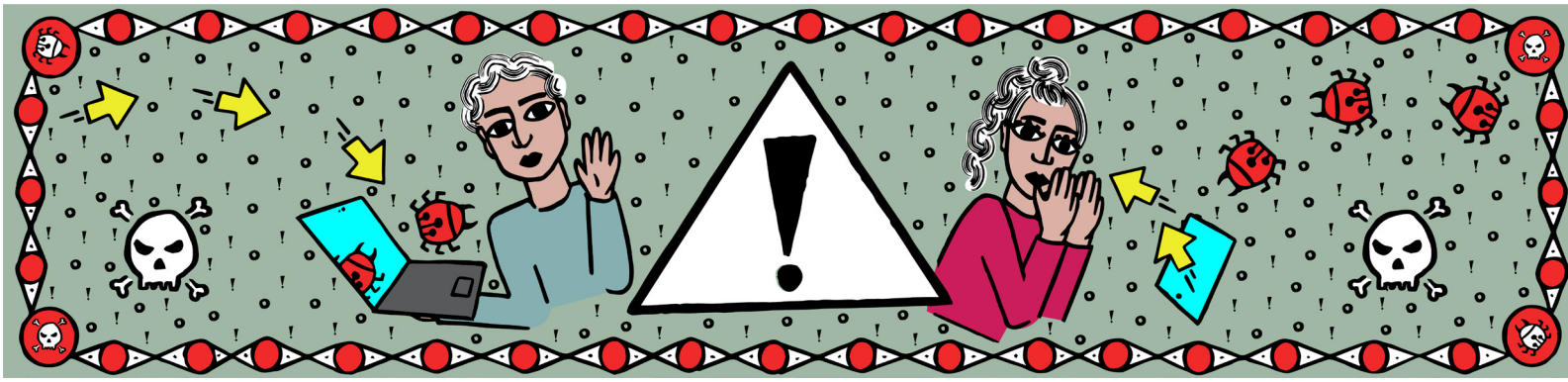
ولا يُمكن لمزود الخدمة تشفيرها. (للمزيد: المحور الرّابع من الفصل الثّاني| أمان الاتصال). على الرّغم من أنّه لا يمكنّنا تجنب مشاركة مواقنا في أثناء استخدام شبكات الهاتف، إلا أنّه يمكنّنا منّع مزودي الخدمات من رصد الخدمات والمواقع نستخدم ونتصفح، وذلك باستخدام ما يسمى بالشبكات الافتراضية الخاصّة، حيث تعمد هذه التقنيّة إلى نقل كل حركة من الجهاز إلى شبكة أخرى غالبًا في بلدٍ آخر عبر نفقٍ مُشفّر لا يمكن ربط بالمُستخدم. للمزيد: القسم الثّاني من المحور الثّالث من الفصل الثّاني: استخدام الشّبكات الافتراضيّة الخاصّة.

قراءات إضافيّة: قسم "أظنّ أنّ ثمّ من يُراقبني،" عدَّة الإسعاف الأوّلي الرّقمي: (قيد الإعداد) منصّة توتم التّعلّميّة الإلكترونيّة، "كيف تتخطّون الحجب على الإنترنت؟ كيف تحاربون الرّقابة على الإنترنت وتحسّنون من خصوصيتكم وأمنكم الرّقمي؟" رابط

1.2| هجمات التّصيّد والهندسة الاجتماعية

يُشير التّصيد إلى قيام خصمٍ أو عدو أو معتدٍ بإرسال روابط أو طلبات بريئة في ظاهرها وخبيثة في باطنها؛ بحيث تستدرج المستخدم لكي يُشارك كلمات المرور أو معلومات الحسابات المصرفيّة الخاصّة به، أو لتثبيت برامج خبيثة تُمكّن المعتدي من التّحكّم بجهاز الضّحيّة عن بُعد، أو سرقة بياناته، أو التّجسّس عليه.

تقدّم منصّة توتم التّعلّميّة الإلكترونيّة مساقًا تدريبيًا بعنوان "هجمات التّصيُّد: لا تضغطوا على هذا الرّابط" رابط



تأتي عمليات التّصيد عادةً بشكل رسالة تستدرجك للقيام بما يلي:

- الدّخول إلى رابط "ما".
- فتح وثيقة.
- تثبيت برنامج أو تطبيق على الجهاز
- إدخال اسم المستخدم وكلمة المرور خاصّتك على موقعٍ ويب مُصمّم خصيصًا لكي يظهر كموقعٍ شرعي ليوقعك في شِراك عمليّة التّصيّد.

أنواع هجمات التّصيد

- تصيّد كلمات المرور، ويُعرف أيضًا بحصاد بيانات الاعتماد (Credential Harvesting)
- التّصيد بالحربة (أو التّصيد الموجّه): يُقصد بهذا النّوع عمليّات التّصيّد الّتي تُبنى على معلوماتٍ يمتلكها المتصيّد عن الضّحيّة، وهنا مربط الهندسة الاجتماعيّة.

- التّصيّد بالصّوت.
- التّصيد بالرّسائل النّصيّة القصيرة.

مؤشرات التّعرّض للتصيّد (الّتي قد تكون قائمة على أساليب الهندسة الاجتماعيّة).

على صعيد المرسل

- عدم التّعرف على عنوان البريد الإلكتروني للمرسل باعتباره جهة اتصال مألوفة ومعتادة.
- البريد الإلكتروني يُشير إلى أنّه لشخص أو جهة خارج المؤسّسة الّتي تعملين بها ولا علاقة له بمهام العمل.
- بريد إلكتروني من شخص ما داخل المنظّمة أو شّريك من غير المعتاد أن يتواصل معك.
- بريد المرسل أو رقمه ينتمي إلى نطاق أو رمز بلد مشبوه.
- لا معرفة شخصيّة بينك وبين المرسل وما من قرينة أو دليل بأنّه شخص موثوق.
- الافتقار لعلاقة عمل أو أي اتصالات سابقة مع المرسل.
- الرّسالة أو البريد الإلكتروني غير متوقع أو غير عادي، كأن يحتوي على رابط تشعبي مضمن أو مرفق من شخص لا اتصال بينك وبينه مؤخرًا.

على صعيد المتلقي أو المستقبل

- نسخ المتلقّي ضمن بريد مُرسل لأكثر من شخصٍ لا يعرفهم شخصيًا؛
- تلقى بريد إلكتروني مُرسل إلى مجموعةً غير متجانسة من الأشخاص. مثال ذلك، بريد إلكتروني إلى مجموعة عشوائيّة من الأشخاص في المؤسّسة يشتركون بالحرف الأوّل من اسم العائلة! أو أن الموجّه إليهم البريد لا صلة لهم ببعضهم البعض.

على صعيد الارتباطات التشعبيّة

- عند تحريك مؤشّر الفأرة على النّص المُضمّن ارتباطًا تشعبيًا يظهر عنوان موقع مختلف.
- احتواء متن البريد الإلكتروني على ارتباطات تشعبيّة طويلة دون أي معلومات إضافية، بمعنى أنّ لا متن للبريد غير الارتباطات التّشعبيّة.
- بريد إلكتروني يحتوي على رابط تشعبي به خطأ إملائيًا لموقع إلكتروني شهير ومعروف.

على صعيد الوقت والتاريخ

- استلام بريد إلكتروني أو رسالة من المعتاد تلقّيها خلال ساعات العمل العاديّة، ولكن استُلِمت في وقتٍ غير معتاد، مثلًا في السّاعة الثّالثة صباحًا.

على صعيد الموضوع

- الموضوع غير ذي صلة بمحتوى الرّسالة أو البريد الإلكتروني.
- متن البريد الإلكتروني عبارة عن رد على شيء لم يسبق للمستلم أن راسل المُرسل بشأنه.

على صعيد المرفقات

- تضمين البريد الإلكتروني أو الرّسالة مرفق غير متوقّع أو ليس له صلة بالرّسالة.
- مرفق من نوع ملف قد يكون خطر.

على صعيد المضمون

- طلب المرسل من المتلقّي النّقر على رابط أو فتح مرفق لتجنيب المتلقي عواقب وخيمة أو للغنيمة بشيء ذي قيمة.
- الرّسالة أو البريد الإلكتروني خارج عن المألوف.
- الرّسالة بها أخطاء نحويّة أو إملائيّة تقوّض من رصانتها.
- طلب المرسل من المتلقّي النّقر على رابط أو فتح مرفق غريب أو لا مبرّر له.
- هل هناك شعور غير مريح حيال طلب المرسل من المستقبل فتح مرفق ما أو النّقر على رابط ما؟
- تضمين البريد الإلكتروني أو الرّسالة طلبًا لإلقاء نظرة على صورة مسيئة أو مُخجلة للمستلم أو شخص يعرفه المستلم.

الوقاية من التّصيّد

للوقاية من التّصيّد، عليك بالخطوات التّالية:

- التّريث قبل النّقر على أي شيء والحذر حيال التّعليمات الواردة في متن البريد الإلكتروني.
- الحفاظ على برامجك مُحدّثة.
- استخدم برنامج مدير كلمات المرور المُضمن بخاصيّة التّعبئة التّلقائيّة لكلمات المرور
- استخدم لوحة المفاتيح الّتي تظهر على الشّاشة لإدخال كلمة المرور، بالذّات للحسابات الحسّاسة جدًا.
- التّحقّق من البريد الوارد، بما فيه من مرفقات وروابط، والإحجام عن فتح أي رابط قبل هذه الخطوة.
- التّحقّق من الرّوابط المُريبة بواسطة هذه المنصّة.
- فتح الوثائق المُريبة بواسطة برمجيات آمنة نحو تايلز أو نظام التخفّي الحي (https://tails.boum.org)، أو منصّة دانجِر زوون، وغوغل دِرايف.
- استعمال المصادقة الثّنائيّة الشّاملة عند التسجيل الدّخول عبر روابط انتقاليّة.
  - للمزيد من المعلومات، يُرجى مراجعة القسم الخامس من المحوّر الأول من الفصل الثّاني المُخصّص لـ"مفتاح المصادقة الثّنائيّة الشّاملة".

رفع الوعي عبر الشّبكة: اختبار غوغل بِشأن التّصيّد.

الاستجابة

لبناء لتنخيل مؤشّرات عمليات التّصيد وبناء الرّد الكابح عليها، عليك بالأقسام التّالية من عدّة الإسعافات الأوّليّة الرّقميّة:
"لا أستطيع الولوج إلى حسابي"
"وصلتني رسالة مريبة"

راجع الأدلة التالية لمجموعة الإسعافات الأولية الرقمية للفرز، وما هو التأثير المحتمل وكيفية الاستجابة:

الرّدود المباشرة:

عِند إدخال بيانات الاعتماد (اسم المستخدم، وكلمة المرور، إلخ.)

- تغيير كلمات المرور (وتوثيق الكلمات الجديدة في برنامج مدير خزنة كلمات المرور فور تغييرها)، وذلك للحساب المعني (أمّا بالنسبة للحسابات الأخرى الّتي تستخدم/ي لها ذات كلمة المرور، فإنّنا نوصيك ونشدّد على ضرورة استخدام كلمة مرور فريدة وعصية على الاختراق لكل حسابٍ على حدة).
  - بهذا الخصوص، من المفيد الاطلاع على القسم الأوّل من المحور الأوّل من الفصل الثّاني "إنشاء وصون كلمات مرور قويّة".
- تفعيل المصادقة الثّنائيّة (إن لم يسبق تفعيلها)
  - بهذا الخصوص، من المفيد الاطلاع على القسم الخامس من المحور الأوّل من الفصل الثّاني "استخدام المصادقة بعاملين".
- في حال تعذّر تغيير كلمات المرور أو تفعيل المُصادقة الثّنائية، أو كلا الأمرين، فخيارُك الأخير: إغلاق الحساب (بعد الاحتفاظ بنسخٍ احتياطيّة من كافّة بيانات الحساب، إن أمكن).
- إعلام مزود الخدمة.

عِند تنزيل ملفّات خبيثة أو ضّارة (افتراضًا)

- وقف اتصال الجهاز بالإنترنت، بما في ذلك وقف تفعيل بيانات المحمول الواصلة بالإنترنت، والواي فاي، والبلوتوث.
- فحص الجهاز بواسطة البرامج المضادّة للبرمجيّات الخبيثة.
- تُعد النّسخة المجّانيّة من برنامج مال-وير بايتس أحد البرامج المضادة المُتاحة| رابط.
- الاطلاع على قسم "جهازي يتصرّف على نحو مريب" ضمن عدّة الإسعافات الأوّليّة الرّقميّة| رابط.
- اللّجوء للدّعم الاحترافي| رابط.
- الاطلاع على المحور الأوّل من القسم الثّالث من الفصل الأوّل من هذا المنشور "المراقبة الرّقميّة: برمجيّات التّجسّس".

1.3| التّحرّش والملاحقّة عبر الإنترنت

ثمّ تزايد في وتيرة التّحرّش والملاحقة عبر الإنترنت لإسكات وتهديد منظّمات المجتمع المدني، والنّشطاء، والكوادر الإعلاميّة؛ علمًا أنّ النّساء وأفراد مجتمع ميم عين ينالون الحصّة الأكبر من هذه الاعتداءات على مختلِف فضاءات وسائل التّواصل الاجتماعي.

الوقاية في خطوات

- تجنّب مشاركة مكانك أو موقعك على وسائل التّواصل الاجتماعي.
  - التّحقّق من آخر منشوراتك على وسائل التّواصل الاجتماعي: هل تتضمّن إشارة إلى موقعك الدّقيق؟ إن كانت الإجابة نعم، فلا بدّ من إلغاء تفعيل وصول تطبيقات الوسائل الاجتماعيّة والخدمات الأخرى لنظام التّموضع العالمي على هاتفك كي لا يظهر موقعك عند نشر تحديثاتك.
  - تحقق من صورك الّتي نشرتها عبر الإنترنت: هل تتضمّن تفاصيل يمكن التّعرف من خلاله على موقعك بوضوح؟ لحماية نفسك من محاولات المُلاحقة المُحتملة، ينبغي ألّا تُظهر موقعك الدّقيق عند نشر صور أو مقاطع فيديو خاصّة بك.
  - من المفيد أيضًا تجنّب تفعيل نظام تحديد التّموضع العالمي طوال الوقت، بحيث يقتصر تفعيله لفترات وجيزة عندما يكون هناك حاجة حقيقية لتحديد موقعك على الخريطة.

- تجنب سهولة الوصول إلى أجهزتك وحساباتك عبر الإنترنت
- التّثبّت من أنّ كلمتك المرور للوصول إلى أجهزتك وحساباتك (مثل Apple-ID) أو حساب غوغل (Google Account) فريدة وطويلة ومعقدة كما ينبغي
  - للمزيد بهذا الخصوص، يُمكنك الاطلاع على القسم الأوّل من المحور الأوّل من الفصل الثّاني "إنشاء وصون كلمات مرور قويّة"
  - تفعيل المُصادقة الثّنائيّة (إن لم يسبق لك تفعيله)
  - للمزيد بهذا الخصوص، يُمكنك الاطلاع على القسم الخامس من المحور الأوّل من الفصل الثّاني "استخدام المصادقة الثّنائيّة الشّاملة"
  - فحص الجهاز للتحقّق برمجيات المُلاحقة والتّجسّس
  - للمزيد بهذا الخصوص، يُمكنك الاطلاع على القسم الأوّل من المحور الثّالث من الفصل الأوّل "المراقبة الرّقميّة: برمجيّات التّجسّس"
- تقليل المعلومات المتاحة عنك للعموم عبر وسائل التّواصل الاجتماعيّة
  - للمزيد بهذا الخصوص، يُمكنك الاطلاع على دليل تجميع المعلومات الذّاتي: لنتعرّف ماهيّة المعلومات المُتاحة عنك على الإنترنت| رابط
- رفض أي رسائل من مرسلين لا تعرفهم. تُتيح بعض تطبيقات الدّردشة—نحو واتس-آب، وسِغنَل، وتطبيق الدّردشة الخاص بمنصّة فيسبوك—معاينة الرّسائل قبل قبول الجهة المرسلة جهةً موثوقٍ بها. بالمِثل، يُتيح تطبيق آمَسِج آبِل (Apple iMessage) تغيير الإعدادات لتنخيل الرّسائل المُتلقّاة من جهات غير معروفة. خلاصة القول، إيّاك قبول رسالة أو جهة اتصال تعتقد بأنّها مشبوهة أو مريبة أو لا تعرفها.

مواجهة التّحرّش والملاحقة الرّقميّة: الخطوات

- لفهم التحرّش والملاحقة الرّقميّة والتّخفيف من آثارها، عليك بالأقسام التّالية من عدّة الإسعافات الأوليّة الرّقميّة:
  - إنّهم يتحرَّشون بي عبر الإنترنت | رابط
  - أحدهم ينتحل هويّتي على الإنترنت | رابط
  - ثَمَّ من يتحرّش بي عبر الإنترنت | رابط (قيد الإعداد)
  - ثمّ من يستهدفني بحملة تشهير | رابط
  - ثمّة من سرّب بياناتي الخاصّة أو نشر معلومات أو ميديا عنّي دون إذني | رابط (قيد الإعداد)
- سواء أكنت تعرف/ين المتحرش بك أم لا، فإنّ الخيار الأفضل دومًا هو الحظر على كافّة منصات التّواصل الاجتماعي—إن أمكن ذلك.
  - لكن قبل الحظر، عليك توثيق الاعتداء، فما أن تحظر/ين المعتدي، تنتفي إمكانيّة الوصول إلى محتواه—تذكّر/ي ذلك. (للمزيد بهذا الخصوص، يُمكنك الاطلاع على 3.5| توثيق انتهاكات الحقوق الرّقميّة)
- كذلك ينبغي التّبليغ عن فعلّة التّحرش، إن كان هذا الخيار آمنًا ومناسبًا، إذ أنّ لكلّ دولةٍ قوانينها لحماية مواطنيها من التّحرّش عبر الإنترنت، وبتّالي ينبغي لكل إنسان استكشاف التّشريعات في البلد المعني أو طلب المشورة القانونيّة للمساعدة في تحديد ما يجب القيام به.
  - أمّا إنْ لم تكن تعلم هويّة متحرّشك، يُمكنك في بعض الحالات تتبع هويّة الجاني من خلال تحليل الطّب الجنائي للآثار الّتي قد يكون تركها الجاني خلفه.

- إن كنت تتلقّى رسائل تهديد، بما في ذلك التّهديد بالعنف الجسدي أو الجنسي، أو الابتزاز، فعليك توثيق ما مررت به قدر الإمكان، بما في ذلك توثيق أي روابط ولقطات للشاشة، والتّبليغ عن المعتدي عبر المنصّة الّتي تمّ الاعتداء في فضائها أو مزود الخدمة ذي الصلة، ثُمّ حظر المعتدي، ولا بد من النّظر في خيار التّحرّك قانونيًّا بحق المعتدي والجهات الضّالعة.
  - راجع/ي المحور الخامس من الفصل الثّالث| "توثيق انتهاكات الحقوق الرّقميّة"
  - راجع/ي قسم "توثيق الحالات الرّقميّة الطّارئة" | رابط (قيد الإعداد)
- تلقي اتصالات غير مرغوب فيها، من مكالمات هاتفيّة، أو رسائل نصيّة قصيرة، أو رسائل عبر تطبيقات الدّردشة المرتبطة برقم هاتف محمول، أو بريد إلكتروني، أو معلومات اتصال خاصة أخرى.
  - حاول تغيير رقم الهاتف المحمول، أو الشّريحة، أو البريد الإلكتروني، أو معلومات الاتصال الأخرى المرتبطة بالحساب.
  - النّظر في التّبليغ عن الرّسائل والحساب ذي الصّلة وحظرها على المنصّة أو التّطبيق محط الاعتداء.
- التّعرض لانتحال الشخصية
  - بهذا الخصوص، يُمكنك الاطلاع على قسم "أحدهم ينتحل هويّتي على الإنترنت،" عدّة الإسعافات الأوّليّة الرّقميّة | رابط

خطاب الكراهية

- للتعرّف على ماهيّة خطاب الكراهيّة ومواجهته، عليك بدليل مكافحة خطاب الكراهية في الفضاء الرّقميّ | رابط

معايير تقييم خطورة خطاب الكراهية

- الجهة الّتي تنتج المحتوى: هل الشّخصيّة عامّة أو صفحة/جهة مؤثّرة، ولها كثير من المتابعين/ات أم شخص عادي غير مؤثر/متابع؟ مدى السّلطة الّتي يمتلكها النّاشر؟
- مدى انتشار الخطاب: هل هذا النوع من الخطاب منتشر أم محدود؟ هل نشر لمرّة أم انتشر على نطاقٍ واسع وبوتيرة متكرّرة؟
- النّيّة: هل النّيّة من تداول المحتوى هي إحداث كراهية وتفرقة وانقسامات؟
- المضمون: هل يُعدّ المضمون خطيراً أم محدود الخطورة؟ هل يدعو للعنف أو الكراهية على نحوٍ مباشر أو غير مباشر؟
- السّياق السّياسي والاجتماعي: هل السّياق السّياسي مهيّأ لجولات عنف جرّاء هذا الخطاب أم لا؟ هل الخطاب موجّه ضد فئات مهمّشة سياسيًّا؟

مبادئ التّصرّف

- التّحقّق من أنّ المحتوى يشكّل خطابًا معزّزًا للكراهية.
- عدم الانخراط والرّد على خطاب الكراهية بخطاب كراهية.
- الرّد على خطاب الكراهية بخطاب عقلاني تنفيذي، إن لم ينطو الأمر على خطر.
- التّعلم والتّثقيف بشأن خطاب الكراهية.
- توثيق المحتوى الضّار.

- **لتوثيق المحتوى الضّار، يجدر جمع المعلومات التّالية:**
  - معلومات الضّحية: اسم الضحية/المتضرّرة/ة؛ البريد الإلكتروني للتواصل معه/ا، وتصنيفه/ا– أي هل الفرد ناشط/ة، أم صحفي/ة، أم أكاديمي/ة، إلخ–العمر، والنّوع الاجتماعي، والموقع الجغرافي، ورقم الهاتف.
  - معلومات الواقعة: على أي منصّة نُشر خطاب الكراهيّة؟ بأي تاريخ نُشر، وما نوع الانتهاك، ونوع المنصّة، والمحتوى، ووصف السّياق الّذي جاء فيه، وصيغة المحتوى.
  - معلومات المعتدي/ـة: اسم المعتدي/ة، واسم المستخدم الخاص به على المنصة الّتي استخدمها لنشر المحتوى الضّار، ونوع الحساب، ورابط، وحساب المعتدي/ة، ورابط المحتوى الضّار، وصورة شاشة للمحتوى، وصورة شاشة للحاسوب، وجنسيّة/سياق المعتدي/ة (فلسطيني أم إسرائيلي).
  - معلومات التّوثيق والمتابعة: تاريخ التّبليغ، والإجراء المتخذ، والنّتيجة.

- **كيف نجمع هذه المعلومات؟**
  - تصوير لقطة شاشة للمحتوى سواء كان تعليقًا، أو منشورًا، أو صورة، أو غيرها من أشكال المحتوى على أن تُظهر اللّقطة المحتوى نفسه واسم النّاشر.
  - نسخ المحتوى وحفظه إن كان نصًّا، وحفظه إن كان صورة أو مقطع فيديو.
  - الضّغط على وقت المنشور الموجود أعلى المحتوى وأسفل اسم حاسب النّاشر، ومن ثم نسخ وحفظ رابط المنشور ذاته.
  - الضّغط على اسم الشّخص الّذي نشر/ت المحتوى للوصول إلى حسابه/ا الشّخصي، وأخذ لقطة شاشة للحساب.
  - حفظ رابط الحساب.
  - تدوين اسم المستخدم، وبريده/ا الإلكتروني إن وجد، وتدوين اسم الضّحيّة ومعلوماتها.
  - تدوين تاريخ النّشر وانتماء هذه الجهة، إن كانت، مثلًا فلسطينيّة أو إسرائيليّة.

- **كيف نبلّغ عن وجود خطاب كراهيّة عبر الفضاء الرّقمي؟**
  - التّبليغ المباشر عن المحتوى بالضّغط على زر التّبليغ على المحتوى نفسه في المنصّة الّتي ينشر عليها.
  - التّبليغ عبر منصّات مثل منصّة حُر التّابعة لمركز حملة.
  - تقديم شكوى رسميّة لجهاز الشّرطة أو نيابة الجرائم الإلكترونيّة.

- **أبرز إجراءات منظّمات المجتمع المدني لمواجهة خطاب الكراهية**
  - رصد وتوثيق المحتوى.
  - تحويل طلبات إلى شركات التّواصل الاجتماعي لإزالة المحتوى الدّاعي للكراهيّة عبر منصّاتها.
  - تنظيم حملة تبليغات جماعيّة لمناهضة المحتوى الدّاعي للكراهيّة.
  - المطالبة بمحاسبة القائمين/ات على نشر خطاب الكراهية من خلال الجهات الرسميّة.

- **إرشادات إضافية**
  - إن كان حديث الكراهية صادراً عن شخص واحد، فإنّ التّبليغ والحظر يبقيان أسهل الطّرق وأسرعها لاحتواء الاعتداء ومنع المعتدي/ة من مواصلة إرسال رسائل الكراهيّة، لكن يجب ألّا ننسى أن الحظر يحول دون تمكّننا من الوصول إلى محتوى الكراهية لتوثيقه. في هذا الصّدد،

يُمكنك الاطلاع على القسم المحور الخامس من الفصل الثّالث "3.5. توثيق الانتهاكات الحقوق الرّقمية."

- إن كان الاعتداء من أكثر من شخص، فقد يكون الشّخص هدفًا لحملة كراهيّة أو تحرّش، لذا لا بدّ من التّفكّر والتّأمل بالاستراتيجيّة الفضلى الّتي تُواجهك. في هذا السّياق وللتعرّف على الاستراتيجيّة الفضلى لحالتك، يُمكنك الاطلاع على صفحة حملة تايك باك ذَا تِك (Take Back The Tech) بشأن استراتيجيّات التّصدي لخطابات الكراهيّة: رابط

موارد

- منصّة توتم التّعلّميّة الإلكترونيّة، تدريب: "كيف تحمون هويّتكم على الإنترنت؟ بعض وصفات المجهوليّة" | رابط
- "مواجهة التّحرّش على الإنترنت: أدوات لمساعدة الصّحفيين في كش الذّباب الإلكتروني والتّعرّف على تكتيكات المتحرّشين" | رابط
- منظّمة خَطُّ مساعدة الأمان الرقمي لمنظمة – أكْسِس ناو، دليل مكافحة استلال المعلومات الشّخصيّة لأغراض التّشهير | رابط
- الأسئلة الشّائعة: مجتمع المدني هدف لحملات التّحرّش عبر الإنترنت | رابط
- نادي القلم الأميركي، دليل ميداني للحماية من الإساءة و المضايقات الإلكترونيّة | رابط
- منظّمة إِكْوَالِتي لابس، دليل النّشطاء لمكافحة حملات اليمين المُتطرّف لاستلال البيانات الشّخصية | رابط
- منصّة فِم-تِك-نِت، لنؤمّن هوّيّتنا الرّقميّة| رابط
- نَاشْنال نِتورك لقضاء على العنف الأسري: نصائح للنجاة لتوثيق الاعتداءات والملاحقات الرّقميّة | رابط

1.4| تصيّد (ترولينغ)

باعتباره أداة يُشهرها أشخاصٌ يُعادون آخرين أو يعمدون لاستفزازهم نحو استجابةٍ عاطفيّة في أنفسهم، بات التّصيد (ترولينغ) أشيع على نطاقٍ واسع، فتعدّى أن يكون فعلًا مباشرًا بل أُكِسبَ أشكالًا وطرائق هجينة باستخدام روبوتات التّحكّم بواسطة لجان التّصيّد وما شاكلها.
تكتيكات التّصيّد وفقًا لما جاء دليل استقصاء التّهديدات الرّقميّة: حملات التّصيّد الصّادر عن الشّبكة العالميّة للصحافة الاستقصائيّة | رابط

- التّضخيم من ديناميّات وسوم (هاشتاغات) وسائل التواصل الاجتماعي
- الاختراق
- التّلاعب العاطفي
- الدّعاية الشّعبيّة السّياسيّة الزّائفة
- استهداف أفراد مؤثّرين
- تصميم الميمات وبثّها
- التّزييف العميق والإعلام المغشوش
- استغلال الانقسامات القائمة

المواجهة

- كشف اعتداءات التّصيّد والبت فيما إذا كان الاعتداء مُفردًا أو محصوراً ببعض الحسابات أم أنّنا أمام حملة تصيّد تضم العديد من الحسابات، وتُنفّذ على عدّة منصّات تواصل اجتماعي، وتنطوي على آليات لمشاركة مضامينها بطريقة آليّة:
  - رصد منصّات التّواصل الاجتماعيّ بحثًا عن أي نشاط مشبوه أو تغييرات مفاجئة في نبرة أو محتوى المناقشات على الإنترنت.
  - استخدم أدوات الاستماع الاجتماعي لتتبّع كلمات بعينها، أو وسوم، أو عبارات قد ترتبط بحملات تصيد أو تحرش، عدا أدوات تحليل الشبكة للخروج بتصورات حيال أي روابط بين الحسابات المشبوهة وكشف أيّ تنسيقٍ محتملٍ فيما بينها.
  - تحليل مضامين الرّسائل بحثًا عن أنماطٍ معيّنة، أو روابط، أو أمارات تضليل كامن.
  - التّحقّق من الملفات الشّخصيّة للمتصيدين المحتملين، بما في ذلك تواريخ إنشاء حساباتهم وأنماط ووتائر النّشر صِلتها بحسابات التّصيّد المعروفة.
  - توثيق البيانات وحفظها باستخدام لقطات الشاشة والأراشيف العامّة مثل واي-باك ماشين (رابط).
    - راجع/ي المحور الخامس من الفصل الثّالث| "توثيق انتهاكات الحقوق الرّقميّة"
  - التّبليغ عن اعتداءات التّصيّد على المنصّات ذات صلة وتقديم شكاية بشأنها.

- **المعلومات التي يجب تضمينها في البلاغات**
  - سياق الحملة
  - الأفراد أو المجتمعات المستهدفة
  - دوافع وأهداف الأفراد أو الجهات الّتي تقف خلف التّحرّش أو التّصيّد
  - دليل على التّنسيق أو الجهود التّنظيميّة الكامنة خلف فعل التّصيّد أو التّحرّش
  - المنهجيّة والأدوات المستخدمة في الكشف والتّحليل
  - البيانات الكميّة والنّوعيّة، مثل حجم الرّسائل أو خطورة التّحرّش
  - العواقب والتّأثيرات المحتملة على الأفراد أو المجتمعات المستهدفة
  - ارتباط فِعل التّحرّش أو التّصيّد بالسّياق الاجتماعيّ أو السّياسيّ—إن كان ذا صلة أو قرينة
  - أي إجراءات تتخذها منصّات التّواصل الاجتماعي، أو جهات إنفاذ القانون، أو غيرها من الأطراف الاختصاص لمعالجة الاعتداء.
- التّبليغ أي حملات تصيّد أو تحرّش مُثبتة للنهوض بالوعي والإسهام بالتّخفيف من آثارها.

موارد

- منصّة توتم التّعلّميّة الإلكترونيّة، "كاشف التّصيد والمتصيّدين؟ أدوات للإعلامين والإعلاميّات للتعرّف على المعتدين عبر الإنترنت وتكتيكاتهم" | رابط
- الشّبكة العالميّة للصحافة الاستقصائيّة، دليل استقصاء التّهديدات الرّقميّة: حملات التّصيّد | رابط

1.5| انتهاكات الخصوصيّة

يعيش الفلسطينيون والفلسطينيّات في الأرض الفلسطينيّة المحتلّة واقعًا مليئًا بالانتهاكات المتشبعة المصدر؛ تهدد حقوق الأفراد المدنيّة، والسّياسيّة، والاقتصاديّة، والاجتماعيّة، والثّقافيّة؛ على أرض الواقع كما بالفضاء الرّقمي. وبشكلٍ خاص، تفرض السّلطات الإسرائيليّة أقسى أنواع الانتهاكات وأشدها وطأة وبشكلٍ ممنهج؛ ويُعدّ جزء من ذلك [ال]اختراق [المتواصل] للحق في الخصوصيّة بما فيها البيانات الشّخصيّة. . وتداولها، وترسيخ نظامًا مترامي الأطراف من الرّقابة، عدا الرّقابة الإلكترونيّة واستخدام البيانات الشّخصيّة لكيل الاتهامات للفلسطينيين والفلسطينيّات في المحاكم الإسرائيليّة العسكريّة. بالمقابل، لا تخضع السّلطات الإسرائيليّة، سواء على الصّعيد المحلّي أو الدّولي، لأي شكلٍ من المحاسبة أو العقاب أو الإجراءات القانونيّة على الجرائم والانتهاكات الّتي ترتكبها بحقّ الفلسطينيين والفلسطينيّات، بما في ذلك انتهاكها لحقّهم الأصيل بالخصوصيّة. عِلاوة على ذلك العلاقة الوطيدة بين سلطات الاحتلال والقطاع الخاص الإسرائيلي، الرّائد في مجال الرّقابة والتّجسّس؛ الّذي أنتج ثكنة من برامج وتقنيات التّجسس للإمعان في انتهاك الخصوصيّة، مثال ذلك تطبيقَي المنسّق وبيغاسوس المعروفين بانتهاكهما لخصوصيّة الأشخاص، لا سيّما الفلسطينيّين/ات في الضفة الغربية المحتلة.

- حملة – المركز العربي لتطوير الإعلام الاجتماعي، 2023، "ورقة موقف: انتهاكات مستمرّة وإهمال واضح تجاه حقّ الخصوصية والبيانات الشّخصية الفلسطينيّة" | رابط

توصيات ورقة الموقف (باستثناء التّوصيّة القانونيّة)

- ضرورة تعزيز الوعي الفلسطيني الحقوقي بشأن مفهوم الخصوصية ومضمون البيانات الشّخصيّة، وحُرمة الحياة الخاصّة، بالذّات فيما يتعلّق بعلاقة الأفراد بالشّركات، والجهات الحكوميّة الرّسميّة.
- تعزيز معرفة الفلسطينيين والفلسطينيّات بالمؤسّسات والمنصّات الّتي تعمل على رصد انتهاكات الحقوق الرّقميّة، نحو المرصد الفلسطيني الأوّل لتوثيق انتهاكات الحقوق الرّقميّة (حُرّ).
- مواصلة وتكثيف العمل على رص الانتهاكات الرّقميّة، لا سيّما تلك المُتعلّقة بالخصوصيّة وتوثيقها ومتابعتها، بما في ذلك عبر المنصّات الفلسطينيّة، نحو المرصد الفلسطيني لتوثيق انتهاكات الحقوق الرّقميّة (حرّ)؛ وتعزيز آليات العمل الأهل المشترك، بالذّات المناصرة والضّغط على صنّاع القرار.

في ضوء هذه التّوصيات، نضع بين أيديكم جُملة أخرى من الخطوات للتصدّي للانتهاكات الرّقميّة:

- توثيق أي شكل من أشكال انتهاك الخصوصيّة: للمزيد بهذا الخصوص، يُمكنك الاطلاع على المحور الخامس من الفصل الثّالث "توثيق انتهاكات الحقوق الرّقميّة."
- إدانة ورفض أي انتهاك لخصوصيتك والمطالبة بحقوقك تجاه وسائل التّواصل الاجتماعي والشّركات المضيفة للتطبيقات محط الانتهاك، وذلك باللّجوء إلى آليات الشّكوى والتّظلم المرعيّة لهذه الشّركات والجهات بالإضافة لطلب دعم منظّمات الحقوق الرّقميّة.
  - المرصد الفلسطيني لتوثيق انتهاكات الحقوق الرّقميّة (حرّ): رابط
  - فريق الاستجابة لطوارئ السّلامة المعلوماتيّة للمجتمع المدني: رابط
- الحرص كل الحرص إن كنت تنشر/ين محتوى على فضاءٍ رقمي، نحو موقع أو مدونة، أن تكون الجهة المضيفة للمساحة ممن لا يتشبثون بالمطالبات القانونيّة المُسيّسة أو بأحسن الأحول أن يكونوا من داعمي حريّة التّعبير وحقوق الإنسان، وفيما يلي بعضهم، تمثيلًا لا حصرًا:
  - https://maddix.net
  - https://greenhost.net
  - https://qurium.org
- أخيرًا وليس آخرًا، تذكُر الأثر النّفسي لمثل هذه الاعتداءات، وبتّالي بناء حصانة عاطفية فردية وجماعية والحفاظ عليها.

2| أدلّة الأمان الرّقمي

يُقدّم هذا الدّليل جُملةً من النّصائح المُفيدة بشأن الموضوعات التّالية:

2.1 | أمان كلمات المرور والحسابات
2.2 | أمان الأجهزة
2.3 | أمن الإنترنت
2.4 | أمن الاتّصال
2.5 | حماية البيانات

أعُدّت كافّة الأدلّة بالاستناد إلى المصدرين التّاليَين بالإضافةِ إلى طيفٍ من المضامين السّياقيّة:

- عُدّة الأمان الرّقمي: أدوات وممارسات للأمان الرّقمي، صادر عن منظّمة فرونت لاين ديفندرز: رابط
- عدَّة الإسعاف الأوّلي الرقمي، صادر عن فريق الاستجابة لطوارئ السلامة المعلوماتية للمجتمع المدني: رابط

دروس عمليّة

رغم ما قد نتخذه من خطواتٍ لتحسين أماننا الرّقمي كُلّ فترة وأخرى، بيد أنّ ذلك لا ينفي أهمية تبني ما يُشبه الرّوتين للحفاظ على أماننا، فلا سبيل لتعزيز أماننا الرّقمي باستدامة وفعاليّة بمعزلٍ عن الحفاظ على نسخ احتياطيّة من بياناتنا واستخدام برامج الشّبكات الافتراضيّة ومدير كلمات المرور. تُظهر البحوث الفسيولوجية للدماغ أنّ قيامنا بأمرٍ ما 300 مرة يحفره في ذاكرتنا العضليّة، بحيث لا نعود نفكّر بهذه الأفعال في أثناء القيام بها، وهذا يُفسّر صعوبة إنشاء كلمات مرورنا والتريث في كلّ مرة نُدخلها في البداية، لكن لاحقًا تركض أصابعنا وحدها على لوحة المفاتيح دون أيّ عناء.

مصادر تعليميّة إضافيّة

- عدَّة الإسعاف الأوّلي الرّقمي | رابط
- فقدت جهازي | رابط
- جهازي يتصرّف على نحو مريب | رابط
- موقعي عطلان! ماذا أفعل الآن؟ | رابط
- ضاعت بياناتي | رابط
- برامج التّعلّم الذّاتي عبر منصّة توتم التّعلّميّة الإلكترونيّة | رابط
- كيف يعمل الإنترنت؟ ليس سُحبًا وإنما كابلات: لنستكشف الإنترنت معًا | رابط
- كلمات السّر الآمنة: Pa$$word123، أحقًا اخترتم هذه الكلمة؟ اتبعوا هذا الدّليل لإدارة كلمات السّر بشكلٍ سليم | رابط

- تطبيقات المراسلة الآمنة: دردشوا، تواصلوا، تراسلوا: كيف تتراسلون بطريقة أكثر أمانًا؟ | رابط
- تأمين الأجهزة: إنها مسألة عادات سليمة! | رابط

2.1| أمان كلمات المرور والحسابات

يكاد لا يوجد جهاز، أو منصّة، أو خدمة نَلج إليها دون أن تُطالبنا بشكلٍ من أشكال التّعريف عن الذّات.
اعتمادًا على نوع الخدمة، تُصبح الهوية مطلبًا لحفظ البيانات أو تخزينها، (على سبيل المثال: رسائل البريد الإلكتروني أو المستندات)، كذلك الأمر بالنّسبة للتفضيلات والإعدادات في مساحة خاصة، عدا ما لذلك من ضرورة للحؤول دون وصول من لا صفة أو تخويل، أفرادًا كانوا أم أنظمة.
في المقابل، لا تتطلب العديد من الخدمات حسابًا لك عليها لاستخدامها، خذ مثلًا محركات البحث والمواقع الإلكترونيّة، غالبًا ما يستخدمون آليات أخرى مثل ملفات تعريف الارتباط **لتعقب وتتبع** سجل تفاعلك مع خدماتهم ومواقعهم.
في معظم الحالات، يتمثل هذا الإجراء بحساب ننشئه للاستخدام خدمات هذه المنصات والمواقع أو للاشتراك فيها، وعند إنشاء الحساب، عادةً ما يتعيّن علينا إدراج اسم المستخدم أو عنوان بريدنا الإلكتروني باعتباره مُعرِّفًا فريداً للحساب. بالإضافة للحساب، يُطلب منّا إنشاء كلمة مرورٍ كمفتاح عبور لحساباتنا ومنها إلى خدمات المواقع والمنصّات.
يستند محتوى هذا الفصل على مادّة "**إنشاء** وإدارة **كلمات سرٍّ قويّة**" المتاحة عبر منصّة دليل عدَّة الإسعاف الأوّلي الرّقمي الصّادر عن **منظّمة فرونت لاين ديفندرز**: رابط

مصادر تعليميّة إضافيّة

- الدّفاع عن أنفسنا أمام مجهر المُراقبة، "وضع كلمات سر قوية"
- تِك رادار، "مخاطر مُشاركة كلمة المرور في العمل"
- جمع باحث الأمن الرّقمي دانييل ميسلر قائمة تضم أكثر 1000 كلمة مرور شيوعًا ينبغي لنا تجنبها لكثرة دورانها واستخدامها بين الناس.
- توفر موسوعة ويكيبيديا مجموعة متنوعة من المقالات التي تغطي مواضيع متعلقة بكلمات المرور. تتضمن هذه المقالات إرشادات تتناول تأمين كلمات المرور وطرق منع المخترقين والمتربصين من الوصول إلى حساباتنا.

2.1.1| إنشاء كلمات مرور قوية والحفاظ عليها

كلمات السرِّ مهمّة للغاية لحفظ بياناتكم وهوياتكم آمنة. والمهاجمون يعلمون هذا بالطبع، لذا فهم يتحايلون بأساليب مختلفة لمعرفة كلمات سرّكم.
لكن بوسعكم مجابهة تلك الحيل باستخدام بعض أدوات وباتّباع بعض الممارسات. الاستراتيجية الأنجع تتمثّل في وضع كلمات سرّ طويلة عشوائية فريدة بقدر الإمكان. لعمل هذا بكفاءة يتعيّن عليكم استعمال مدير لكلمات السرّ. من المهم أيضًا استعمال التّحقّق أو ما يُعرف أيضًا بالمصادقة بعِدَّة عوامل كلمّا أمكن ذلك.

معرفة ما إذا كانت كلمات المرور الخاصة بك قد تم اختراقها

- بحثوا في موقع "Have I Been Pwned" بعناوين بريدكم التي تستخدمونها في فتح الحسابات في المواقع والخدمات لتعرفوا ما إذا كان أحد تلك الحسابات قد تسرّبت معلومات منه.
  - بدّلوا فورًا كلمات سرّ الحسابات التي تظهر لكم في نتيجة البحث، متّبعين الإرشادات التالية لتنصيب واستعمال مدير لكلمات السرّ.
- وحتّى إذا لم يظهر أيّ من حساباتكم في نتائج البحث، فيُستحسن أنْ تتّبعوا الإرشادات التالية، لأنّ اختراقات الحسابات لا تعُرف كلّها فورًا، إنْ عُرِفَت.

المزيد عن سبب توصيتنا هذه

يبحث المهاجمون عن كلمات سرّ الحسابات التي تسرّبت معلوماتها مِنْ قَبْل، ثم يُجرّبون الدخول بها إلى حساباتكم في خدمات أخرى حتّى يفلحوا. لذا فاستخدام كلمة السرّ نفسها مع أكثر من حساب خطير للغاية. انظروا في Have I Been Pwned لتروا ما إذا كانت كلمات سرّكم موجودة في أيٍّ من القوائم التي يستعملها المهاجمون.

تفادي توليفات كلمات السرّ الضعيفة الشائعة

فيما يلي الطرق الأكثر شيوعًا التي يصل من خلالها المتربصين بنا لكلمات السّر الّتي نستخدمها:
هذه هي الطرق الأكثر شيوعًا بين المهاجمين لمعرفة كلمات سرّكم:

1. **بالتخمين:**
   - باستخدام بياناتكم الشخصية مثل التواريخ المهمّة والأسماء والاقتباسات وعناوين الأغاني أو أسماء المؤلفين المعروف حبّكم لهم
   - باستخدام مُعجم
   - بإحداث تغييرات طفيفة في كلمات سرّ سبق لكم استخدامها
   - باستخدام برمجيات تجري كُلَّ التوافيق والتباديل الممكنة لكلمة السرّ
2. **ولفعل ذلك فهم يسعون إلى معرفة:**
   - المواضع التي تضعون فيها كلمات سرّكم (مثل قصاصات الملاحظات على المكتب)
   - ضربات المفاتيح عندما تدخلون كلمات السرّ
   - كلمات السرّ التي سبق وانكشفت ومتاحة على الإنترنت
3. **كما يسعون إلى التحايل عليكم لدفعكم إلى:**
   - تنصيب برمجية خبيثة تسجّل كلمات سرّكم وترسلها إليهم
   - إدخال كلمات سرّكم في صفحات ولوجٍ مزيّفة بطريق التصيُّد
   - الإفصاح عن كلمات سرّكم بانتحالهم صفة عاملي الدعم الفني في خدمة ما أو انتحال هوية بعض معارفكم (المعروف باسم الهندسة الاجتماعية)
4. **ويستغلون الثغرات:**
   - لاختراق مواقع الويب التي تستعملون لها كلمات السرّ
   - لسرقة كلمات سرّكم إنْ كانت محفوظة في المتصفّح
   - لسرقة كلمات سرّكم من التطبيقات في هواتفكم

اتّبعوا الإرشادات التالية لحماية أنفسكم من تلك الهجمات:

- استعملوا دومًا للولوج إلى حساباتكم جهاز نظيف مُحدَّث محمي تثقون به، وكذلك عند النفاذ إلى بياناتكم الحسّاسة.
- انتبهوا إلى أن الممارسات التالية وحدها لا تزيد أمان كلمات السرّ:
  - استخدام كلمات أو أرقام ذات علاقة بكم أو بالأشخاص والمنظّمات ذات الصلة بكم، مثل:
    - أسماء الناس والحيوانات الأليفة والمنظّمات
    - تواريخ الميلاد والمناسبات الشخصية المهمّة والعطلات
    - أرقام الهواتف والعناوين
    - كُلُّ ما تمكن معرفته عن الشخص بالبحث ومِنْ المحيطين به
  - استخدام العبارات الشائعة، مثل الاقتباسات وأبيات الشعر والأغاني.
  - استبدال بعض المحارف بأخرى مشابهة، مثل استبدال حرف a بالرمز @، إلخ.
  - زيادة علامات التعجّب والأرقام وعلامات الترقيم إلى آخر الكلمة
  - ابتداء كل كلمة بحرف لاتيني كبير
  - استخدام كلمات مفردة من الواردة في معجم
  - تغيير كلمات السّر دوريًّا

اتّبعوا الإرشادات التالية لحماية أنفسكم من تلك الهجمات:

2.1.2| استخدام مدير كلمات المرور

- قوموا بتحميل KeePassXC (لنظام لينُكس أو ويندوز أو ماك) أو KeePassDX (لأندرويد) StrongBox (لآي. أو. اِس)
- لا تكرّروا استخدام كلمات السرّ أبدًا.
- اجعلوا مدير كلمات السرّ يولّد لكم كلمة سرّ طويلة عشوائية فريدة ويحفظها، لكلٍّ من حساباتكم.
- قد ترغبون في إعداد مدير كلمة السرّ مع زملائكم، بوسعكم مساعدة بعضكم بعضًا.
  - كما قد ترغبون كذلك في الإلمام بصيرورة التشارك في كلمات السرّ بأمان. علمًا بأن الأفضل دومًا إنشاء حسابات مختلفة للمستخدمين المختلفين طالما كان ذلك ممكنًا.
- طالعوا [دليلينا] عن KeePassXC و KeePassDX
- إذا رغبتم في مدير لكلمات السرّ على الوِب، فطالعوا القسم التالي.

المزيد عن سبب توصيتنا هذه

ليس لأي منّا القدرة على تأليف ما يكفي من كلمات السرّ الطويلة العشوائية الفريدة لزوم حفظ أمان أجهزتنا وحساباتنا. مدير كلمات السرّ برمجية تُولِّد كلمات السرّ وتحفظها محميّةً بالتعمية.

بدورنا ننصحكم KeePassXC وKeePassDX وStrongBox ، وجميعها تطبيقات يمكن استخدامها مجّانا، وشهد خبراء متخصّصون بكونها آمنة، كما أنّ تطويرها متواصل. وهي تحفظ كلمات السرّ لكم في ملف على أجهزتكم لا يوضع على الإنترنت، ما يعني قدرتكم على التحكّم في موضع حفظ بياناتكم وكيفية إدارتها.

حفظ نسخة احتياطية من خزنة مدير كلمات السرّ

- كيفية حفظ خزنة مدير كلمات المرور KeePassXC
- كيفية حفظ خزنة مدير كلمات المرور KeePassDX
- كيفية حفظ نسخة احتياطية بواسطة خزنة مدير كلمات السّر Strongbox

تذكّروا كلمات سرّ قوية قليلة

سيكون هناك بعض كلمات المرور التي يجب حفظها، بما في ذلك كلمة المرور الرئيسة لمدير كلمات المرور الخاص بنا. هناك استراتيجيات يمكن أن تساعدنا في إنشاء كلمات مرور سهلة التذكر لكن يصعب تخمينها، حتى بالنسبة للمهرة من المتربصين بنا ممن يستخدمون برامج "اختراق كلمات المرور".

- يمكنكم باستخدام أسلوب النّرد توليد كلمات سرٍّ قوية لمدير كلمات السرِّ وكلمات السِّر الأخرى التي يتوجّب عليكم حفظها (مثل كلمة السرِّ التي تفتح خزنة مدير كلمات السِّر، أو تلِجون بها إلى أجهزتكم):
  - جهّزوا قائمة مُرقَّمة من الكلمات وقِطَع نَرد.
  - دحرجوا النَّرد خمس مرات للحصول على رقم عشوائي من خمس منازل (مثلا: 6 و 2 و 5 و 1 و 1).
  - استخرجوا الكلمات المقابلة للأرقام مما في القائمة.
  - كرّروا هذا خمس مرّات، ثم استخدموا الكلمات التي حصلتم عليها "عبارةَ سرٍّ" لحساب واحد.
    - لا تستخدموا كلمة السرِّ هذه لأي غرض آخر.
  - ثم اصنعوا صورة عقلية باستخدام هذه الكلمات لكي تساعدكم على تذّكرها
- وتدرّبوا على إدخال كلمات السرّ تلك دوريًّا، يوميًّا ابتداءً، ثم أسبوعيًّا بعد ذلك. التكرار يساعد على ترسيخ كلمات السرّ في الذهن.

كلمات السرِّ وأكواد الدخول الاحتياطيّة الواجب حفظها خارج مدير كلمات السرِّ

- إذا تعيّنت عليكم كتابة كلمات السرِّ على ورقة فيجب حفظها في مكان آمن موصد، مثل خزانة أو أدراج.
  - من المهم ألا تكون كلمة السرّ ظاهرة للعيان، وألّا يسُهلَ العثور عليها.
  - لا تحفظوا كلمات السرّ في محفظتكم أبدًا.
- أتلفوا الأوراق التي تحوي كلمات سرٍّ أو أكواد الدخول الاحتياطية فور انتفاء حاجتكم إليها.
- كما يمكن حفظ كلمات السرِّ تلك على جهاز آخر، وإخفائها بين ملاحظات أخرى بلا عنوان و لا وصف.

إذا قرّرنا استخدام مدير كلمات المرور عبر الإنترنت

- تجنّبوا حفظ كلمات السرّ شديدة الحساسية فيه (كالتي تخصّ الحسابات المالية أو مسوّغات الدخول إلى الحسابات التي تُستخدم لاسترجاع حسابات أخرى).
- تنبغي حماية خزنة مدير كلمات السرّ على الإنترنت بأسلوب التحقق بخطوتين.
- ننصحكم بتطبيق Bitwarden لإدرات لكلمات مروركم المستخدمة على الإنترنت.

تطبيقات إدارة كلمات السرّ التي تزامن تلقائيًّا الأجهزة المختلفة المتّصلة بها قد تكون أيسر في الاستخدام، فهي تحفظ كلمات السرّ في خزنة مدير مركزية معمّاة على الخادم، إلّا أن استخدامها يشكّل خطرًا إضافيًا يمكن للمهاجم استغلاله بتظهير الخزنة مدير واستخراج كلمات السرّ منها دون علمك.
بدورنا نوصي KeePassXC و KeePassDX و StrongBox لأنها لا تحفظ كلمات السرّ في أي موضع على الإنترنت. إذا فضّلت استعمال مدير كلمات سرٍّ على الإنترنت فإنّنا نوصي باتّباع الخطوات التالية لحماية كلمات سرّكم.

- تجنّبوا مشاركة كلمات السّر ما أمكنكم ذلك:
  - إذا اضطررتم إلى مشاركة كلمة سرٍّ مع آخرين فاعمدوا قبل مشاركتها إلى استبدالها بأخرى مؤقتّة، ثمّ استبدلوا تلك المؤقتة مجدّدًا بكلمة آمنة عقَب انتفاء الحاجة إلى مشاركتها.
  - تفّكروا كذلك في إنشاء حسابات منفصلة لكل شخص يلزمه النفاذ إلى المعلومات والوظائف، كثير من الخدمات تتيح ذلك، كما يمكن أحيانا تحديد الأفعال التي يمكن لتلك الحسابات فعلها، والمعلومات التي يمكنهم النفاذ إليها. طالعوا إعدادات الأمان الأساسية لأندرويد و آي. أو. إس. ولينُكس وماك و ويندوز لتفاصيل كيفية فعل ذلك.
  - يمكنكم ضبط مدير كلمات السر الذي تستخدمونه بحيث يمكن استخدامه بالتشارك بين زملاء، علما أنّ KeePassXC يتيح ذلك.

إيّاك ومشاركة كلمة السّر مع شخص راسلك عبر البريد الإلكتروني أو هاتفك أو بعث لك برسالة نصيّة

ينتحل المهاجمون هويّات أخرى، مثل موظّفي الدعم التقني في البنك، لإقناع ضحاياهم بالإفصاح عن بيانات حسّاسة. كما أنهم يتلاعبون عاطفيًّا بضحاياهم لأجل ذلك.
إذا تلقيّتم مكالمة أو رسالة بريد إلكترونياً أو رسالة قصيرة تطلب كلمة سرٍّ أو بيانات حسّاسة أخرى، أو إذا أوصلكم رابط إلى صفحة تطلب معلومات كهذه، فهي على الأرجح محاولة تصيُّد.

- افتح صفحة الخدمة أو التطبيق الذي تظنّ أنها أرسلت إليك الرسالة للتحقُّق من ذلك الطلب.
  - طالعوا أدلّتنا في شأن حماية أنفسكم وبياناتكم عند استخدام الشبكات الاجتماعية لمعرفة كيف تجدون سجلّات التنويهات التي أرسلتها الخدمة إليكم.
- إذا بدا أن الرسالة وردت من شخص ما من معارفكم أو من جهة ما تربطكم بها علاقة، فتواصلوا معهم عبر قناة اتّصال أخرى للتحقُّق من أنهم أرسلوها.
  - على سبيل المثال، إذا وصلتك الرسالة بالبريد الإلكتروني، فاطلبهم بمكالمة صوتية.
  - تجنّبوا اتّباع الروابط الواردة في رسالة البريد الإلكتروني، وكذلك إرسال ردٍّ.
- انتبهوا لمحاولات بعض الرسائل إخافتكم، أو إثارة فضولكم أو إيهامكم بوجود فرصة ستضيع ما لم تستجيبوا بسرعة. تريّثوا وفكّروا في كيفية التحقُّق من صحة الرسالة.

2.1.3| متى يجب تغيير كلمة المرور

يجب تغيير كلمة السرّ فورًا في الحالات التالية:

- إذا بدا لكم أن أحد حساباتكم أو أجهزتكم أو زملائكم والمحيطين بكم قد تعرّضوا لاختراقات
- وصلكم إخطار موثوق به من مشغِّل خدمة تستعملونها بوجود محاولة للولوج إلى الحساب من جهاز غير مصرَّح لها أو من موضع غير مُعتاد
  - ابحث في الأخبار الجارية عن أحداث اختراقات
  - إذا وصلتكم رسائل بريد أو تنويها فتحقّقوا من موقع مقدِّم الخدمة على الوِب من أنّهم أرسلوها.
- إذا ولجتم إلى أحد حساباتكم بإدخال كلمة السرّ مستخدمين جهازاً غير موثوق بها، أو مشترَكة أو عمومية (فقد تكون بها برمجيات خبيثة)
- إذا ظننتم أنَّ شخصًا كان يراقبكم وأنتم تدخلون كلمة السرِّ.

اعملوا على تقليل الضرر بتنبيه الآخرين الذين قد يكونون معرّضين للخطر.

طالعوا أدلّتنا في شأن الشبكات الاجتماعية وأساسيّات أندرويد وآي. أو. اِس، ولينُكس وماك، ووِيندوز لإرشادات بشأن كيفية تغيير كلمات سرّ الأجهزة.

بيّنت الأبحاث أن تغيير كلمات السرِّ دوريًا لا تزيد الأمان بالضرورة. فعندما يُفرض على الناس تغيير كلمات السرِّ كثيرًا فإنهم عادة ما يُجرون تغييرات طفيفة على تلك المستعملة حاليا، عوضًا عن تأليف كلمات سرٍّ مختلفة كُليًّا. طالعوا المزيد عن نتائج تلك الأبحاث.

من المهم تغيير كلمة السرِّ عند وقوع اختراق لدى مُقدِّم خدمة نستخدمها، ولأنّ أخبار الاختراقات لا تصلنا دومًا فور وقوعها فإنّنا ننصح بتغيير كلمات السرّ سنويًّا أو كلَّ بضعة أشهر، أو فور وصول أخبار بوقوع اختراق.

2.1.4| أين نحن ومن يستطيع أن يرانا

- إذا كنت في مكان عام وأردت إدخال كلمة سرّك فانتبه لما إذا كنت مُراقبًا أو يوجد من يصوِّرك.
- انتبه لوجود مَنْ يراقب لوحة مفاتيحك أو هاتفك في أثناء إدخالك كلمة السرّ.
- استخدم شاشة حافظة للخصوصية لتصعيب مراقبة ما يظهر على شاشة جهازك عند الكتابة.

2.1.5| تفعيل مصادقة الدّخول بمعاملين

من الأفضل وجود عدَّة طبقات من الحماية للولوج إلى الحسابات، فإذا اختُرِقت الأولى صّدت الثانية هجوم المخترقين. التّحقّق بعدة معاملات (MFA) أو الاستيثاق أو المصادقة بمعاملين باستخدام جهاز آخر أو رسالة بريد يوجد طبقة الحماية الإضافية هذه. الرّسائل النّصية القصيرة هي أقل تلك الوسائل أمانًا برغم استسهال الكثير من الناس لها.

قد يبدو المصادقة بمعاملين عبء زائد، لكن تذكّروا أن ما هو عبء قليل لكم هو عبء كبير على المهاجمين، وأنّ سرقة حساباتكم أو انتحال شخصياتكم أو مراقبة مراسلاتكم تشكِّل تباعته عبئا أكبر على المدى الطويل.

- طالعوا الخدمات التي تتيح وظيفة المصادقة بمعاملين.
- من المهم تفعيل وظيفة المصادقة بمعاملين لأغراض:
  - الحسابات البنكية والتطبيقات المالية
  - حسابات البريد الإلكتروني والشبكات الاجتماعية وغيرها مما يُستخدم في استرجاع التحكم في حسابات أخرى
- خيارات المصادقة بمعاملين قد تشمل:
  - استخدام تطبيق أو برنامج مصادق كـ Google Authenticator أو Okta أو Duo. نوصي باستخدام تطبيق Aegis على نظام Android أو تطبيق Raivo OTP على نظام آي. أو. إس.
  - من أمثلة تلك الأجهزة:
    - Yobikey
    - Nitrokey
    - Google Titan Key
    - Thetis Key
  - قد يتعذّر استعمال وثائق المصادقة الاعتيادية مع هاتف محمول إلا إن كان كليهما يدعمان NFC.
- يمكن استعمال تطبيق مصادقة واحد أو جهاز مصادقة واحدة لعدة خدمات، أو ضبط كل خدمة بوسيلة مختلفة للمصادقة بعاملين.
- وظيفة المصادقة بمعاملين بطريق تطبيقات TOTP أو الأجهزة الاعتيادية لا تتطلب اتّصالا بالإنترنت، أما بطريق البريد الإلكتروني فتتطلب اتصالا.
- بترتيب وسائل المصادقة بمعاملين حسب الأمان، فإن تطبيقات المصادقة والأجهزة الاعتيادية هي الأكثر أمنًا، يليها البريد الإلكتروني ثم الرسائل التلفونية القصيرة SMS. مع ملاحظة أن الرسائل القصيرة قد لا تصل في حال كونكم خارج بلد إقامتكم.
- رسائل نصية قصيرة ليست مشفّرة ويمكن للمهاجمين اعتراضها لسرقة أكواد TOP.
- بتفعيل وظيفة المصادقة بمعاملين في حساب، فسيُطلب منك عند الدخول إلى الحساب برهاناً لإثبات هويتك، إضافة إلى متطلبات الدخول المعتادة من اسم مستخدم وكلمة سرٍّ، وذلك بطريق وصل جهاز المصادقة أو بإدخال رمز من تطبيق المصادقة ، أو رمز تلقيته في رسالة.
- لا تُعطّلوا وظيفة المصادقة بمعاملين بعد تفعيلها. بعض الخدمات تتيح إيقافها مؤقتًا عند الحاجة، لكن تعطيلها نهائيًا قد تكون له تبعات على أمانكم.

احفظوا رموز الأمان الاحتياطية لوظيفة المصادقة بمعاملين معزولة وآمنة

معظم خدمات على الإنترنت ستعطيكم رموز ولوج احتياطية عند تفعيل وظيفة المصادقة بمعاملين لحساباتكم. تلك الرموز وسيلتكم للولوج إلى الحساب إذا حدث وفقدتم الجهاز الذي تستعملونه للمصادقة. تلك الأكواد لا تنتهي صلاحيتها، من المهم حفظها بحرص لأنّ كل من تقع في يديه وفي حوزته كلمة السرّ سيكون بوسعه الدخول إلى الحساب.

- إذا استلمتم رموزًا احتياطية في أثناء تفعيل وظيفة المصادقة بمعاملين فاحفظوها في مدير كلمات السرٍّ.
- ويُستحسن إنشاء خزنة مدير كلمات سرٍّ (KeePassXC) جديدة منفصلة لحفظ رموز الدخول إلى الحسابات على جهاز آخر.

2.1.6| تجنّبوا البصمات وخاصيّة التعرف على ملامح الوجه (البيومترية)

قد تُسهِّل الوسائل البيومترية الدخول إلى أجهزتكم وحساباتكم، إلا أنّها أقل أمانًا من الوسائل الأخرى، لأنّها على غير حال كلمات السرِّ لا يُمكن تغييرها. الكثيرون منّا يُجبرون على إعطاء بياناتهم البيومترية في المطارات والهيئات الحكومية وغيرها، مما يُشكِّل خطرًا بسبب احتمال استعمالها في الولوج إلى حساباتنا دون إذن منّا. كذلك، إذا تمكّن المهاجمون من تقييدكم أو إكراهكم فقد يسهل عليهم فتح أجهزتكم أكثر مما إذا استعملتم كلمات السرِّ.

- إذا كانت أجهزتكم مضبوطة بحيث تُفتح ببصمات الأصابع أو بالتعرف على ملامح الوجه فغيّروها بحيث يتطلب الفتح كلمة سرٍّ بدلا من ذلك.
- طالعوا المحور الثّاني من الفصل الثّاني: "أمان الأجهزة."

2.1.7| وضع أسئلة استرجاع آمنة

أسئلة الاسترجاع مهمّة لمساعدة الخدمات توكيد هويّاتكم في حال شكّهم في كون شخص غيركم يحاول الولوج إلى الحساب، كما تُستخدم إجابات تلك الأسئلة لأجل تغيير كلمة السّر إنْ ضاعت منكم أو نسيتموها. لكن إجابات أسئلة من قبيل "ما اسم البلدة التي وُلدتم فيها؟" أو "ما اسم حيوانكم الأليف؟" يمكن معرفتها بسهولة. لذا ينبغي وضع إجابات مُختلَقة تصعبّون على المهاجمين اختراق حساباتكم.

- ضعوا إجابات مُختلقة غير حقيقية لتلك الأسئلة
- يمكنكم كذلك وضع أكواد عشوائيّة فريدة من التي يولِّدها مدير كلمات السرِّ
- احفظوا الأسئلة وإجاباتها المُختَلقة في مدير كلمات السّر لكي لا تنسوها فتوصد حساباتكم.

2.2| أمان الأجهزة

على حين نركّز في هذا الدّليل على أمان الحواسيب والهواتف المحمولة، تجدر الإشارة لوجود أجهزة أخرى كالأجهزة اللّوحيّة، والسّاعات، والسّمّاعات الذّكية، وأجهزة التّلفزة الزّكيّة، وغيرها من أجهزة منزليّة قد يُساء استخدامها ضدّنا أو تُصمّم لجمع وحفظ بيانات حسّاسة عنّا. تُشابه الأجهزة اللّوحية الهواتف المحمولة العاملة بنظامي أندرويد أو آي.أو.إس (لذا يُمكن الرّجوع للأدلّة ذات الصِّلة أدناه)، أمّا أنظمة تشغيل سائر الأجهزة المذكورة بعديدة ومتنوعة؛ لذا لا بدّ لنا من فهم كيفيّة عملها، وما قد تنطوي عليه من تهديدات وكيفية الوقاية منها!

علينا التّيقّظ أيضًا لاحتماليّة ارتباط أو اتصال الأجهزة الذّكيّة المذكورة أعلاه بذات الحسابات المستخدمة على أجهزة أخرى، لكن قد لا يكون لدينا ذات القدرة على حمايتها على هذه الأجهزة؛ لذا قد يعتبر عزل المعلومات (حساب لكل جهاز) خيارًا جيد لتأمين حساباتنا المرتبطة بأجهزة أخرى أو البيانات المتصلّة بهذه الحسابات.

2.2.1| الحواسيب (المكتبيّة والمحمولة)

نظام تشغيل ويندوز

نجد في الرّابط التّالي دليلًا مرئيًا يطلعنا على كافّة الأدلّة أدناه:
رابط

استخدام أحدث إصدار من نظام تشغيل الجهاز

عند تحديث البرمجيات علينا التّحقّق من أنّ أجهزتنا تعمل بأحدث إصدار من نِظام تشغيلها، على أن نقوم بهذه الخطوة ونحن في مكان آمن وموثوق، مثل منازلنا أو مكاتبنا، وليس في مركز إنترنت أو مقهى.
قد يتطلب التحديث نظام التّشغيل تنزيل برمجيّات وإعادة تشغيل الجهاز عدّة مِرار؛ لذا لا بدّ لنا من تخصيص وقت لذلك—وقت لا نستخدم فيه أجهزتنا. لمقارنة أحدث نسخة من نظام التّشغيل بنسخة الحالية لدينا، علينا بالخطوات إلى أن يتوقّف الجهاز من تقديم تحديثات إضافيّة وجديدة.
في حال تعذّر تشغيل أحدث إصدار من نظام التّشغيل، فمن الأفضل التّفكير في خيار شراء جهاز جديد.
نذكر في هذا السّياق، تَعذُّر تحديث ويندوز 7 بعد كانون الثّاني/يناير 2020؛ لذا إن كنّا نستخدم ويندوز 7، لا بدّ لنا من تحديثها إلى نسخةٍ أجَد، أو النّظر في استخدام نظام تشغيل آخر مثل لينكس أو ماك.
التّثبّت من إعادة تشغيل الحاسوب بعد تنزيل التحديث، وذلك للتحقّق من تثبيت التّحديث بالكامل.
اختيار أحدث نسخة متاحة من النّظام.
مقارنة النّسخة المُحدّثة بتلك المثبّتة على جهازنا.
تحديث نظام تشغيل أجهزتنا.
تعد النّسخة 11 أحدث إصدارات ويندوز. علينا التّحقّق ما إذا كان حاسوبنا متوافقًا مع هذا التّحديث،

أو نخْتَر بدء > الإعدادات > التّحديث والأمان > تحديث ويندوز > التّحقّق من وجود تحديثات. جدير بالذّكر أنّ الوقت اللّازم لتنزيل وتثبيت ويندوز 11 يعتمد سرعة اتصالنا بالإنترنت وسرعة حاسوبنا. أمّا عمليّة التّرقية، فتتطلّب مساحةً كافيةً على حاسوبنا.

يجدر بنا ضبط ويندوز 10 أو 11 لتثبيت التّحديثات تلقائيًا، أو يُمكننا اتباع الإرشادات المدرجة هنا تحت عنوان "كيف يمكنني تحديث حاسوبي يدويًا؟" يُمكن لهذه الإرشادات مساعدتنا على تحديث أنظمة حواسبنا يدويًا كما التّأكد من عدم توقيف التّحديثات.

ملاحظة: قد نجد الكثير من التّحديثات، ما قد يتطلّب إعادة تشغيل حاسوبنا عدّة مرّات للتأكد أنّ برمجياتنا مُحدّثة بالكامل، ونكرر ذات خطوات التّحديث إلى أن يخبرنا ويندوز بأنّ برمجيات حاسوبنا محدّثة وما من تحديثات إضافيّة في الوقت الرّاهن.

تعطيل التّحكّم الصّوتي

- إيقاف تشغيل خاصّية كورتانا، المساعد الشّخصي لنظام ويندوز، وحذف سجل البحث.
- إدارة البيانات الّتي تحتفظ بها كورتانا في حساب ويندوز الخاص بنا، وذلك من خلال خاصّيات الخصوصيّة في لوحة التّحكم.
- إذا ارتأينا أنّ منافع استخدام السّمّاعات (مكبّرات الصوت) الذّكيّة (مثل أليكسا أو سيري) تفوق مخاطرها بالنّسبة لنا، يجدر بنا اتباع الإرشادات التّالية لضمان استخدام أكثر أمنًا لهذه السّمّاعات.

تعطيل خاصيّة تحديد الموقع وحذف سجل تحديد الموقع

لتحقيق تعطيل خاصيّة تحديد الموقع وحذف سجل تحديد الموقع علينا:

- اعتياد تعطيل خاصيّة تحديد الموقع كليًّا، أو في حال عدم الاستخدام، سواء لجهازنا بالكامل كما ولكل تطبيق على حدة.
- تفقد سجل الموقع ومسحه بوتيرة منتظمة، وذلك في حال لم عدم اختيارنا تعطيله أصلًا.
- الاطلاع على كيفيّة تعطيل خاصّية تحديد الموقع.

التّحقّق من أذونات التّطبيقات

علينا تدقيق كل الأذونات المنوحة للتطبيقات، تطبيقًا تطبيق، بحيث نتأكّد من أن التّطبيقات الّتي نستعملها وحدها لديها تصريح تلك الأذون؛ في هذا السّياق، علينا تعطيل الأذونات التّالية في التّطبيقات التي لا نستخدمها، واعتبار تفعيل هذه الأذونات من تطبيقات لا نعرفها موضعًا للرّيبة والشّك:

- الموقع
- جهات الاتصال
- الرّسائل النّصيّة القصيرة
- الميكروفون
- التّعرّف على الصّوت أو الكلام
- كاميرا (الويب)
- تسجيل الشّاشة
- سجلّات المكالمات أو سجل المكالمات

- الهاتف
- التّقويم
- البريد الإلكتروني
- الصّور
- الأفلام أو الفيديوهات ومجلداتهما (مكتبتاهما)
- قارئ البصمات
- الاتصالات قريبة المدى
- البلوتوث
- أي إعدادات تتطلب "الوصول إلى القرص،" أو "الملفّات،" أو "المجلّدات"، أو "النّظام،" أو بعض أو كل ما سبق
- أي إعدادات تتطلب "التّثبيت"
- خاصّيّة التّعرف على الوجه
- السّماح بتنزيل تطبيقات أخرى

من الضّروري تفقّد إعدادات تطبيقاتنا والتأكد من أن التطبيقات التي تستخدمها فقط لديها الأذونات التّالية:

- معلومات الحساب
- الحركة
- الإذاعات
- المهام

من مصادر موثوقة

تمتلك شركات آبل، وغوغل، ومايكروسوفت، وأمازون متاجر رسميّة للتطبيقات. توفر هذه المتاجر التطبيقات في مكان واحد ما يسهّل علينا العثور على التطبيقات التي نريد تثبيتها، كما يسهل على هذه الشرّكات مراقبة التّطبيقات للتثبّت من خلوّها من أي انتهاكات أمنيّة كبرى.

علينا تفقّد تحديثات التّطبيقات المتاحة بوتيرة منتظمة (مثلاً أسبوعيًا) لتثبيتها ومواكبة أحدث تحسينات الأمان المُضافة لتطبيقاتنا.

علينا تثبيت التطبيقات فقط من متاجرها الرّسميّة أو مواقع مطوّريها، إذ قد تكون مواقع التنزيل "المُقلِّدة" محل شك، إلّا إذا كنّا نعرف الجهات المزوّدة لهذه الخدمات ونثق بها. وفي حال ارتأينا أنّ منفعة تطبيق ما تفوق المخاطر المحتملة، يتعيّن علينا اتخاذ إجراءات وقائيّة إضافيّة لحمايّة أمننا، كالتّخطيط المُسبق لعدم تخزين معلومات حسّاسة أو شخصيّة على الجهاز الّذي يحوي ذلك التّطبيق، وفيما يلي جُملة من هذه الإجراءات:

- البحث في متجر مايكروسوفت عن التّطبيقات التي ثبتناها لتحقّق من قانونيّتها
- التّحقّق من أنّ برنامج مايكروسوفت المُثبّت لدينا أصلي

يُشار إلى أن مايكروسوفت لا تقدم لمستخدميها درجة حماية مماثلة كما تفعل بعض المنصّات الأخرى فيما يتعلّق بالتّحقّق من موثوقيّة البرمجيّات. لذلك، علينا تقييم الأمان بدقّة قبل تثبيت أي برنامج أو تطبيق. وفي حال عدم القدرة على التحقق بأنفسنا، يُفضل استشارة خبير تقني قبل الإقدام على التثبيت.

إزالة التّطبيقات التي لا حاجة لنا بها ولا نستخدمها

يوميًا، يتم كشف نقاط ضعف جديدة في الأكواد التي تدير أجهزتنا وتطبيقاتنا، ولا يمكن للمبرمجين التنبؤ دائمًا بأماكن هذه النقاط نظرًا لتعقيد الأكواد. يمكن للمهاجمين استغلال هذه الثغرات لاختراق أجهزتنا. لذا، يُساعد حذف التطبيقات التي لا نستخدمها في تقليص عدد التطبيقات المحتمل تعرضها للخطر. زيادة على ذلك، قد تقوم التطبيقات غير المستخدمة بنقل بيانات عنا، كموقعنا الجغرافي، قد لا نرغب في مشاركتها. إذا كان من الصعب حذف التطبيقات، يمكننا على الأقل تعطيلها.

- إلغاء تثبيت أو إزالة التطبيقات والبرامج في الإصدار العاشر من نظام تشغيل ويندوز رابط
- إلغاء تثبيت أو إزالة التّطبيقات والبرامج في الإصدار الحادي عشر من ويندوز رابط

إنشاء حسابات منفصلة على كل جهاز من أجهزتي

نشدّد على تجنّب مشاركة الأجهزة الّتي نستخدمها للقيام بأعمال حسّاسة مع أي أطراف أخرى؛ وإن اضطررنا لمشاركتها مع زملاء من العمل أو أحد أفراد أسرتنا، فيمكننا ضمان درجة أفضل من الحماية لمعلومات الحسّاسة بإعداد حسابات منفصلة على كل جهاز، بحيث إن شاركنا أحدها أجهزتنا طرف آخر فإنّ وصوله يقتصر على ذاك الجهاز فيما تبقى ملفّاتنا الحسّاسة المرتبطة بحاسبتنا على الأجهزة الأخرى في مأمن ومنأى عن الاختراق.

من المهم النظر في إنشاء حساب محلي على الأجهزة لزيادة الأمان، حيث يكون هذا الحساب مستقلاً وغير متصل بشبكة الإنترنت. تجدر الإشارة إلى أن اختيار حساب محلي بدلاً من حساب مايكروسوفت يحد من إمكانية المزامنة ومشاركة البيانات بسهولة بين الأجهزة المختلفة المرتبطة بنفس حساب مايكروسوفت.

يُعد إنشاء عدة حسابات على الجهاز الواحد استراتيجية فعالة لتعزيز الأمان. يُمكن تخصيص أحد هذه الحسابات بصلاحيات "المدير." أما باقي الحسابات، فيُفضل منحها صلاحيات "عادية" أو "غير إداريّة."

- يجب ألّا يكون لأحد سوانا إذن الوصول إلى حساب المدير.
- ينبغي ألّا نُصرّح للحسابات العادية بالوصول إلى كافّة التّطبيقات، أو الملفّات، أو الإعدادات على أجهزتنا.
- يجدر بنا استخدام حساب عادي لإنجاز أعمالنا اليوميّة:
- ينبغي لنا ألّا نستخدم حساب المدير إلّا عن الحاجة لإجراء تغييرات تؤثّر على أمن أجهزتنا، مثل تثبيت برمجيّات معيّنة.
- يعتبر استخدام حساب عادي للأنشطة اليوميّة خطوة جيدة للحماية من التّهديدات الأمنية، خاصة تلك التي تنجم عن البرمجيات الخبيثة؛ فالحسابات العادية تحدّ من الصلاحيات، وبالتّالي يصعب على البرمجيات الخبيثة إحداث تغييرات كبيرة في النظام.
- خلال السّفر عبر الحدود، قد تكون فكرة إنشاء حساب "للسفر" خطوة مفيدة ذكية لإخفاء معلوماتنا أكثر حساسية يقلل من المخاطر في حالة تفتيش الأجهزة من قبل السلطات الحدودية. يعتمد قرار استخدام حساب السفر على تقييم المخاطر والتوقعات بشأن مستوى التدقيق الذي قد يتعرض له الجهاز. في الحالات التي لا يُتوقع فيها تمحيص الجهاز، يمكن استخدام حساب عادي للأعمال غير الحسّاسة، ما يوفر درجة من الحماية وإمكانية الإنكار المبرر.

إضافة حسابات المستخدمين ضمن الإصدار العاشر من نظام تشغيل ويندوز: رابط
إضافة حسابات المستخدمين ضمن الإصدار الحادي عشر من نظام تشغيل ويندوز: رابط

إزالة الحسابات غير الضّروريّة من على أجهزتنا

من الضّروري تقليص فرص الوصول غير المصرح به إلى أجهزتنا، أي غير تلك الّتي صرّحنا بها؛ لتحقيق ذلك لا بدّ ألّا نترك ذلك "الباب،" إن جاز التّعبير مفتوحًا (تُعرف هذه العمليّة بتقليص سطح انكشاف أجهزتنا للهجمات والاعتداءات). يُضاف لذلك التّفقّد الدّوري للحسابات المسجلة على أجهزتنا، لضمان عدم وجود حسابات مجهولةٍ لنا.
إزالة حسابات المستخدمين ضمن الإصدار العاشر من نظام تشغيل ويندوز: رابط
إزالة حسابات المستخدمين ضمن الإصدار الحادي عشر من نظام تشغيل ويندوز: رابط

الحفاظ على أمن الحسابات المرتبطة بأجهزتنا

ترتبط معظم الأجهزة الإلكترونيّة بحسابات خاصة مثل حسابات غوغل لأجهزة الأندرويد، والهواتف المحمولة من نوع كروم، وتلفاز غوغل، وكذلك حسابات آبل المستخدمة للأجهزة اللّوحيّة مثل الآي-باد، وساعات آبل، وأجهزة ماك المحمولة، وتلفاز آبل. قد يُسجَّل الدخول لنفس الحساب على أجهزة متعددة في ذات الوقت، مثل الهاتف، والحاسوب المحمول والتلفاز. وعليه إذا تمكّن شخص آخر من الوصول دون تصريح إلى حسابتنا، فإنّ هذا المكان يمكّننا من كشف ذلك واتخاذ الإجراءات اللازمة لإيقاف هذا الوصول.

- عند رصد نشاط مشبوه على حسابنا، مثل تسجيل الدخول من أجهزة لم تعد بحوزتنا أو لا نعرفها، يُمكننا توثيق ذلك بالتقاط صورة أو لقطة شاشة لتلك الصفحات.
- ينبغي لنا مراجعة الإعدادات الأمنية في حسابات وسائل التواصل الاجتماعي للتأكد من تحمي بياناتنا ونشاطنا بالقدر الكافي.
- للحصول على معلومات مفصلة عن كيفية الحفاظ على أمن الحسابات المرتبطة بأجهزتنا، يمكن الرجوع إلى المادة المتاحة في الرابط.

ضبط إعدادات قفل الشّاشة ووضعيّة السّكون

قد يبدو الهجوم التقني أكبر همّنا، بيد أنّ المحتمل أكثر هو مصادرة أجهزتنا أو سرقتها واختراقها طرف أو أطراف ما؛ لذا يجدر بنا قفل شاشات أجهزتنا بكلمة مرور تحول دون ولوج أحد إلى أجهزتنا بمجرّد تشغيلها. يفضّل استخدام خيار كلمات أو رمز المرور لقف الشّاشة وتجنب خيارات القفل الأخرى، فقد نُجبر في حال اعتقالنا أو تفتيشنا لفتح جهازنا بخاصيّة التّعرف على الوجه، أو بصمات الصّوت، أو الأصابع، أو العين، في حال كنّا قد اخترنا إحدى طرق القفل هذه.
في ذات السياق، ثمَّ مخاطر تتعلق بوسائل القفل المختلفة، مثلًا برامج تخمين كلمات المرور يمكنها اختراق الرّموز القصيرة أو الأرقام السرية السّهلة. كذلك الأمر بالنّسبة لإقفال الأنماط، يمكن تخمينها بتقصي آثار الأصابع على شاشة الجهاز. وفي حال استخدام قفل بصمة الإصبع، يمكن جمع بصمات صاحب/ة الجهاز وصنع نسخة مزيفة عن البصمة لفتح الجهاز. كما أن تقنيات الفتح بالوجه ليست محصنة بالمطلق، حيث طُوِّرت طرق لخداع هذه الأنظمة.
في ضوء كل ذلك، تبقى عِبَارات المرور الطّويلة أكثر أنواع الأقفال أمانًا، وفيما يلي عِدّة من نصائح أُخَر:

- ينبغي ضبط الشّاشة لتقفل بُعيد فترة قصيرة من التّوقّف عن استخدامها (5 دقائق فترة جيدة).
- علينا استخدام عبارة مرور طويلة، تزيد على 16 حرفًا، وعدم الاكتفاء بكلمة مرور قصيرة أو رقم سري.
- يُمكن لخاصّيّات فتح الجهاز ببصمات الأصابع، أو العين، أو الوجه، أو الصوت أن تُستخدم ضدنا بإرغامنا على فتح أجهزتنا؛ لذا علينا ألّا نستخدم هذه الخيارات إلّا إذا كان لدينا إعاقة ما تحول دون اللجوء لخيار كتابة عبارات المرور الطّولية.
  - علينا أيضًا إزالة بصماتنا أو مُدخلات التّعرّف على وجهنا من جهازنا إن سبق لنا إدخال أي منهما أو كلاهما.
- في المقابل علينا إنشاء كلمة مرور لحماية حسابنا وفقًا لهذه الإرشادات.
- يجب ألّا ننسى تفعيل متطلب تسجيل الدخول وضبط وقت القفل، وتعطيل تسجيل الدّخول التّلقائي:
- كذلك التأكد من تعطيل تقنيّة Hello وHello Face.
- أيضًا، لا بدّ لنا من اعتياد الضّغط على شعار ويندوز وحرف الـا (أو مِيم بالعربيّة) لقفل الشّاشة قُبيل الابتعاد عن جهازنا.

التّحكّم فيما يمكن رؤيته عندما يكون الجهاز مُقفلًا

- وقف ظهور الإشعارات عند قفل الجهاز: إنّ وضع قفل شاشة متين لا يحصّننا من كافّة المخاطر. مثلًا إن تركنا تطبيقاتنا تظهر على الشّاشة خلال الإقفال، فإن ذلك يتيح لمن قد يضعون يدهم على جهازنا من معاينة المعلومات الحسّاسة الّتي قد تظهر في الإشاعات، سواء كانت رسائل، أو جهات اتصال، أو بريد إلكتروني وارد. لذا، من الضروري إيقاف ظهور الإشعارات على شاشة القفل لمنع تسرب مثل هذه المعلومات.

استخدم الحوائل الماديّة لمنع الغير من رؤية شاشة أجهزتنا

عند التفكير في الهجمات على الأمان الرقمي، غالبًا ما أنّها محصورة بعمليّات معقدة تقنيًا، المفاجأة أنّ بعض عمليات اختراق معلومات المدافعين/ات عن حقوق الإنسان تمّت من خلال استراق النّظر على شاشات أجهزتهم أو استخدام كاميرات المراقبة. لذا فإن استخدام الحوائل الماديّة لحماية خصوصيّتنا تقلل من احتمال تعرّضنا لمثل هذه المحاولات. يمكن العثور على حوائل الخصوصية المادّية في متاجر ملحقات الأجهزة الإلكترونيّة.
للمزيد من المعلومات عن أدوات حماية الخصوصيّة لشاشات الأجهزة يُمكن الاطلاع على الرّابط

استخدام غطاء الكاميرا

قد تتمكن بعض البرمجيات الخبيثة من تفعيل كاميرا الأجهزة سرًا لتصوير المستخدمين ومحيطهم أو أماكن عملهم دون علمهم.

- أولًا، من المهم تحديد مواقع الكاميرات الموجودة في الأجهزة التي نستخدمها. قد يكون لدينا أكثر من كاميرا واحدة في الجهاز نفسه، ويجب أيضًا أخذ الكاميرات الخارجية في الاعتبار إذا كنا نستخدمها بالإضافة إلى الكاميرا المدمجة.
- لحماية الخصوصية، يمكن استخدام ضمادات الجروح الصغيرة اللاصقة كغطاء بسيط وفعّال لكاميرا الجهاز. هذه الضمادات مفيدة لأن الجزء الأوسط منها خالٍ من اللاصق، مما يمنع ترك

آثار لاصقة على عدسة الكاميرا. ويمكن إزالة الضمادة عند الحاجة إلى استخدام الكاميرا.
- يمكننا أيضًا البحث في متاجر بيع ملحقات الأجهزة الإلكترونية عن غطاء كاميرا الويب الرقيق والقابل للسحب. من الضروري اختيار غطاء رقيق لأن بعض الأغطية السميكة قد تمنع إغلاق الحاسوب المحمول بشكل صحيح.

إيقاف نقاط الاتصال التي لا نستخدمها

تتيح شبكة الواي فاي لأجهزتنا الاتصال بالإنترنت عبر الموجات الراديوية والموجهات، التي تربطنا بدورها بالشبكة العنكبوتيّة الأوسع عن طريق اتصال سلكي. توفر شبكات الهاتف المحمول الاتصال بالأجهزة الأخرى في مختلف أرجاء العالم من خلال شبكة من الأبراج ومكررات إشارات الاتصال. كما يُمكن للاتصالات قصيرة المدى والبلوتوث ربط أجهزتنا بأجهزة أخرى قريبة باستخدام الموجات الراديوية. هذه الاتصالات مهمة للتواصل، لكنها قد تشكل خطراً إذا استغلها شخص ما للوصول إلى أجهزتنا وما عليها من معلومات حساسة.

لذا، ينبغي لنا إيقاف تشغيل شبكات الاتصال مثل الواي فاي والبلوتوث عندما لا نحتاج إليها؛ فهذا يقلل من فرص وصول المخترقين إلى بياناتنا الحسّاسة دون علمنا. أحيانًا قد لا نلاحظ التغييرات الغريبة في سلوك جهازنا، مثل تباطؤ أدائه أو ارتفاع درجة حرارته دون استخدام مكثف. وعليه ينبغي لنا:
- إيقاف تشغيل أجهزتنا بالكامل ليلاً.
- الاعتياد على إيقاف شبكة الواي فاي، والبلوتوث، و/أو مشاركة الشبكة في حال عدم استخدامنا لها.
- تفعيل وضع الطيران وإيقاف شبكة الواي فاي| رابط
- ضبط إعدادات الشّبكة على أنّها خاصّة عند الاتصال بشبكةٍ في مكانٍ نثق به (مثل المنزل أو المكتب)، وضبطها على إعدادات الشّبكات "العامّة" عند الاتصال بالإنترنت عبر الشّبكات العامّة (مثل شبكات الاتصال المتاحة في المقاهي، ومراكز الإنترنت، إلخ.)| رابط
- التّثبّت من إيقاف شبكة البلوتوث| رابط
- التّأكد من أن جهازنا لا يوفّر نقطة اتصال إنترنت لجهاز شخص آخر باستخدام خاصيّة نقطة الاتصال النّقّالة؛ لا بدّ لنا من تعطيل هذه الخاصيّة من خلال الإعدادات| رابط

إيقاف نقاط المشاركة الّتي لا نستخدمها

تقدم الأجهزة الحديثة خيار مشاركة الملفات أو الخدمات مع الآخرين بسهولة، وهي ميزة مفيدة جدًا، لكن إذا تُركت هذه الميزة مشرّعة دون استخدام، قد تصبح فرصة للمتربصين للتسلّل إلى الملفات الموجودة على أجهزتنا. لمنع ذلك، من الضّروري:
- إيقاف مشاركة الملفّات والمجلّدات على خدمة التّخزين السّحابي ون-درايف OneDrive| رابط
- إيقاف مشاركة الملفّات عبر شبكة ضمن نظام تشغيل ويندوز| رابط
- إيقاف مشاركة الأشياء مع الأجهزة القريبة ضمن نظام تشغيل ويندوز| رابط

إيقاف خاصيّة التّشغيل التّلقائي

قد تؤدّي ميزة التّشغيل التّلقائي في ويندوز بتفعيل الأكواد الضّارة تلقائيًا من قرّص أو محرّك ندخله

إلى أجهزتنا أو نُوصله به؛ لذا فإن إيقاف هذه الميزة يحمينا من هذه المخاطر؛ لتحقيق ذلك، ينبغي لنا:
- العثور على إعدادات التّشغيل التّلقائي وإيقافها| رابط

إيقاف الإعلانات وخيارات الخصوصيّة الأخرى
مشاركة بيانات إضافية من أجهزتنا تعني توفر المزيد من المعلومات عنّا للجمهور؛ لذا، فإنّ تقييد هذه المشاركة يُعد إجراءً إضافيًا مهمًا لحماية خصوصيتنا وأماننا؛ لذا لا بدّ لنا من:
- مراجعة خيارات الخصوصيّة (الإعدادات > الخصوصيّة) وإيقاف الإعدادات التي لم تُغَطَّى في أجزاء أخرى من هذه القائمة التّدقيقيّة.
- وتفعيل خاصيّة السمارت سكرين (SmartScreen)، الّتي يُمكنها منع البرمجيات الضّارة من النّزول على أجهزتنا.

استخدام جدار الحماية
تساعدنا جدران الحماية (Firewalls) على حماية أجهزتنا من البرمجيات غير المتوقعة التي قد تسترق السّمع على معلوماتنا أو تحاول الوصول إليها. تُعد هذه الأدوات بمثابة حارس الّذي يبقى عند باب البيت المفتوح، سواء أكان هذا الباب مفتوحًا بالخطأ أو فتحه المتربصين داخل المبنى. جدران الحماية التي تتابع الاتصالات الصادرة يمكنها أحيانًا تنبيهنا إذا حاولت برمجيات خبيثة سرقة البيانات أو التواصل مع مصادر خارجية لتلقي تعليمات. عند تثبيت جدار حماية خاص لتقييد الاتصالات الصادرة أو تكوين جدار الحماية المدمج لأداء هذه المهمة، يجب أن نكون مستعدين لبذل الوقت اللازم لتدريبه عليها إلى أن يصل لتنبيهنا فقط عند ملاحظة أنشطة غير اعتيادية.
كيفيّة تفعيل جدار الحماية على جهازنا: رابط

نظام تشغيل أو. اِس لحواسيب ماك (MacOS)
إذا كنّا نستخدم حاسوب ماك، قد نكون سمعنا أسطورة أن أجهزة ماك أكثر أمانًا؛ إلّا أن هذه الأسطورة ليست بالضرورة صحيحة. يعتمد الأمان على مزيج من كيفية استخدامنا لأجهزتنا، وبرمجياتها الخاصة، التي يمكن اكتشاف نقاط الضعف فيها في أي وقت. فيما يلي جُملة من الخطوات الّتي يُمكنها مساعدتنا على زيادة أمان أجهزة الماك خاصّتنا:
لا بد لنا من اعتياد التحقق من هذه الإعدادات من وقت لآخر، للتأكد من أن لا شيء قد تغير.

نجد في الرّابط التّالي دليلًا مرئيًا يطلعنا على كافّة الأدلّة: رابط

استخدم أحدث نسخة من نظام أو. اِس المُشغِّل لأجهزتنا
مع كل صباح، تُكتشف نقاط ضعف وثغرات في الأكواد المشغّلة لأجهزتنا وتطبيقاتنا؛ لذا من المُحال لمطوّري هذه الأكواد التّنبؤ أي سيُعثر عليها نظرًا للطبيعة المعقّدة للأكواد؛ أمّا المتربّصون، فقد يستغلون هذه نقاط الضّعف هذه لاختراق أجهزتنا.
وفي ضوء ما يُكتشف من نقاط ضعف، يعمل المطورون على إصدار تحديثات تُعالج هذه الثّغرات؛ لذا، لا بدّ لنا من تثبيت التّحديثات واستخدام أحدث نسخة من نظام التشغيل لكل جهاز نستعمله؛ من المفيد أيضًا ضبط أجهزتنا على تحديث أنظمتها تلقائيًا لتخفف عنّا هذه المهمة.

- لنحرص تحديث البرمجيات ونحن في مكانٍ موثوق مثل المنزل أو المكتب—ليس مراكز الإنترنت أو المقاهي على سبيل المثال.
- قد يتطلب تحديث أنظمة تشغيل أجهزتنا لأحدث إصداراتها تنزيل برمجيات وإعادة تشغيل الأجهزة مرات عدة؛ لذا، سنحتاج إلى استقطاع بعض الوقت لذلك، وقت لا نكون بحاجة فيه للعمل على الجهاز المُراد تحديث نظامه. لمقارنة أحدث إصدار من نظام تشغيل جهازنا والإصدار المثبت حاليًا لدينا، ينبغي لنا تتبع الخطوات أدناه، هكذا إلى أن يكف الجهاز عن إظهار الحاجة لأي تحديثات إضافية.
- في حال تعذّر تشغيل أحدث نسخة من نظام التّشغيل، فمن الأفضل التّفكير في خيار شراء جهاز جديد.
- التأكد من إعادة تشغيل الحاسوب بعد تنزيل التحديث، وذلك للتحقّق من تثبيت التّحديث بالكامل.
- البحث عن أحدث إصدار متاح من النّظام: رابط
  - مقارنة النّسخة المُحدّثة بتلك المثبّتة على جهازنا: رابط
  - تحديث نظام تشغيل أجهزتنا: رابط
  - ضبط جهازنا ليُحدّث نظام تشغيله تلقائيًا: رابط

ملاحظات:

- قد تتصرّف حواسبنا بغرابة إن أرغمناها على تثبيت إصدار من نظام التشغيل لا يمكنه تشغيله: رابط
- يقدّم الرّابط التّالي معلومات عن كيفيّة تحديث الإصدارات القديمة من أنظمة تشغيل أو. اِس لحواسيب ماك: رابط

استخدام التطبيقات وتحديثها من مصادر موثوقة

تمتلك شركات آبل، وغوغل، ومايكروسوفت، وأمازون متاجر رسميّة للتطبيقات. توفر هذه المتاجر التطبيقات في مكان واحد ما يسهّل علينا العثور على التطبيقات التي نريد تثبيتها، كما يسهل على هذه الشرّكات مراقبة التّطبيقات للتثبّت من خلوّها من أي انتهاكات أمنيّة كبرى.

علينا تفقّد تحديثات التّطبيقات المتاحة بوتيرة منتظمة (مثلاً أسبوعيًا) لتثبيتها ومواكبة أحدث تحسينات الأمان المُضافة لتطبيقاتنا.

علينا تثبيت التطبيقات فقط من متاجرها الرّسميّة أو مواقع مطوّريها، إذ قد تكون مواقع التنزيل "المُقلِّدة" محل شك، إلّا إذا كنّا نعرف الجهات المزوّدة لهذه الخدمات ونثق بها. وفي حال ارتأينا أنّ منفعة تطبيق ما تفوق المخاطر المحتملة، يتعيّن علينا اتخاذ إجراءات وقائيّة إضافيّة لحمايّة أمننا، كالتّخطيط المُسبق لعدم تخزين معلومات حسّاسة أو شخصيّة على الجهاز الّذي يحوي ذلك التّطبيق، وفيما يلي جُملة من هذه الإجراءات:

- العثور على متجر التطبيقات: رابط
- تعطيل "التثبيت من مصادر غير معروفة": رابط
- خطوة متقدّمة: التّثبّت من أصالة التحديثات: رابط

إزالة التّطبيقات التي لا حاجة لنا بها ولا نستخدمها

يوميًا، يتم كشف نقاط ضعف جديدة في الأكواد التي تدير أجهزتنا وتطبيقاتنا، ولا يمكن للمبرمجين التنبؤ دائمًا بأماكن هذه النقاط نظرًا لتعقيد الأكواد. يمكن للمهاجمين استغلال هذه الثغرات لاختراق أجهزتنا. لذا، يُساعد حذف التطبيقات التي لا نستخدمها في تقليص عدد التطبيقات المحتمل تعرضها للخطر. بالإضافة إلى ذلك، قد تقوم التطبيقات غير المستخدمة بنقل بيانات عنا، كموقعنا الجغرافي، قد لا نرغب في مشاركتها. إذا كان من الصعب حذف التطبيقات، يمكننا على الأقل تعطيلها.

لحذف التّطبيقات، يُمكننا اتباع الخطوات الواردة في هذا الرّابط: رابط

ملحوظة: من الصعب بل والخَطِر قليلًا إلغاء تثبيت العديد من التّطبيقات المُثبّتة مسبقًا على أجهزة الماك خاصّتنا، مثل Safari أو iTunes.

التّحقّق من أذونات التّطبيقات

يمكن للتطبيقات الّتي تصل إلى تفاصيل رقميّة حسّاسة أو الخصائص الموجودة على أجهزتنا—نحو تحديد الموقع، والميكروفون، والكاميرا، أو الإعدادات—أن تسرّب ما تصل إليه من معلومات كما قد تُضحي مداخل يستغلها المتربّصون؛ وعليه، في حال انتفاء حاجتنا لتطبيق أو خدمة ما، حري بنا الإحجام عن منحها مثل هذه الأذونات. كما علينا:

- مراجعة جميع أذونات الوصول واحدًا تلو الآخر، علمًا أنّ الأذونات أدناه تُعد الأكثر شُبهة نظرًا لشيوع استغلال التّطبيقات الضّارّة لها:
  - الموقع
  - الصور
  - جهات الاتصال
  - التقويم
  - الميكروفون
  - الكاميرا التحكم في المعلومات الشخصية التي تشاركها مع التطبيقات
  - سجلات الاستخدام.
- مراجعة الموضوعات المتناولة تحت عنوان "التحكم في المعلومات الشخصية التي تشاركها مع الأصدقاء: رابط

إيقاف خدمات الموقع ومسح السّجل

إذا كانت أجهزتنا تحتفظ بإحداثيّات أماكن وجودنا، فإنّه من الممكن تتبّع مواقعنا باستخدام نظام التّموضع العالمي، أو أبراج الهاتف المحمول، أو شبكات الواي-فاي الّتي نستخدمها، كما يمكن تحديد موقعنا أو استخدام هذا السّجل لإثبات وجودنا في أماكن معيّنة أو ارتباطنا بأشخاص محدّدين، وعليه ينبغي لنا:

- اعتياد تعطيل خاصيّة تحديد الموقع كليًّا، أو في حال عدم الاستخدام، سواء لجهازنا بالكامل كما ولكل تطبيق على حدة.
- تفقد سجل الموقع ومسحه بوتيرة منتظمة، وذلك في حال لم عدم اختيارنا تعطيله أصلًا.
- إيقاف خدمات الموقع لتطبيقات محددة: رابط
- لتعطيل تتبع الموقع وسجل التّتبع في تطبيق الخرائط إن كُنّا نستخدمه: رابط

إنشاء حسابات منفصلة على كل جهاز

نشدّد على تجنّب مشاركة الأجهزة الّتي نستخدمها للقيام بأعمال حسّاسة مع أي أطراف أخرى؛ وإن اضطررنا لمشاركتها مع زملاء من العمل أو أحد أفراد أسرتنا، فيمكننا ضمان درجة أفضل من الحماية لمعلومات الحسّاسة بإعداد حسابات منفصلة على كل جهاز، بحيث إن شاركنا أحدها أجهزتنا طرف آخر فإنّ وصوله يقتصر على ذاك الجهاز فيما تبقى ملفّاتنا الحسّاسة المرتبطة بحاسبتنا على الأجهزة الأخرى في مأمن ومنأى الاختراق.

- يُعد إنشاء عدة حسابات على الجهاز الواحد استراتيجية فعالة لتعزيز الأمان. يُمكن تخصيص أحد هذه الحسابات بصلاحيات "المدير." أما باقي الحسابات، فيُفضل منحها صلاحيات "عادية" أو "غير إداريّة."
  - يجب ألّا يكون لأحد سوانا إذن الوصول إلى حساب المدير.
  - ينبغي ألّا نُصرّح للحسابات العادية بالوصول إلى كافّة التّطبيقات، أو الملفّات، أو الإعدادات على أجهزتنا.
- يجدر بنا استخدام حساب عادي لإنجاز أعمالنا اليوميّة:
  - ينبغي لنا ألّا نستخدم حساب المدير إلّا عن الحاجة لإجراء تغييرات تؤثّر على أمن أجهزتنا، مثل تثبيت برمجيّات معيّنة.
  - يعتبر استخدام حساب عادي للأنشطة اليوميّة خطوة جيدة للحماية من التّهديدات الأمنية، خاصة تلك التي تنجم عن البرمجيات الخبيثة؛ فالحسابات العادية تحدّ من الصلاحيات، وبالتّالي يصعب على البرمجيات الخبيثة إحداث تغييرات كبيرة في النظام.
  - خلال السّفر عبر الحدود، قد تكون فكرة إنشاء حساب "للسفر" خطوة مفيدة ذكية لإخفاء معلوماتنا أكثر حساسيّة يقلّل من المخاطر في حالة تفتيش الأجهزة من قبل السلطات الحدودية. يعتمد قرار استخدام حساب السفر على تقييم المخاطر والتوقعات بشأن مستوى التدقيق الذي قد يتعرض له الجهاز. في الحالات التي لا يُتوقع فيها تمحيص الجهاز، يمكن استخدام حساب عادي للأعمال غير الحسّاسة، ما يوفر درجة من الحماية وإمكانية الإنكار المبرر.
  - لمعرفة كيفية إعداد حسابات جديدة، يُمكن الاطلاع على المادّة في الرّابط التّالي: رابط

الحفاظ على أمن الحسابات المرتبطة بأجهزتنا

ترتبط معظم الأجهزة الإلكترونيّة بحسابات خاصة مثل حسابات غوغل لأجهزة الأندرويد، والهواتف المحمولة من نوع كروم، وتلفاز غوغل، وكذلك حسابات آبل المستخدمة للأجهزة اللّوحيّة مثل الآي-باد، وساعات آبل، وأجهزة ماك المحمولة، وتلفاز آبل. قد يُسجَّل الدخول لنفس الحساب على أجهزة متعددة في ذات الوقت، مثل الهاتف، والحاسوب المحمول والتلفاز. وعليه إذا تمكّن شخص آخر من الوصول دون تصريح إلى حسابتنا، فإنّ هذا المكان يمكّننا من كشف ذلك واتخاذ الإجراءات اللازمة لإيقاف هذا الوصول.

- عند رصد نشاط مشبوه على حسابنا، مثل تسجيل الدخول من أجهزة لم تعد بحوزتنا أو لا نعرفها، يُمكننا توثيق ذلك بالتقاط صورة أو لقطة شاشة لتلك الصفحات.
- مراجعة قائمة أجهزة Apple ID لمعرفة الأجهزة المسجّل دخولنا إليها: رابط
- مراجعة حسابات iCloud الخاصة بنا: رابط

إزالة حسابات الأجهزة الّتي لا حاجة لنا بها

من الضّروري تقليص فرص الوصول غير المصرح به إلى أجهزتنا، أي غير تلك الّتي صرّحنا بها؛ لتحقيق ذلك لا بدّ ألّا نترك ذلك "الباب،" إن جاز التّعبير مفتوحًا (تُعرف هذه العمليّة بتقليص سطح انكشاف أجهزتنا للهجمات والاعتداءات). يُضاف لذلك التّفقّد الدّوري للحسابات المسجلة على أجهزتنا، لضمان عدم إدخال حسابات على أجهزتنا دون علمنا.

إزالة حسابات الأجهزة غير المرغوبة: رابط

ضبط إعدادات قفل الشّاشة ووضعيّة السّكون

قد يبدو الهجوم التقني أكبر همّنا، بيد أنّ المحتمل أكثر هو مصادرة أجهزتنا أو سرقتها واختراقها طرف أو أطراف ما؛ لذا يجدر بنا قفل شاشات أجهزتنا بكلمة مرور تحول دون ولوج أحد إلى أجهزتنا بمجرّد تشغيلها. يفضّل استخدام خيار كلمات أو رمز المرور لقف الشّاشة وتجنب خيارات القفل الأخرى، فقد نُجبر في حال اعتقالنا أو تفتيشنا لفتح جهازنا بخاصيّة التّعرف على الوجه، أو بصمات الصّوت، أو الأصابع، أو العين، في حال كنّا قد اخترنا إحدى طرق القفل هذه.

في ذات السياق، ثمَّ مخاطر تتعلق بوسائل القفل المختلفة، مثلًا برامج تخمين كلمات المرور يمكنها اختراق الرّموز القصيرة أو الأرقام السرية السّهلة. كذلك الأمر بالنّسبة لإقفال الأنماط، يمكن تخمينها بتقصي آثار الأصابع على شاشة الجهاز. وفي حال استخدام قفل بصمة الإصبع، يمكن جمع بصمات صاحب/ة الجهاز وصنع نسخة مزيفة عن البصمة لفتح الجهاز. كما أن تقنيات الفتح بالوجه ليست محصنة بالمطلق، حيث طُوِّرت طرق لخداع هذه الأنظمة.

في ضوء كل ذلك، تبقى عِبَارات المرور الطّويلة أكثر أنواع الأقفال أمانًا، وفيما يلي عِدّة من نصائح أُخَر:

- ينبغي ضبط الشّاشة لتقفل بُعيد فترة قصيرة من التّوقّف عن استخدامها (5 دقائق فترة جيدة).
- علينا استخدام عبارة مرور طويلة، تزيد على 16 حرفًا، وعدم الاكتفاء بكلمة مرور قصيرة أو رقم سري.
- يُمكن لخاصّيّات فتح الجهاز ببصمات الأصابع، أو العين، أو الوجه، أو الصوت أن تُستخدم ضدنا بإرغامنا على فتح أجهزتنا؛ لذا علينا ألّا نستخدم هذه الخيارات إلّا إذا كان لدينا إعاقة ما تحول دون اللجوء لخيار كتابة عبارات المرور الطّولية.
    - علينا أيضًا إزالة بصماتنا أو مُدخلات التّعرّف على وجهنا من جهازنا إن سبق لنا إدخال أي منهما أو كلاهما.
- يجب ألّا ننسى تفعيل متطلّب كلمة المرور لتسجيل الدّخول وضبط وقت القفل، وتعطيل تسجيل الدّخول التّلقائي: رابط
    - (إذا قمنا بذلك من قبل، قد نحتاج للنقر على القفل في الأسفل وإدخال عبارة مرور جهازنا لتغيير الإعدادات).

التّحكّم فيما يمكن رؤيته عندما يكون الجهاز مُقفلًا

وقف ظهور الإشعارات عند قفل الجهاز: إنّ وضع قفل شاشة متين لا يحصّننا من كافّة المخاطر. مثلًا إن تركنا تطبيقاتنا تظهر على الشّاشة خلال الإقفال، فإن ذلك يتيح لمن قد يضعون يدهم على جهازنا من معاينة المعلومات الحسّاسة الّتي قد تظهر في الإشاعات، سواء كانت رسائل، أو جهات اتصال، أو بريد إلكتروني وارد. لذا، من الضروري إيقاف ظهور الإشعارات على شاشة القفل لمنع تسرب مثل هذه المعلومات. ثمَّ طريقتان للقيام بذلك من خلال:

- اتباع التّعليمات الواردة في الرّابط التّالي بشأن الإشعارات واستخدام ميزة وضع عدم الإزعاج: رابط اختيار إيقاف عرض الإشعارات "في وضع السّكون،" وعند "إقفال الشّاشة،" "وعند العرض على التلفاز أو بواسطة أجهزة العرض".
- إن كان جهازنا قديمًا ولا يحتوي على خاصيّة عدم الإزعاج، يُمكننا اتباع تعليمات "إيقاف الإشعارات" لكل تطبيق في القائمة، ولا بد ألّا ننسى إيقاف إظهار إشعارات كافّة التطبيقات على شاشة القفل، كما يمكننا التّفكير بخيار إيقاف الإشعارات بالكامل بدلاً من ذلك.

تعطيل التّحكم الصّوتي

عندما نضبط أجهزتنا لتقبل الأوامر الصوتية من خلال خدمات مثل سيري، كورتانا، غوغل فويس، إيكو، أو أليكسا، فهذا يعني أن الجهاز يظل في وضع الاستماع طوال الوقت. قد يؤدي ذلك إلى تسجيل بعض المحادثات وإرسالها إلى شركات مثل أمازون أو مايكروسوفت لأغراض مراقبة الجودة، حيث يُحْتَفَظ بهذه التسجيلات ومراجعتها من طرف جهات متعاقدة مع هذه الشّركات. كما يوجد احتمال لتثبيت أكواد ضارة على الأجهزة تُمكّن من التقاط كل ما يُسمع، مما يشكل خطرًا على خصوصيّتنا وخصوصيّة من حولنا.

إذا كان لدينا إعاقة تجعل من الصّعب الكتابة أو استخدام عناصر التّحكم اليدويّة، فإنّ استخدام خواص التحكم الصوتي قد يكون ضروريًا. يمكن اتباع بعض الإرشادات لضمان استخدام أكثر أمانًا لهذه الخاصية. ومع ذلك، إذا لم تكن هناك حاجة لاستخدام التحكم الصوتي لهذا السبب، فمن الأفضل تعطيل هذه الخاصية لتعزيز الأمان.

إذا ارتأينا أنّ منافع استخدام السّمّاعات (مكبّرات الصوت) الذّكيّة (مثل أليكسا أو سيري) تفوق مخاطرها بالنّسبة لنا، يجدر بنا اتباع الإرشادات التّالية لضمان استخدام أكثر أمنًا لهذه السّمّاعات: رابط.

- اتباع هذه الإرشادات في الرّابط التّالي للوصول إلى إعدادات خاصّية سيري والتّحكّم: رابط
- تعطيل خيار "اسأل سيري".
- حذف سجل تاريخ سيري والإملاء من خادم آبل باتباع التّوجيهات المدرجة فيما يتعلّق "سجل تاريخ Siri والإملاء:" رابط

استخدام غطاء للكاميرا

قد تتمكن بعض البرمجيات الخبيثة من تفعيل كاميرا الأجهزة سرًا لتصوير المستخدمين ومحيطهم أو أماكن عملهم دون علمهم.

- أولًا، من المهم تحديد مواقع الكاميرات الموجودة في الأجهزة التي نستخدمها. قد يكون لدينا أكثر من كاميرا واحدة في الجهاز نفسه، ويجب أيضًا أخذ الكاميرات الخارجية في الاعتبار إذا كنا نستخدمها بالإضافة إلى الكاميرا المدمجة.
- لحماية الخصوصية، يمكن استخدام ضمادات الجروح الصغيرة اللاصقة كغطاء بسيط وفعّال لكاميرا الجهاز. هذه الضمادات مفيدة لأن الجزء الأوسط منها خالٍ من اللاصق، مما يمنع ترك آثار لاصقة على عدسة الكاميرا. ويمكن إزالة الضمادة عند الحاجة إلى استخدام الكاميرا.
- يمكننا أيضًا البحث في متاجر بيع ملحقات الأجهزة الإلكترونية عن غطاء كاميرا الويب الرقيق والقابل للسحب. من الضروري اختيار غطاء رقيق لأن بعض الأغطية السميكة قد تمنع إغلاق الحاسوب المحمول بشكل صحيح.

استخدم الحوائل الماديّة لمنع الغير من رؤية شاشة أجهزتنا

عند التفكير في الهجمات على الأمان الرقمي، غالبًا ما أنّها محصورة بعمليّات معقدة تقنيًا، المفاجأة أنّ بعض عمليات اختراق معلومات المدافعين/ات عن حقوق الإنسان تمّت من خلال استراق النّظر على شاشات أجهزتهم أو استخدام كاميرات المراقبة. لذا فإن استخدام الحوائل الماديّة لحماية خصوصيّتنا تقلل من احتمال تعرّضنا لمثل هذه المحاولات. يمكن العثور على حوائل الخصوصية المادّية في متاجر ملحقات الأجهزة الإلكترونيّة.

للمزيد من المعلومات عن أدوات حماية الخصوصيّة لشاشات الأجهزة يُمكن الاطلاع على الرّابط التّالي | رابط

إيقاف نقاط الاتصال التي لا نستخدمها

تتيح شبكة الواي فاي لأجهزتنا الاتصال بالإنترنت عبر الموجات الراديوية والموجهات، التي تربطنا بدورها بالشبكة العنكبوتيّة الأوسع عن طريق اتصال سلكي. توفر شبكات الهاتف المحمول الاتصال بالأجهزة الأخرى في مختلف أرجاء العالم من خلال شبكة من الأبراج ومكررات إشارات الاتصال. كما يُمكن للاتصالات قصيرة المدى والبلوتوث ربط أجهزتنا بأجهزة أخرى قريبة باستخدام الموجات الراديوية. هذه الاتصالات مهمة للتواصل، لكنها قد تشكل خطراً إذا استغلها شخص ما للوصول إلى أجهزتنا وما عليها من معلومات حساسة. لذا، ينبغي لنا إيقاف تشغيل شبكات الاتصال مثل الواي فاي والبلوتوث عندما لا نحتاج إليها؛ فهذا يقلل من فرص وصول المخترقين إلى بياناتنا الحسّاسة دون علمنا. أحيانًا قد لا نلاحظ التغييرات الغريبة في سلوك جهازنا، مثل تباطؤ أدائه أو ارتفاع درجة حرارته دون استخدام مكثف. وعليه ينبغي لنا:

- إيقاف تشغيل أجهزتنا بالكامل ليلاً.
- الاعتياد على إيقاف شبكة الواي فاي، والبلوتوث، و/أو مشاركة الشبكة في حال عدم استخدامنا لها.
- التأكد من إيقاف البلوتوث: رابط
- التأكد من إيقاف شبكة الواي فاي: رابط
  - تعطيل خيار "طلب الانضمام إلى نقاط الاتصال الشخصية"
  - تعطيل خيار "المطالبة بالانضمام لشبكات جديدة"
  - تفعيل ميزة "عرض حالة الواي فاي في شريط القائمة" للتمكّن من معاينة حالة الواي فاي بسهولة وسلاسة أكبر
  - الاطلاع على الدّليل المضمّن في الرّابط التّالي لفهم رموز الواي فاي على ماك: رابط
- اتباع التّعليمات المدرجة في الرّابط التّالي للوصول إلى نافذة "تفضيلات النظام" للمشاركة وتأكد من عدم تحديد خيار "مشاركة الاتصال بالإنترنت:" رابط

مسح شبكات الواي فاي المحفوظة

عند تفعيل اتصال الواي فاي في أجهزتنا، تبدأ الأجهزة تلقائيًا بالبحث عن شبكات الواي فاي المعروفة لها، مما يشبه النداء إلى كل شبكة سبق الاتصال بها. هذه العملية قد يستغل المتطفلون القريبون ذلك لتحديد جهازك، حيث إن قائمة الشبكات المتصل بها عادة ما تكون فريدة وتشمل شبكات المنزل، والمكتب، ومنازل الأصدقاء، والمقاهي وما إلى ذلك من أماكن نرتادها. تسهل هذه البصمة

الفريدة للشبكات المعروفة على المتطفلين تحديد واستهداف أجهزتنا أو حتى تحديد أماكن وجودنا.
للوقاية من التّعرّف على أجهزتنا عبر قائمة شبكات الواي فاي المعروفة، علينا مسح هذه الشبكات المحفوظة وتعديل إعدادات الجهاز لكي لا يحتفظ بتفاصيل الشبكات التي يتصل بها. قد يجعل ذلك عملية الاتصال بالشبكات أكثر صعوبة، لكن يمكننا الاحتفاظ بمعلومات الاتصال في مدير كلمات المرور، مما يسهل الوصول إليها عند الحاجة دون تعريض الأجهزة للخطر.

- حفظ أسماء الشبكات وكلمات المرور في مدير كلمات المرور عوضا عن قائمة الشبكات على أجهزتنا.
- مسح قوائمنا من شبكات الواي فاي وإلغاء خيار تذكر الشبكات التي سبق وأن اتصل عبرها حاسوبنا: رابط

إيقاف نقاط المشاركة الّتي لا نستخدمها

تقدم الأجهزة الحديثة خيار مشاركة الملفات أو الخدمات مع الآخرين بسهولة، وهي ميزة مفيدة جدًا، لكن إذا تُركت هذه الميزة مشرّعة دون استخدام، قد تصبح فرصة للمتربصين للتسلّل إلى الملفات الموجودة على أجهزتنا. لمنع ذلك، من الضّروري:

- إيقاف خاصيّة الإرسال السّريع AirDrop، كما خاصيّة الاستقبال، فضلًا عن إزالة أي شخص أو جهة لا نريد مشاركته عبر هذه الخاصيّة: رابط
- اتباع التّعليمات في الرّابط التّالي للوصول إلى التّحكّم بالخيارات المفضّلة للنظام فيما يتعلّق بنقاط المشاركة، وتعطيل الخدمات التي لا نستخدمها، وإدارة تلك التي نستخدم (قد نستخدم مشاركة الشاشة أو مشاركة الطابعة للعمل، أو مشاركة الوسائط للاستماع إلى الموسيقى): رابط

استخدام جدار الحماية

تساعدنا جدران الحماية (Firewalls) على حماية أجهزتنا من البرمجيات غير المتوقعة التي قد تسترق السّمع على معلوماتنا أو تحاول الوصول إليها. تُعد هذه الأدوات بمثابة حارس الّذي يبقى عند باب البيت المفتوح، سواء أكان هذا الباب مفتوحًا بالخطأ أو فتحه المتربصين داخل المبنى. جدران الحماية التي تتابع الاتصالات الصادرة يمكنها أحيانًا تنبيهنا إذا حاولت برمجيات خبيثة سرقة البيانات أو التواصل مع مصادر خارجية لتلقي تعليمات. عند تثبيت جدار حماية خاص لتقييد الاتصالات الصادرة أو تكوين جدار الحماية المدمج لأداء هذه المهمة، يجب أن نكون مستعدين لبذل الوقت اللازم لتدريبه عليها إلى أن يصل لتنبيهنا فقط عند ملاحظة أنشطة غير اعتيادية.

- في هذا السّياق، نُوصي باتباع الإرشادات المدرجة في الرّابط التّالي: رابط
- نوصي بتفعيل "وضع التّخفّي" كما هو موصى به في المصدر السّابق.

عدّة من توصيات أُخَر للحماية

- في إعدادات النظام > خاصيّة سبوتلايت للبحث > نتائج البحث، إلغاء جهات الاتصال، والأحداث والتذكيرات، والبريد والرسائل، واقتراحات سيري، على الأقل.
- في إعدادات النظام > عبر خاصيّة سبوتلايت للبحث > وصولًا لإعدادات الخصوصية، قد نرغب في إضافة مجلدات حساسة لا نريد أن تصل لها خاصيّة سبوتلايت للبحث.
- التأكّد من تشفير قرص الحاسوب بالكامل، وتفعيل تفعيل ميزة خزنة الملفّات: رابط
- عِلاوة لما سبق، يُمكننا أيضًا الاستعانة بقائمة التّدقيق المتاحة عبر هذا الرّابط: رابط

نظام تشغيل لنكس

للحفاظ على أمان أجهزتنا العاملة بنظام تشغيل لينكس، يُرجى اتباع الدليل المتاح عبر هذا الرّابط.

2.2.2| الهواتف المحمولة

نظام تشغيل الأندرويد

استخدام أحدث إصدار من نظام تشغيل أندرويد

مع كل صباح، تُكتشف نقاط ضعف وثغرات في الأكواد المشغّلة لأجهزتنا وتطبيقاتنا؛ لذا من المُحال لمطوّري هذه الأكواد التّنبؤ أي سيُعثر عليها نظرًا للطبيعة المعقّدة للأكواد؛ أمّا المتربّصون، فقد يستغلون هذه نقاط الضّعف هذه لاختراق أجهزتنا. وفي ضوء ما يُكتشف من نقاط ضعف، يعمل المطورون على إصدار تحديثات تُعالج هذه الثّغرات؛ لذا، لا بدّ لنا من تثبيت التّحديثات واستخدام أحدث نسخة من نظام التشغيل لكل جهاز نستعمله؛ من المفيد أيضًا ضبط أجهزتنا على تحديث أنظمتها تلقائيًا لتخفف عنّا هذه المهمة.

- لنحرص تحديث البرمجيات ونحن في مكانٍ موثوق مثل المنزل أو المكتب—ليس مراكز الإنترنت أو المقاهي على سبيل المثال.
- قد يتطلب تحديث أنظمة تشغيل أجهزتنا لأحدث إصداراتها تنزيل برمجيات وإعادة تشغيل الأجهزة مرات عدة؛ لذا، سنحتاج لاستقطاع بعض الوقت لذلك، وقت لا نكون بحاجة فيه للعمل على الجهاز المُراد تحديث نظامه. لمقارنة أحدث إصدار من نظام تشغيل جهازنا والإصدار المثبت حاليًا لدينا، ينبغي لنا تتبع الخطوات أدناه، هكذا إلى أن يكف الجهاز عن إظهار الحاجة لأي تحديثات إضافية.
- في حال تعذّر تشغيل أحدث نسخة من نظام التّشغيل، فمن الأفضل التّفكير في خيار شراء جهاز جديد.
- التّثبّت من إعادة تشغيل الحاسوب بعد تنزيل التحديث، وذلك للتحقّق من تثبيت التّحديث بالكامل.
- للاطلاع على أحدث الإصدارات المتاحة، يُمكن البحث في الرّابط التّالي: رابط
- تحديث نظام تشغيل أجهزتنا: رابط
  - ضبط نظام التشغيل للقيام بالتّحديثات المتاحة عليه تلقائيًا: رابط
  - بالإضافة إلى ذلك، التّحقّق من "تصحيحات الأمان" المتعلقة بنوع جهاز أندرويد الخاص بنا: رابط
  - ولنكن على دراية بأن مصنعي الهواتف قد يتأخرون أحيانًا من شهر إلى سنة في إصلاح هذه الثغرات.
  - إذا لاحظنا أن التصحيحات الأمنية في أجهزتنا تتأخر دائمًا عن الإصدارات الأحدث، قد يكون من الحكمة التفكير في اقتناء هاتف من مُصنِّع يقدم تحديثات أمنية أسرع، مثل غوغل بيكسل. على الرغم من أن هذا قد يكون خيارًا أكثر تكلفة، إلا أنه يوفر مستوى أعلى من الحماية الأمنية.

استخدام التّطبيقات وتحديثها من مصادر موثوقة

متجر غوغل بلاي (Google Play) هو المنصة الرسمية للتطبيقات المخصصة لأجهزة الأندرويد. تجميع التطبيقات في مكان واحد يسهل علينا العثور على التطبيقات التي نحتاجها وتثبيتها، كما يتيح

لغوغل إمكانية مراقبة التطبيقات بشكل أفضل لضمان عدم وجود انتهاكات أمنية خطيرة. لذلك، من الأفضل دائمًا تثبيت التطبيقات فقط من متجر غوغل بلاي لضمان الأمان.
علينا تفقّد تحديثات التّطبيقات المتاحة في متجر غوغل بلاي بوتيرة منتظمة (مثلاً أسبوعيًا) لتثبيتها ومواكبة أحدث تحسينات الأمان المُضافة لتطبيقاتنا.
علينا تثبيت التطبيقات فقط من متاجرها الرّسميّة أو مواقع مطوّريها، إذ قد تكون مواقع التنزيل "المُقلِّدة" محل شك، إلّا إذا كنّا نعرف الجهات المزوّدة لهذه الخدمات ونثق بها. وفي حال ارتأينا أنّ منفعة تطبيق ما تفوق المخاطر المحتملة، يتعيّن علينا اتخاذ إجراءات وقائيّة إضافيّة لحمايّة أمننا، كالتّخطيط المُسبق لعدم تخزين معلومات حسّاسة أو شخصيّة على الجهاز الّذي يحوي ذلك التّطبيق.
في بعض الأحيان، توعز الحكومات الاستبدادية لشركات التّقانة بحجب تطبيقات معينة داخل حدودها، لتجاوز ذلك يجنح البعض لعمل "روت" أو "جذر" لأجهزتنا، وذلك بهدف تثبيت التطبيقات المحظورة من متاجر تطبيقات أخرى أو عبر مواقع إلكترونية.
نوصي بدورنا بالإحجام عن عمل روت لأجهزتنا، إذ يعرضنا ذلك لمخاطر أكبر ويكشفنا أكثر للبرمجيات الخبيثة، وعليه ينبغي لنا:

- تجنب "عمل روت" لأجهزتنا.
- واستخدام متجر غوغل بلاي لتنزيل التّطبيقات والتّحديثات.
- والتّحقق مما إذا كانت التطبيقات الخاصة بنا قد ثُبِّتَت من متجر غوغل وتعطيل تثبيت التطبيقات من مصادر غير معروفة باستخدام تقنية غوغل بلاي للحماية.

إزالة التّطبيقات التي لا حاجة لنا بها وتلك الّتي لا نستخدمها

يوميًا، يتم كشف نقاط ضعف جديدة في الأكواد التي تدير أجهزتنا وتطبيقاتنا، ولا يمكن للمبرمجين التنبؤ دائمًا بأماكن هذه النقاط نظرًا لتعقيد الأكواد. يمكن للمهاجمين استغلال هذه الثغرات لاختراق أجهزتنا. لذا، يُساعد حذف التطبيقات التي لا نستخدمها في تقليص عدد التطبيقات المحتمل تعرضها للخطر. بالإضافة إلى ذلك، قد تقوم التطبيقات غير المستخدمة بنقل بيانات عنا، كموقعنا الجغرافي، قد لا نرغب في مشاركتها. إذا كان من الصعب حذف التطبيقات، يمكننا على الأقل تعطيلها.
قد تشارك التطبيقات قد تشارك الكثير من بياناتنا مثل مُعرّف الهاتف، ورقم الهاتف، والشبكات اللّاسلكية التي نتصل بها. وفي كثير من الأحيان، لا نحتاج إلى تطبيق مُحدد للوصول إلى المواقع الإلكترونية والخدمات التي نستخدمها، بما في ذلك منصات وسائل التواصل الاجتماعي مثل فيسبوك أو واتساب. يُعد استخدام هذه الخدمات من خلال المتصفح على الجهاز بديلاً أكثر أمانًا لحماية خصوصيتنا.

- للتعرّف على كيفية حذف التطبيقات، يُمكن الاطلاع على الرّابط التّالي: رابط
- قد يتعذّر إلغاء تثبيت التطبيقات المثبّتة من المصنِّع على الهاتف، مع ذلك يُمكننا محاولة ذلك أو أقلّه تعطيلها باتباع الإرشادات المتاحة في الرّابط
- يُفضل الوصول إلى وسائل التّواصل الاجتماعي والمواقع الأخرى عن طريق تسجيل الدخول من خلال المتصفح (فيَرفُكس) بدلًا من تطبيقاتها.

التّحقّق من الأذونات الممنوحة للتطبيقات

يمكن للتطبيقات الّتي تصل إلى تفاصيل رقميّة حسّاسة أو الخصائص الموجودة على أجهزتنا—نحو تحديد الموقع، والميكروفون، والكاميرا، أو الإعدادات—أن تسرّب ما تصل إليه من معلومات كما قد

تُضحي مداخل يستغلها المتربّصون؛ وعليه، في حال انتفاء حاجتنا لتطبيق أو خدمة ما، حري بنا الإحجام عن منحها مثل هذه الأذونات. كما علينا:

- مراجعة جميع أذونات الوصول واحدًا تلو الآخر، علمًا أنّ الأذونات أدناه تُعد الأكثر شُبهة نظرًا لشيوع استغلال التّطبيقات الضّارّة لها:
  - الموقع
  - جهات الاتصال
  - الرّسائل
  - الميكروفون
  - التّعرّف على الصّوت أو الكلام
  - كاميرا (الويب)
  - تسجيل الشّاشة
  - سجلّات المكالمات أو سجل المكالمات
  - الهاتف
  - التّقويم
  - البريد الإلكتروني
  - الصّور
  - الأفلام أو الفيديوهات ومجلداهما (مكتبتاهما)
  - قارئ البصمات
  - الاتصالات قريبة المدى
  - البلوتوث
  - أي إعدادات تتطلب "الوصول إلى القرص،" أو "الملفّات،" أو "المجلّدات"، أو "النّظام،" أو بعض أو كل ما سبق
  - أي إعدادات تتطلب "التّثبيت"
  - خاصّيّة التّعرف على الوجه
  - السّماح بتنزيل تطبيقات أخرى

للمزيد من المعلومات والإرشادات بهذا الخصوص، يُمكننا:
قراءة هذا المقال: رابط
ثم اتباع هذه الخطوات:
سواء للإصدار السّادس من نظام أندرويد وما بعده: رابط
أو للإصدار 5.1 وما قبله: رابط

إيقاف خدمات الموقع ومسح السّجل

إذا كانت أجهزتنا تحتفظ بإحداثيّات أماكن وجودنا، فإنّه من الممكن تتبّع مواقعنا باستخدام نظام التّموضع العالمي، أو أبراج الهاتف المحمول، أو شبكات الواي-فاي الّتي نستخدمها، كما يمكن تحديد موقعنا أو استخدام هذا السّجل لإثبات وجودنا في أماكن معيّنة أو ارتباطنا بأشخاص محدّدين، وعليه ينبغي لنا:

- اعتياد تعطيل خاصيّة تحديد الموقع كليًّا، أو في حال عدم الاستخدام، سواء لجهازنا بالكامل كما ولكل تطبيق على حدة. (رابط)
- تفقد سجل الموقع ومسحه بوتيرة منتظمة، وذلك في حال لم عدم اختيارنا تعطيله أصلًا: رابط
- قد يختلف مكان إعدادات الموقع باختلاف جهاز أندرويد، ولكنها غالبًا في مكان ما في الإعدادات، أو خيارات الخصوصية، أو الأمان، كما وفي إعدادات حساب غوغل الخاص بنا.
- لحذف سجل الموقع السابق وضبطه بحيث لمنع أجهزتنا وخرائط غوغل من حفظ أماكن وجودنا وتحرّكنا، يُمكننا اتباع الإرشادات في الرّابط. كما في الرّابط.

إنشاء حسابات منفصلة على كل جهاز

نشدّد على تجنّب مشاركة الأجهزة الّتي نستخدمها للقيام بأعمال حسّاسة مع أي أطراف أخرى؛ وإن اضطررنا لمشاركتها مع زملاء من العمل أو أحد أفراد أسرتنا، فيمكننا ضمان درجة أفضل من الحماية لمعلومات الحسّاسة بإعداد حسابات منفصلة على كل جهاز، بحيث إن شاركنا أحدها أجهزتنا طرف آخر فإنّ وصوله يقتصر على ذاك الجهاز فيما تبقى ملفّاتنا الحسّاسة المرتبطة بحاسبتنا على الأجهزة الأخرى في مأمن ومنأى الاختراق.

- يُعد إنشاء عدة حسابات على الجهاز الواحد استراتيجية فعالة لتعزيز الأمان. يُمكن تخصيص أحد هذه الحسابات بصلاحيات "المدير." أما باقي الحسابات، فيُفضل منحها صلاحيات "عادية" أو "غير إداريّة."
  - يجب ألّا يكون لأحد سوانا إذن الوصول إلى حساب المدير.
  - ينبغي ألّا نُصرّح للحسابات العادية بالوصول إلى كافّة التّطبيقات، أو الملفّات، أو الإعدادات على أجهزتنا.
- يجدر بنا استخدام حساب عادي لإنجاز أعمالنا اليوميّة:
  - ينبغي لنا ألّا نستخدم حساب المدير إلّا عن الحاجة لإجراء تغييرات تؤثّر على أمن أجهزتنا، مثل تثبيت برمجيّات معيّنة.
  - يعتبر استخدام حساب عادي للأنشطة اليوميّة خطوة جيدة للحماية من التّهديدات الأمنية، خاصة تلك التي تنجم عن البرمجيات الخبيثة؛ فالحسابات العادية تحدّ من الصلاحيات، وبالتّالي يصعب على البرمجيات الخبيثة إحداث تغييرات كبيرة في النظام.
  - خلال السّفر عبر الحدود، قد تكون فكرة إنشاء حساب "للسفر" خطوة مفيدة ذكية لإخفاء معلوماتنا أكثر حساسية يقلل من المخاطر في حالة تفتيش الأجهزة من قبل السلطات الحدودية. يعتمد قرار استخدام حساب السفر على تقييم المخاطر والتوقعات بشأن مستوى التدقيق الذي قد يتعرض له الجهاز. في الحالات التي لا يُتوقع فيها تمحيص الجهاز، يمكن استخدام حساب عادي للأعمال غير الحسّاسة، ما يوفر درجة من الحماية وإمكانية الإنكار المبرر.
  - للتعرّف على كيفيّة حذف حسابات المستخدمين أو التبديل بينها أو إضافتها، عليك بالمصدر التّالي: رابط

إزالة حسابات المرتبطة بأجهزتنا ولا حاجة لنا بها

من الضّروري تقليص فرص الوصول غير المصرح به إلى أجهزتنا، أي غير تلك الّتي صرّحنا بها؛ لتحقيق ذلك لا بدّ ألّا نترك ذلك "الباب،" إن جاز التّعبير مفتوحًا (تُعرف هذه العمليّة بتقليص سطح انكشاف أجهزتنا للهجمات والاعتداءات). يُضاف لذلك التّفقّد الدّوري للحسابات المسجلة على أجهزتنا،

لضمان عدم إدخال حسابات على أجهزتنا دون علمنا.
- لإزالة حسابات المستخدمين غير المرغوبة، يُمكننا الاطلاع على الإرشادات المدرجة في الرّابط.

الحفاظ على أمن حسابات جيميل المرتبطة بأجهزتنا

ترتبط معظم الأجهزة الإلكترونيّة بحسابات خاصة مثل حسابات غوغل لأجهزة الأندرويد، والهواتف المحمولة من نوع كروم، وتلفاز غوغل، وكذلك حسابات آبل المستخدمة للأجهزة اللّوحيّة مثل الآي-باد، وساعات آبل، وأجهزة ماك المحمولة، وتلفاز آبل. قد يُسجَّل الدخول لنفس الحساب على أجهزة متعددة في ذات الوقت، مثل الهاتف، والحاسوب المحمول والتلفاز. وعليه إذا تمكّن شخص آخر من الوصول دون تصريح إلى حسابتنا، فإنّ هذا المكان يمكّننا من كشف ذلك واتخاذ الإجراءات اللازمة لإيقاف هذا الوصول. لتحقيق ذلك ينبغي لنا:
- تسجيل الدخول إلى كل حساب جيميل مرتبط بأجهزتنا.
- معاينة سجل الأجهزة التي تستخدم حسابتنا: رابط
- عند رصد نشاط مشبوه على حسابنا، مثل تسجيل الدخول من أجهزة لم تعد بحوزتنا أو لا نعرفها، يُمكننا توثيق ذلك بالتقاط صورة أو لقطة شاشة (رابط) لتلك الصفحات.
- التّفكير بخيار الانضمام إلى برنامج الحماية المتقدمة من غوغل: رابط

ضبط إعدادات قفل الشّاشة ووضعيّة السّكون

قد يبدو الهجوم التقني أكبر همّنا، بيد أنّ المحتمل أكثر هو مصادرة أجهزتنا أو سرقتها واختراقها طرف أو أطراف ما؛ لذا يجدر بنا قفل شاشات أجهزتنا بكلمة مرور تحول دون ولوج أحد إلى أجهزتنا بمجرّد تشغيلها. يفضّل استخدام خيار كلمات أو رمز المرور لقف الشّاشة وتجنب خيارات القفل الأخرى، فقد نُجبر في حال اعتقالنا أو تفتيشنا لفتح جهازنا بخاصيّة التّعرف على الوجه، أو بصمات الصّوت، أو الأصابع، أو العين، في حال كنّا قد اخترنا إحدى طرق القفل هذه. في ذات السياق، ثمَّ مخاطر تتعلق بوسائل القفل المختلفة، مثلًا برامج تخمين كلمات المرور يمكنها اختراق الرّموز القصيرة أو الأرقام السرية السّهلة. كذلك الأمر بالنّسبة لإقفال الأنماط، يمكن تخمينها بتقصي آثار الأصابع على شاشة الجهاز. وفي حال استخدام قفل بصمة الإصبع، يمكن جمع بصمات صاحب/ة الجهاز وصنع نسخة مزيفة عن البصمة لفتح الجهاز. كما أن تقنيات الفتح بالوجه ليست محصنة بالمطلق، حيث طُوِّرت طرق لخداع هذه الأنظمة.

في ضوء كل ذلك، تبقى عِبَارات المرور الطّويلة أكثر أنواع الأقفال أمانًا، وفيما يلي عِدّة من نصائح أُخَر:
- ينبغي ضبط الشّاشة لتقفل بُعيد فترة قصيرة من التّوقّف عن استخدامها (من دقيقة إلى 5 دقائق فترة جيدة).
- علينا استخدام عبارة مرور طويلة، تزيد على عشرة حروف، وعدم الاكتفاء بكلمة مرور قصيرة أو رقم سري.
- يُمكن لخاصّيّات فتح الجهاز ببصمات الأصابع، أو العين، أو الوجه، أو الصوت أن تُستخدم ضدنا بإرغامنا على فتح أجهزتنا؛ لذا علينا ألّا نستخدم هذه الخيارات إلّا إذا كان لدينا إعاقة ما تحول دون اللجوء لخيار كتابة عبارات المرور الطّولية.
- يجب أيضًا إزالة بصماتنا أو مُدخلات التّعرّف على وجهنا من جهازنا إن سبق لنا إدخال أي منهما أو كلاهما، يختلف مكان التّحكم بهذه الخواص باختلاف أجهزة أندرويد، كما قد تكون في عدّة مواضع الجهاز، لكن عادة تكون حيث إعدادات قفل الجهاز تكون: رابط

- يمكن تخمين أقفال الأنماط؛ لذا لنبتعد عن هذا الخيار.
- كذلك إنّ خيار التّمرير (المسح) السّريع للشاشة ليس بقفل آمن؛ لذا فلنتجنّبه.
- ينبغي لنا أيضًا تعطيل خيار إظهار كلمة المرور.
- لا غنى لنا عن إنشاء كلمة مرور طويلة: رابط
  - لنضبط جهازنا ليدخل في وضعية السّكون بعد فترة وجيزة من الكف عن استخدامه؛ بحيث لا بد لنا من إدخال كلمة المرور للخروج من وضعية السّكون. تجدر الإشارة إلى تباين مكان هذه الإعدادات بتباين نوع الأجهزة العاملة بنظام الأندرويد؛ لكن غالبًا تكون في دائرة إعدادات "العرض،" أو "النّظام،" أو "الأمان".

التّحكّم فيما يمكن رؤيته عندما يكون الجهاز مُقفلًا

وقف ظهور الإشعارات عند قفل الجهاز: إنّ وضع قفل شاشة متين لا يحصّننا من كافّة المخاطر. مثلًا إن تركنا تطبيقاتنا تظهر على الشّاشة خلال الإقفال، فإن ذلك يتيح لمن قد يضعون يدهم على جهازنا من معاينة المعلومات الحسّاسة الّتي قد تظهر في الإشاعات، سواء كانت رسائل، أو جهات اتصال، أو بريد إلكتروني وارد. لذا، من الضروري إيقاف ظهور الإشعارات على شاشة القفل لمنع تسرب مثل هذه المعلومات.

للحؤول دون ظهور أي إشعارات عند قفل الجهاز، علينا بالتباع الإرشادات المدرجة في الرّابط.

إذا وجدنا خيار "إضافة مستخدمين من شاشة القفل" في إعدادات الأمان > شاشة القفل أو النظام > الإعدادات المتقدّمة > المستخدمون المتعددون، علينا التأكد من أن هذا الخيار معطل.

تعطيل التّحكّم الصّوتي

عندما نضبط أجهزتنا لتقبل الأوامر الصوتية من خلال خدمات مثل سيري، كورتانا، غوغل فويس، إيكو، أو أليكسا، فهذا يعني أن الجهاز يظل في وضع الاستماع طوال الوقت. قد يؤدي ذلك إلى تسجيل بعض المحادثات وإرسالها إلى شركات مثل أمازون أو مايكروسوفت لأغراض مراقبة الجودة، حيث يُحْتَفَظ بهذه التسجيلات ومراجعتها من طرف جهات متعاقدة مع هذه الشّركات. كما يوجد احتمال لتثبيت أكواد ضارة على الأجهزة تُمكّن من التقاط كل ما يُسمع، مما يشكل خطرًا على خصوصيّتنا وخصوصيّة من حولنا.

إذا كان لدينا إعاقة تجعل من الصّعب الكتابة أو استخدام عناصر التّحكم اليدويّة، فإنّ استخدام خواص التحكم الصوتي قد يكون ضروريًا. يمكن اتباع بعض الإرشادات لضمان استخدام أكثر أمانًا لهذه الخاصية. ومع ذلك، إذا لم تكن هناك حاجة إلى استخدام التحكم الصوتي لهذا السبب، فمن الأفضل تعطيل هذه الخاصية لتعزيز الأمان.

- لنعطل مساعد غوغل أو خاصيّة التّحكم الصّوتي، أو كليهما. يختلف مكان التّحكم بهذه الخواص باختلاف أجهزة أندرويد، كما قد تكون في عدّة مواضع الجهاز، لكن عادة تكون حيث إعدادات غوغل تكون. في هذا السّياق، من المفيد مراجعة الإرشادات المدرجة تحت عنوان الخصوصيّة في الرّابط.
- إذا ارتأينا أنّ منافع استخدام السّمّاعات (مكبّرات الصوت) الذّكيّة (مثل أليكسا أو سيري) تفوق مخاطرها بالنّسبة لنا، يجدر بنا اتباع الإرشادات التّالية لضمان استخدام أكثر أمنًا لهذه السّمّاعات: رابط

استخدم الحوائل الماديّة لمنع الغير من رؤية شاشة أجهزتنا

عند التفكير في الهجمات على الأمان الرقمي، غالبًا ما أنّها محصورة بعمليّات معقدة تقنيًا، المفاجأة أنّ بعض عمليات اختراق معلومات المدافعين/ات عن حقوق الإنسان تمّت من خلال استراق النّظر على شاشات أجهزتهم أو استخدام كاميرات المراقبة. لذا فإن استخدام الحوائل الماديّة لحماية خصوصيّتنا تقلل من احتمال تعرّضنا لمثل هذه المحاولات. يمكن العثور على حوائل الخصوصية المادّية في متاجر ملحقات الأجهزة الإلكترونيّة.

- للمزيد من المعلومات عن أدوات حماية الخصوصيّة لشاشات الأجهزة يُمكن الاطلاع على الرّابط التّالي | رابط

استخدام غطاء للكاميرا

قد تتمكن بعض البرمجيات الخبيثة من تفعيل كاميرا الأجهزة سرًا لتصوير المستخدمين ومحيطهم أو أماكن عملهم دون علمهم.

- أولًا، من المهم تحديد مواقع الكاميرات الموجودة في الأجهزة التي نستخدمها. قد يكون لدينا أكثر من كاميرا واحدة في الجهاز نفسه، ويجب أيضًا أخذ الكاميرات الخارجية في الاعتبار إذا كنا نستخدمها بالإضافة إلى الكاميرا المدمجة.
- لحماية الخصوصية، يمكن استخدام ضمادات الجروح الصغيرة اللاصقة كغطاء بسيط وفعّال لكاميرا الجهاز. هذه الضمادات مفيدة لأن الجزء الأوسط منها خالٍ من اللاصق، مما يمنع ترك آثار لاصقة على عدسة الكاميرا. ويمكن إزالة الضمادة عند الحاجة إلى استخدام الكاميرا.
- يمكننا أيضًا البحث في متاجر بيع ملحقات الأجهزة الإلكترونية عن غطاء كاميرا الويب الرقيق والقابل للسحب. من الضروري اختيار غطاء رقيق لأن بعض الأغطية السميكة قد تمنع إغلاق الحاسوب المحمول بشكل صحيح.

إيقاف نقاط الاتصال التي لا نستخدمها

تتيح شبكة الواي فاي لأجهزتنا الاتصال بالإنترنت عبر الموجات الراديوية والموجهات، التي تربطنا بدورها بالشبكة العنكبوتيّة الأوسع عن طريق اتصال سلكي. توفر شبكات الهاتف المحمول الاتصال بالأجهزة الأخرى في مختلف أرجاء العالم من خلال شبكة من الأبراج ومكررات إشارات الاتصال. كما يُمكن للاتصالات قصيرة المدى والبلوتوث ربط أجهزتنا بأجهزة أخرى قريبة باستخدام الموجات الراديوية. هذه الاتصالات مهمة للتواصل، لكنها قد تشكل خطراً إذا استغلها شخص ما للوصول إلى أجهزتنا وما عليها من معلومات حساسة. لذا، ينبغي لنا إيقاف تشغيل شبكات الاتصال مثل الواي فاي والبلوتوث عندما لا نحتاج إليها؛ فهذا يقلل من فرص وصول المخترقين إلى بياناتنا الحسّاسة دون علمنا. أحيانًا قد لا نلاحظ التغييرات الغريبة في سلوك جهازنا، مثل تباطؤ أدائه أو ارتفاع درجة حرارته دون استخدام مكثف. وعليه ينبغي لنا:

- إيقاف تشغيل أجهزتنا بالكامل ليلاً.
- الاعتياد على إيقاف شبكة الواي فاي، والبلوتوث، و/أو مشاركة الشبكة في حال عدم استخدامنا لها.
- تفعيل وضع الطيران وإيقاف شبكة الواي فاي.
- تعلّم كيفية تشغيل الواي فاي والبلوتوث بشكل انتقائي بعد تفعيل وضع الطائرة، لاستخدام الخدمات التي نرغب بها فقط.

- تعطيل خاصية "نقطة الاتصال الشّخصيّة" عندما لا نستخدمها.
- تفعيل وضع الطّائرة والتّثبّت من إيقاف الواي فاي والبلوتوث:
  - تختلف خطوات القيام بذلك باختلاف الهاتف، لكن لا ضير في تجربة الخطوات المدرجة في الرّابط، أو في هذا الرّابط.
  - كذلك علينا بالاطلاع على الإرشادات المتاحة بالرّابط التالي بخصوص بإحداث تغييرات أكثر على صعيد شبكة الواي فاي: رابط؛ كما علينا التّأكد من تعطيل خيار التّشغيل التّلقائي لشبكة الواي فاي والاتصال بالشبكات المفتوحة.
  - أيضًا، لا بدّ لنا من التأكد من أن جهازنا لا يوفر اتصال إنترنت لشخص آخر باستخدام خاصيّة نقطة الاتصال الشخصية؛ لذا علينا العثور على إعدادات هذه الخاصيّة وتعطيلها. يُمكننا الاستفادة من الإرشادات المتاحة في هذا الرّابط، أو الخطوات المتاحة هنا.

مسح شبكات الواي فاي المحفوظة

عند تفعيل اتصال الواي فاي في أجهزتنا، تبدأ الأجهزة تلقائيًا بالبحث عن شبكات الواي فاي المعروفة لها، مما يشبه النداء إلى كل شبكة سبق الاتصال بها. هذه العملية قد يستغل المتطفلون القريبون ذلك لتحديد جهازك، حيث إن قائمة الشبكات المتصل بها عادة ما تكون فريدة وتشمل شبكات المنزل، والمكتب، ومنازل الأصدقاء، والمقاهي وما إلى ذلك من أماكن نرتادها. تسهل هذه البصمة الفريدة للشبكات المعروفة على المتطفلين تحديد واستهداف أجهزتنا أو حتى تحديد أماكن وجودنا.
للوقاية من التّعرّف على أجهزتنا عبر قائمة شبكات الواي فاي المعروفة، علينا مسح هذه الشبكات المحفوظة وتعديل إعدادات الجهاز لكي لا يحتفظ بتفاصيل الشبكات التي يتصل بها. قد يجعل ذلك عملية الاتصال بالشبكات أكثر صعوبة، لكن يمكننا الاحتفاظ بمعلومات الاتصال في مدير كلمات المرور، مما يسهل الوصول إليها عند الحاجة دون تعريض الأجهزة للخطر.

- حفظ أسماء الشبكات وكلمات المرور في مدير كلمات المرور بدلاً من قائمة الشبكات على أجهزتنا.
- ينبغي لنا اعتياد على مسح قائمة شبكات الواي فاي بانتظام باتباع الإرشادات المتاحة في الرّابط التّالي، وذلك لكل شبكة نتصل بها: رابط
- أخيرًا وليس آخرًا، علينا تعطيل خيار التشغيل التّلقائي لخاصيّة الواي فاي تلقائيًا والاتصال بالشبكات المفتوحة: رابط

إيقاف نقاط المشاركة الّتي لا نستخدمها

تقدم الأجهزة الحديثة خيار مشاركة الملفات أو الخدمات مع الآخرين بسهولة، وهي ميزة مفيدة جدًا، لكن إذا تُركت هذه الميزة مشرّعة دون استخدام، قد تصبح فرصة للمتربصين للتسلّل إلى الملفات الموجودة على أجهزتنا.

- يتخلف موضع إعدادات هذه الخصائص باختلاف الجهاز العامل بنظام، لكن يُمكننا الوصول إليها بالحث عن خيار الأجهزة المتصلة، أو شبكات الجهاز، أو خيار مشابه في الإعدادات، المهم أن نُعطّل الاتصال بجميع الأجهزة المدرجة هناك أو نزيلها.
- لنعطل ميزة مشاركة الملفات والروابط مع أجهزة الأندرويد القريبة منّا: رابط
- إذا اضطررنا لاستخدام المشاركة مع شخص قريب، لنحرص المشاركة بالوضع المخفي: رابط

خيارات وتدابير متقدّمة: استخدام أندرويد دون حساب غوغل

إذا كنا قلقين بشأن تتبع غوغل لحركاتنا وسكناتنا، يمكننا إزالة حساب غوغل من أجهزتنا باتباع الخطوات المتاحة في الرابط. ومن الأفضل لنا تخطي خطوة "تسجيل الدخول" عند التكوين الأول لهواتفنا؛ بهذه الطريقة، نضمن عدم ارتباط أجهزتنا بأي حساب غوغل، مما يمنع إضافة معلومات إلى ملفاتنا الشخصية من موقعنا، أو سجلّات بحثنا، أو تطبيقاتنا، إلى ما ذلك من بيانات.

لكن إن لم يكن لدينا حساب غوغل على جهازنا، لا سبيل لنا لتثبيت ما نريد من تطبيقات إلّا من مصادر خارج متجر غوغل بلاي.

في هذه الحالة يُمكننا استخدام متاجر بديلة، مثل متجر إف-درويد F-Droid ومتجر أورورا Aurora | رابط
https://gitlab.com/AuroraOSS/AuroraStore/-/blob/master/README.md

- لا يتيح إف-درويد سوى التّطبيقات مفتوحة المصدر والمجّانيّة. لتثبيت هذا المتجر علينا تنزيل ملف F-Droid (رابط)، ومنحه إذن التّثبيت على جهازنا. نتيجة ذلك قد نحتاج مؤقتًا السّماح لتثبيت تطبيقات مجهولة المصدر (رابط)؛ لذا علينا التّثبّت من تعطيل هذا الخيار بمجرّد تثبيت متجر إف-درويد على جهازنا.
- من جهة أخرى يُمكننا العثور على كافّة التّطبيقات الموجودة في متجر غوغل بلاي على في متجر أورورا الّذي يُمكننا تنزيله من متجر إف-درويد: رابط
- من المهم التحقق يدويًا وبانتظام من توافر تحديثات التطبيقات من خلال فتح متجري إف-درويد وأورورا؛ عدا التّثبت من أصالة التّرقيات المتاحة لبعض التّطبيقات نظرًا لأن التحديثات التلقائية قد لا تعمل دائمًا في هذه الحالة، لذا لا بدّ من التّيقّظ لهذه المسألة لما قد يسفر عنه استخدام التّطبيقات القديمة من مخاطر وثغرات مع مرور الوقت.

المزيد من الخيارات والتدابير متقدّمة: تغيير نظام تشغيل أجهزة أندرويد

نظام أندرويد، الذي تطوره شركة غوغل، يأتي مزودًا بتطبيقات غوغل التي تتتبع أنشطتنا وتجمع بيانات كثيرة حول أفعالنا ومواقعنا. في بعض الحالات، من الممكن تثبيت نظام تشغيل أندرويد بديل يوفر مزيدًا من الأمان والخصوصية، مثل نظام لينيج (lineage) المتاح على lineageos.org، أو نظام كالِكس (Calyx) على calyxos.org، أو نظام غرافين (Graphene) على grapheneos.org. يعتبر هذا الخيار حلًا متقدمًا، لكن وقبل الشروع فيه، من الضروري التحقق من توافق هذه الأنظمة مع جهازنا. علاوة على ذلك، هناك العديد من الخطوات الواجب اتباعها لتثبيت هذه الأنظمة، وإذا حدث أي خطأ، قد يؤدي ذلك إلى عطب الجهاز.

2.3| الأمان على الإنترنت

2.3.1| أمن الشبكات

- يمكن أن نتعرض نحن وأجهزتنا، بالإضافة إلى اتصالنا بالإنترنت وتصفحنا له، لمجموعة متنوعة من الهجمات التي تختلف باختلاف أنواع الشبكات التي نستخدمها.
- إمكانيّة الاختراق قائمة سواء شبكة الواي-فاي، أو جهاز التّوجيه بالكوابل، ونقاط الاتصال، والأجهزة المستخدمة—جميعها عُرضة للمهاجمة والاختراق؛ لذا علينا:
  - التثبّت من تحديث البرامج الثّابتة باستمرار
  - تغيير آليات الوصول القياسية مثل اسم شبكة الواي-فاي، أو كلمة المرور الخاصّة بها، أو كلمة المدير.
  - تفعيل جدار الحماية الخاص بجهاز التّوجيه لحماية جهاز التّوجيه وسائر أجهزتك من كافّة الهجمات عبر الإنترنت.
- يُمكن لأجهزة التّنصّت آي إم إس آي كاتشر الموضعة بين موقعنا وأقرب برجٍ من أبراج شبكة المحمول اعتراض اتصالنا بالبرج؛ وبالتّالي التّنصّت على مكالماتنا. تعمل هذه الأجهزة كوسيطٍ بين أجهزتنا والبرج، ما يُعطيها كوة للاطلاع خلسة على كافّة العناوين الّتي نتصفح، وبالعناوين لا نقصد المحتوى—فقط العناوين—عدا إمكانيّة الوصول إلى رسائلنا أو مكالماتنا. على ذات الغرار، يُمكن—قانونًا—حمل أبراج شبكة المحمول (اللواقط)، أو مزودي خدمات الإنترنت الواي-فاي والّتي تعمل بالكوابل أو الخطوط الأرضية على تسليم هذه البيانات أو تمكين جهات إنفاذ القانون من الوصول والحصول عليها.
  - التّأكد من عدم مشاركة أي محتوى حساس عبر المكالمات أو الرسائل النّصيّة القصيرة.
  - إخفاء حركات تصفحك للإنترنت بواسطة الشبكات الافتراضيّة الخاصّة (للمزيد بهذا الخصوص، عليك بالقسم الثّاني من المحور الثالث من الفصل الثّاني| استخدام الشّبكات الافتراضيّة الخاصّة) أو تطبيقات البروكسي أو متصفح التّوجيه البصلي (Tor Browser) (للمزيد بهذا الخصوص، يُمكنك مراجعة القسم الثّالث من المحور الثالث من الفصل الثّاني| التّحايل على الرّقابة: سبل وطرائق)
  - لا بدّ لنا من اختبار أيّ أداة نستخدمها للالتفاف على حظر وحجب المواقع عند توافر اتصال جيد بالإنترنت. جدير بالذّكر أنّه من الصّعب التّيقّن من دقّة استخدامنا لمثل هذه الأدوات لا سيّما في الظّروف الطّارئة، يُضاف لذلك أنّ المواقع الّتي تتيح مثل تنزيل هذه الأدوات كثيرًا ما تُحظر.
- أولًا، نتعرّف على عنوان بروتكول الإنترنت الخاصّ بنا (IP) على موقعٍ نحو IPLocation أو WhatIsMyIP.
- عادةً ما يكون النّسق والشّكل العام لعنوان الIP شبيه لما يلي 192.168.10.1 أو db8:0:1234:0:567:8:1:2001.
- ثم، على نفس الجهاز، نُشغّل التّطبيق الّذي نريد استخدامه للالتفاف على نقاط أو عقبات الحجب والحظر على الإنترنت.
- بعد ذلك، نعود إلى عنوان الIP ونبحث في الموقع الّذي استخدمناه ونعيد تحديثه (Refresh).
- الآن نتأكد من أنّ عنوان الIP قد اختلف.

- أمّا إذا ما كان العنوان ذاته، فذلك يعني أنّ التّطبيق الّذي نستخدمه لم يخف عنوانها، بعبارةً أخرى، معلومات تصفحنا ما زالت مكشوفة ويمكن تعقّبها.

فيما يلي جملة من الموارد المُساعدة لفهم التّهديدات المرتبطة باستخدام الإنترنت والشّبكات:

- عِدّة الأمان: آليّة عمل الإنترنت، وكيفيّة قيام بعض البلدان بحظر المواقع| رابط
- منصّة توتم التّعلّميّة الإلكترونيّة، "كيف يعمل الإنترنت؟ ليس سحبًا وإنما كابلات: لنكتشف الإنترنت معًا"| رابط

2.3.2| استخدام الشّبكات الافتراضيّة الخاصّة (VPNs)

بفضل الشّبكات الافتراضيّة الخاصّة (VPN) يُمكننا جعل اتصالنا بالإنترنت وكأنه يتم من منطقة أو بلدٍ غير منطقتك وبلدك الفعليين، كما يُمكن لهذه الشّبكات أن تحمي اتصالك بالإنترنت من التّطفل على شبكة الواي-فاي الخاصّة بنا. لو كان اتصالنا بالإنترنت يشبه نفقًا، تكون الشّبكة الافتراضيّة الخاصّة جداره الخارج الحامي.

تعتمد بعض خدمات الشّبكات الافتراضيّة الخاصّة على خصائص مضمّنة في أنظمة التّشغيل— ويندوز، ولِنُكس، وماك، والآ. أو. اِس، فيما يتطلّب البعض الآخر تثبيت برامج إضافيّة وتكوينها، مثل تطبيقي OpenVPN أو WireGuard. يوفّر بعض مزودي خدمات الشبكات الافتراضيّة الخاصّة أدوات تثبيت مُحاكة خصيصًا للتعامل مع كل شيء هذه الجبهة بالنيابة عنّا.

في هذا السّياق، من المفيد الإبقاء على جُعبة من تطبيقات الشبكات الافتراضيّة، فإن حُظِر أحدها، نستخدم آخرًا، كون هذه التّطبيقات تفتقر لخاصيّة اجتياز الحظر، إن حُظرت.

نجد في هذا الرّابط طيفًا من تطبيقات الشّبكات الافتراضيّة الخاصّة: رابط

2.3.3| التّحايل على الرّقابة: طرائق وسُبل

استخدام متصفّح تور (TOR)

Tor هو تطبيق مجاني ومفتوح المصدر يستخدم شبكة من المرحلات التطوعية لإخفاء نشاطك عبر الإنترنت مع توفير الوصول إلى بعض المواقع المحجوبة. قد تكون شبكة Tor محظورة في بعض المناطق، وقد يؤدي استخدامها إلى جعل اتصالك يبدو مريبًا لأي شخص قد يراقب نشاطك عبر الإنترنت.

متصفّح التّوجيه البصيلي (The Router Onion) أو ما يُعرف اختصارًا بتور (TOR)— هو تطبيق مجاني مفتوح المصدر يستخدم شبكة من التتابعات (الخوادم) التّطوعية الّتي تعمل على إخفاء هويتنا ونشاطنا على الإنترنت وتتيح لنا الوصول إلى بعض المواقع المحظورة. تحظر بعض الدّول استخدام شبكة تور، مما قد يجعل استخدامنا لها موضع ريبة بالنّسبة للجهات المُحدَوْدِبة على رصد تحرّكاتنا على الإنترنت.

هو تطبيق مجاني ومفتوح المصدر يستخدم شبكة من المرحلات التطوعية لإخفاء نشاطك عبر الإنترنت مع توفير الوصول إلى بعض مواقع الويب المحظورة. قد يتم حظر شبكة تور في بعض المناطق، وقد يؤدي استخدامها إلى جعل اتصالك يبدو مريبًا لأي شخص قد يراقب نشاطك عبر الإنترنت.

يعمل متصفح تور بمنهجيّة تُشبه عمل الشّبكات الافتراضيّة الخاصّة، لكن بدلاً من توجيه تحرّكاتك على الإنترنت إلى مزود خدمة واحد، يوزّعها على ثلاثة خوادم على الأقل، وبذلك يُخفي من طلب زيارة

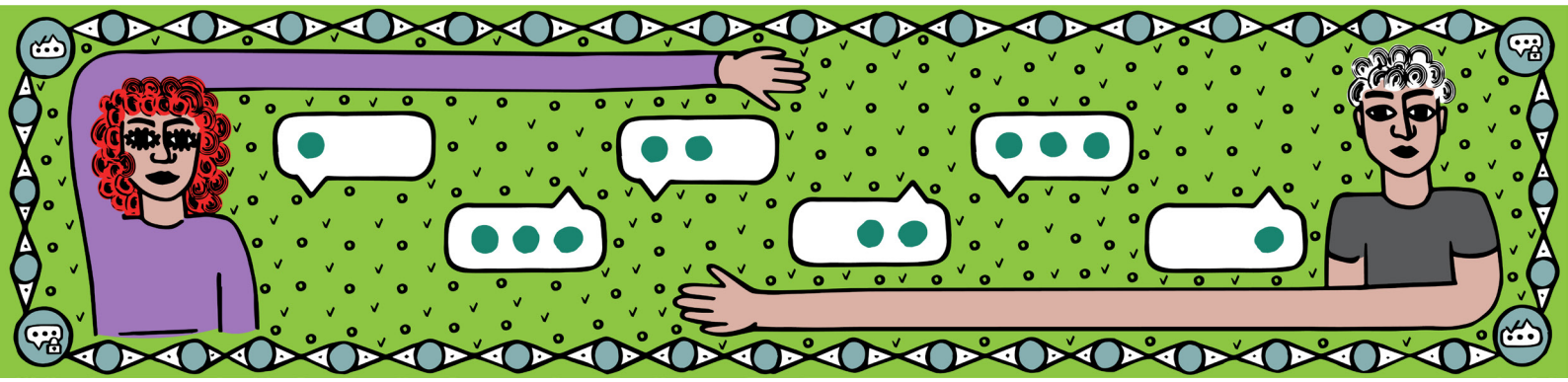
ماذا ويعزّز خصوصيتنا. يُذكر أنّ لتور ألوف مؤلّفة من الخوادم الّتي يديرها متطوعون ومتطوعات في مختلف أرجاء العالم.
وإن كنّا في أحد البلدان الّتي تحظر متصفّح تور أو تُدرجه ضمن المنوعات أو المواقع غير الآمنة، يُمكننا استخدام نسخة تور برِدج (TOR Bridge).
تور برِدج متاح للتنزيل عبر الرّابط.
يعمل متصفّح تور على حل ثلاثة من إشكاليّات الخصوصيّة: رابط

1. يمنع تور المواقع الإلكترونيّة والخدمات الأخرى ذات الصِّلة من تحديد موقعنا—هذه البيانات الّتي يُمكن يتمخّض عن تجميعها قواعد بيانات عن عاداتنا واهتماماتنا. ب باستخدام تور، لن تُقدَّم بياناتنا كمسلّمة من مسلّمات استخدامنا للشبكة، بحيث يسلّمنا تور زمام التّحكم بكل اتصال لنا مع مكوّنات الإنترنت وما المعلومات الّتي نوافق على مشاركتها بملء اختيارنا.
2. يمنع تور الأشخاص المتربصين بتحرّكاتك على الشّبكات المحليّة لمعرفة المعلومات الّتي تجمعها ومن أين تجلبونها، ويشمل ذلك مزودي خدمات الإنترنت أو أي شخص لديه إمكانية الوصول إلى شبكة الواي-فاي المنزليّة أو جهاز التّوجيه الخاص بنا، كما يمنعهم من تحديد ما يُسمح لنا معرفته ونشره، فمتى نصل إلى أي جزء من شبكة تور، نستطيع أن نصل لأي موقع إلكتروني على الشّبكة العنكبوتيّة.
3. ينقل متصفح تور اتصالك من خلال أكثر من مُرحِّل كي لا يحول دون تمكّن أي مرحل من تفصيل نشاطك على الإنترنت، ويتحقّق ذلك نتيجة أنّ كل مرحل تُديره منظّمات أو أفراد مختلفون، هكذا يُحقّق توزيع الثّقة أمانًا أوثق من نهج وكيل المرحلة الواحدة.

استخدام خدمة الوكيل (البروكسي)

إن كانت إحدى خواص تنخيل النّشاط على الإنترنت تمنع الوصول إلى موقع ما، أو تحجب الوصول إليه من منطقة ما، يُمكن لبرمجيات البروكسي أن تجعل طلب الوصول لسين أو صاد من المواقع المحجوبة كأنه من مكان آخر يُتاح فيه الوصول لتلك المواقع واجتياز الحجب.

- يُمكن تجريب برنامج لانترن لهذا الغرض (https://lantern.io/ar). يناسب هذا التّطبيق أنظمة تشغيل أندرويد، آي. أو. اِس، ولِنُكس، وماك، وويندوز، يعد أداة آمنة ومفتوحة المصدر تمكّننا تجاوز الحجوبات العامّة باستخدام بروكسات بروتوكول الHTTPS لتأمين وصول لا رقابة عليه للمضامين والمحتويات المتاحة على الشّبكة العنكبوتيّة.
- كذلك يُمكن استخدام تطبيق سايفِن (Psiphon) لهذا الغرض (https://psiphon.ca/). يُناسب هذا التّطبيق أنظمة أندرويد، وآي. أو. اِس وماك، وويندوز، ويعدّ أداة آمنة ومفتوحة المصدر تمكّننا تجاوز الحجوبات العامّة باستخدام الشّبكات الافتراضيّة الخاصّة وبروكسات بروتوكول الـ SSH لتأمين وصول لا رقابة عليه للمضامين والمحتويات المتاحة على الشّبكة العنكبوتيّة. يموّل سايفن من خلال الإعلانات والمعلنين الّذي يقدّمون الدّعم المالي للتطبيق بهدف الوصول بإعلاناتهم لمستخدميه ومستخدماته.
- إن حُجبت عنك صفحة التّنزيل الخاصّة بتطبيق سايفن، يُمكنك التّواصل مع مطوريه على البريد الإلكتروني التّالي: get@psiphon3.com، وهم سيرفدونك برابطٍ بديل.
- يُذكر أنّ رابط التّنزيل المباشر لتطبيق سايفن على الأجهزة العاملة بنظام أندرويد تتطلّب السّماح بتثبيت تطبيقاتٍ مجهولة؛ وهذه الخطوة تجعل جهازكم منكشفًا للبرمجيات الخبيثة.



2.4| أمن الاتصالات

يستند محتوى هذا الفصل على مادّة "سُبل الحفظ الآمن للملفّات" المتاحة عبر منصّة دليل عدَّة الإسعاف الأوّلي الرّقمي: رابط
لكل طريقة اتصال، رقمية كانت أم غير رقميّة، مزاياها وعيوبها، من حيث ملاءمتها للأغراض المرجوة منها، وشيوعها، وتكلفتها، وما توفره من أمان، إلى ما هنالك من اعتبارات أخرى. لكن يبقى التّقييم الأخير متروكاً لكل منّا كي نزن مزايا ومخاطر الطّرائق والسّبل الّتي نستخدمها للتواصل. لكننا قد لا نختلف بأن زيادة المخاطر تقتضي تريّثًا وتدبّرًا في اختيار ما نستخدمه أدوات اتصال.

الآن دعني أخبرك ملاحظة صغيرة عن وسائل التّواصل الاجتماعي: من زاوية تبدو وسائل التواصل الاجتماعي مساحة وأداة للتواصل مع الآخرين ونشر ما نجده مهمًا من مضامين، لكن في من جهة أخرى، تستخدم وسائل التواصل الاجتماعي تفاعلنا واتصالاتنا عبرها لجني المال؛ وذلك بمشاركة معلومات عنا بعلمنا أو دونه مع أطرافٍ ثالثة، مثل عاداتنا في الشراء، وأنماط تواصلنا الاجتماعي، وأماكن وجودنا، وتواريخ ميلادنا، وغيرها من المعلومات التعريفية. بمجرّد استخدامنا لأحد هذه المنصّات، فذلك يعني موافقتنا على شروط استخدامها التي تجيز لشركات هذه المنصّات بمشاركة معلوماتك أو بيعها. وفي بعض الأحيان تفتقر هذه الشّروط للواضح حيال مدى استخدامهم هذه المعلومات وإتاحتها للعموم.

تزداد مراقبة الحكومات وأجهزة إنفاذ القانون لوسائل التواصل الاجتماعي، حيث يتم جمع البيانات المتاحة علنًا و"البيانات الوصفية" المرافقة لها، والتي قد تتضمن تفاصيل كوقت التقاط صورة أو سجلات التواصل بين الأشخاص. في بعض الحالات، قد توعز هذه الجهات إلى شركات التواصل الاجتماعي تسليم معلومات خاصة عن أفراد محددين، خاصةً النشطاء في مجال حقوق الإنسان.
نظرًا للتغيّر المستمر في إعدادات خدمات وسائل التّواصل الاجتماعي، فإنّ هذا الدليل لا يقدّم اقتراحات خاصة بأمن الحسابات على وسائل التواصل الاجتماعي باستثناء:

- استخدام كلمات مرور آمنة وتفعيل المصادقة ذات العاملين (للمزيد يُمكن الاطلاع على المحور الأول في الفصل الثّاني: كلمات المرور والحسابات)
- والتّفكير في خيار الشّبكات الافتراضيّة الخاصّة (المعروفة اختصارًا بـVPN) أو تطبيقات البروكسي للإخفاء، وهي أدوات قد تكونين تستخدميها (للمزيد يُمكن الاطلاع على القسم الثاني "استخدام الشّبكات الافتراضية الخاصّة" والثالث "التّحايل على الرّقابة: طرائق وسُبل" من المحور الثّالث في الفصل الثّاني)

في الأزمات، لا نفكر بنفس القدر من الوضوح، وقد نضطر إلى التصرف بسرعة بل واتخاذ قرارات خطرة؛ لذا لا بدّ لنا من استراتيجيّة اتصال جاهزة للطوارئ والأزمات لتساعدنا في الحفاظ على أمننا.

إعداد خطة للتواصل والاتصال

لا بدّ لنا من بناء خطة تواصل لنا شخصيًا ولمجتمعنا الصّغير، بل وعلينا مُحكاة تنفيذها مرارًا كي نضمن تمكّنا من الإبقاء على حبل على التواصل والاطمئنان على بعضنا البعض في ساعات اشتداد الأزمات.

- نتحدث مع جهات الاتصال الخاصة بنا. نقترح ونناقش ونتفق على خطة محدّدة لكيفية التواصل (أو الإحجام عن التواصل) على أن تشمل الخطّة:
  - المخاطر المُدركَة
  - التطبيقات والخدمات التي سنستخدمها وتلك الّتي سنتجنبها
  - الخطوات الّتي علينا اتخاذها حال حدوث خطأ في تنفيذ الخطة
- نفكر في الخطوات غير الرسمية التي يمكننا اتخاذها، بما في ذلك:
  - إنشاء وتبادل عناوين البريد الإلكتروني الاحتياطية (البديلة)
  - وتبادل أرقام الهواتف
  - ومشاركة جهات الاتصال في حالات الطوارئ
- نفكر في المزيد من الخطوات الرسمية التي يمكننا اتخاذها، بما في ذلك:
  - سُبل الاتصال المُدعّمة بموجب سياسة الأمان التّنظيمي، أو حفظ البيانات، أو الإبقاء على المستندات
- التّفكير بما نريد التّعبير عنه وأين نعبّر عنه، بما في ذلك:
  - أيسر السّبل للحؤول دون تمكّن الآخرين من معرفة معلومات حساسة هي عدم إرسالها أو قولها.
  - على سبيل المثال، علينا التخطيط لتفادي إرسال رسائل نصية في أوقات عبور من نتصل بهم لمعابر حدودية أو في حال احتجازهم.
  - لا بدّ لنا من تطوير لغة رمزية نستخدمها لتجنب المجاهرة في الأسماء والعناوين والخطوات الّتي نحن بصددها، إلخ.
- أخيرًا وليس آخِر، التّدريب ثُم التّدريب ثُم التّدريب على تنفيذه خطّة الاتصال المُعدّة.

معايير اختيار الأدوات أو المنصّات

قبل اختيار أي منصّة تواصل أو تطبيق أو برنامج، ينبغي لنا تحرّيه أولًا، وفيما يلي بعض الأسئلة المهمة التي ينبغي لبحثنا الإجابة عنها:

- هل المنصة ناضجة بما فيه الكفاية؟ منذ متى تم تعمل؟ هل ما زال يجري تطويرها بوتيرة نشطة؟ هل لديها مجتمع كبير من المطورين النشطين؟ كم عدد مستخدميها النشطين؟
- هل توفر المنصة التشفير؟ هل تدعم التّشفير التّام أو الجامع والمانع (End-to-End) أم أنها أن التشفير فقط من الخادم؟
- لأيّ تشريعات يخضع مالكو المنصّة وأين تقع خوادمهم؟ هل يشكل هذا تحديًا محتملاً لنا أو لشركائنا؟
- هل تسمح المنصة بالاستضافة الذاتية (Self-Hosting)

- هل المنصة مفتوحة المصدر؟ هل توفر كود المصدر لمن أراد تفحّصه؟
- هل تم تدقيق المنصة بشكل مستقل؟ متى كانت آخر مراجعة؟ ماذا يقول الخبراء عن المنصة؟
- ما هو تاريخ تطوير وملكية المنصة؟ هل واجهت أي تحديات أمنية؟ كيف استجاب ملّاكها ومطوروها لهذه التحديات؟
- كيف نتواصل مع الآخرين عبر هذه المنصّة؟ هل نحتاج إلى علينا إدخال رقم الهاتف، أو البريد الإلكتروني، أو اسم مستخدم؟ هل نحتاج لتثبيت تطبيق/برنامج خاص لاستخدامها؟ ما الجزئيات التّي يتطلّب التطبيق/البرنامج الوصول إليه على أجهزتنا؟ سجل العناوين، أم الموقع، أم الميكروفون، ربما الكاميرا، إلخ؟
- ما البيانات الّتي تُحفظ على خوادم المنصّة؟ وأي هذه البيانات يستطيع مالك المنصة الوصول إليه؟
- هل تضم المنصّة الخصائص اللازمة للأغراض المرجو تحقيقها من استخدامها؟
- هل تكلفة استخدام المنصّة مِمّا يُقدر عليها؟ على أن يشمل ذلك رسوم الاشتراك المحتملة، والتعلم والتنفيذ، والدعم التقني اللازم، وتكاليف الاستضافة، وما إلى ذلك من أمور.

2.4.1| التّصفّح الآمن

فيَرفُكس كمتصفح قياسي

يستند محتوى هذا المحور على مادّة "متصفح فيَرفُكس" المتاحة عبر منصّة دليل عدَّة الإسعاف الأوّلي الرّقمي: رابط
نوصي بشدة باستخدام متصفح فيَرفُكس من موزيلا، لما له من خصائص أمان بنيويّة، كما أنّه مجاني ومفتوح المصدر.

التّأكد من تحديث نسخة المتصفح الّتي نستخدمها

- من المفترض أن يتم تحديث فيَرفُكس تلقائيًا، لكن يمكننا التحقق مما إذا كان لدينا أحدث إصدار من المتصفح عبر الرّابط.

إيقاف تشغيل مدير كلمات المرور المدمج في المتصفح

- يستطيع فيَرفُكس حفظ كلمات المرور وتشفيرها لك، إلَّا أنّنا نوصي بعدم تفعيل هذه الميزة واستخدام مدير كلمات مرور منفصل مثل KeePassXC بدلاً من ذلك. (للمزيد يُمكن الاطلاع على القسم الثّاني من المحور الأوّل من الفصل الثّاني "استخدام برامج إدارة كلمات المرور "). يُذكر في هذا السّياق أنّ ملحقات إدارة كلمات المرور المزروعة في بنية المتصفح تعرضنا لخطر أكبر من قيام مهاجم بخداع متصفحك وبالتّالي الوصول لكافّة كلمات المرور الخاصة بك.
- ينبغي إزالة كافّة عمليات تسجيل الدخول المحفوظة وتعطيل خاصيّة إدارة كلمات المرور على المتصفّح: رابط.

التّحقّق من أذونات الوصول أو تشغيل الكاميرا والميكروفون وسائر الأذونات الّتي تطلبها المواقع

يمكن تشبيه الأذونات ببابٍ أو نافذة مشرّعة إلى بيتنا: بعبارة أخرى إن كان بإمكان سين من المواقع الويب الدخول، فقد يتمكن آخرون من ذلك أيضًا. لذا لا التّثبت من أن مواقع الويب التي تستخدمها

وتثق بها هي فقط التي لديها الإذن باستخدام الخصائص الحساسة مثل الكاميرا أو الميكروفون. قد تستخدم البرامج الضارة هذه الأذونات للسماح لشخص ما برؤية مكانك أو التّنصت عليك.

- وعليه علينا إدارة الأذونات التي لربما سبق وأن منحنها لسين وصاد من مواقع الويب المختلفة | رابط

تعطيل التشغيل مشغّل الفلاش (Flash) في كافّة المتصفحات

باختصار، الفلاش هي حزمة برمجيات تسهل على أي شخص تشغيل تعليمات برمجية ضارة على جهازك دون إذنك.

- يُمكنك التّعرف على آلية تعطيل الفلاش على متصف ال فيَرفُكس: رابط

التّحقّق من إعدادات حماية التتبع المطوّرة

تقوم ملفات تعريف الارتباط وأجهزة التتبع الأخرى بجمع تفاصيل عن هويتك ومكان تواجدك وما تصفحته عبر الإنترنت. لذا عليك التّفكير فيما قد يحدث إذا وقعت هذه الأشياء في أيدي خصومك، واتخذ هذه الخطوات للحد من احتمالات التّعقّب والتّتبع عبر الإنترنت.

- تحقق من الإعدادات الخاصة بك، على الأقل بتفعيل إعدادات الحمايّة المطوّرة من التّعقب والتّتبع: رابط، كما عليك التفكير بخيار تشديد هذه الإعدادات وما قد ينشأ عن ذلك من عدم تمكنك من الدّخول على الكثير من المواقع.

تعيين محرك البحث الافتراضي

تقوم محركات البحث مثل غوغل (Google) وبينغ (Bing) بإنشاء ملفات تعريف لمستخدميهما، وتتبع جهازك على وجه التحديد، بل وتشارك معلوماتك الشخصية مع أطراف ثالثة. بتعيين محرّك بحث افتراضي سيستخدم متصفحك محرك بحث واحد في كل مرّة تبحث فيها عن شيء عبر الإنترنت ما لم تُحدّد محرّك بحث آخر.

- وعليه علينا استخدام القوائم المنسدلة المُدرجة ضمن خيار "تخصيص هذه الأداة" للعثور على الإرشادات المناسبة لأجهزتنا على هذه الصفحات، بحيث:
  - نُعيّن محرك البحث الافتراضي الّذي نرتضيه: رابط
  - ونضيف ونزيل ما أردنا من محركات البحث: رابط

استخدام أدوات إضافيّة لتعزيز الحماية على المتصفح

بتصفحنا الإنترنت فإنّنا نتعرض لطيف من الأكواد البرمجية من مصادر مجهولة، وهذا هو أحد الأسباب التي تجعل صفحات الويب مرتعًا للغالبية العظمى من أفخاخ البرامج الخبيثة وبرامج التجسس. بالإضافة إلى ذلك، يستخدم الأشخاص الذين لديهم مواقع إلكترونيّة أو يعلنون عبر صفحات الويب "ملفات تعريف الارتباط،" وهي عبارة عن أجزاء صغيرة من المعلومات التي تتعقبنا في أثناء التصفح. الأهم من ذلك، أن مواقع الويب لا تشفر كل ما ترسله أو تستقبله منّا؛ حيث لا يستخدم بعضها بروتوكول نقل النص التشعبي الآمن (HTTPS).

وعليه، فإنّنا نوصي بتثبيت الأدوات والخصائص الإضافية للمتصفح للحماية من هذا الضّرب من مشكلات الأمان والخصوصية.

- يمكننا اختيار الخصائص الإضافية التي نريد تثبيتها وتحديد كيفية تكوينها، وفقًا لظروفنا واحتياجاتنا.

- في حال كنّا نستخدم حاسوب يديره شخص آخر (مثلًا في مقهى إنترنت أو في مكان العمل)، فقد يتعين علينا إجراء هذه التعديلات بوتيرة متكرّرة.
- التثبيت والتكوين:
  - غرير الخصوصية: https://privacybadger.org/
    - لماذا علينا تسليح متصفحنا به؟ يحظر هذا البرنامج أجهزة التتبع التي تجمع البيانات عن المكان الذي كنّا فيه عند اتصالنا بالإنترنت.
    - برنامج uBlock Origin
    - لماذا؟ يحظر الإعلانات وأجهزة التتبع، التي قد يكون بعضها ضارًا.
    - برنامج Cookie AutoDelete
    - لماذا؟ يحذف أدوات التتبع التي تجمع البيانات عن المكان الذي كنّا فيه عند اتصالنا بالإنترنت.
    - فيسبوك كونتينر (Facebook Container)
    - لماذا؟ يمنع منصّة فيسبوك من جمع البيانات عن المكان الذي كنّا فيه عند اتصالنا بالإنترنت وربطها بملفاتنا الشّخصيّة.
    - Zoom Redirector: لماذا؟ من خلال فتح روابط Zoom في متصفحك، تحافظ هذه الوظيفة الإضافية على المكالمة ضمن وسائل حماية متصفحك.
    - الخيار المتقدم: NoScript
    - تجدر الإشارة إلى أنّ خاصيّة NoScript كثيرًا ما تتسبب بأن تظهر الصّفحات الّتي نزورها فارغة أو معطّلة؛ لذا ينبغي التعرف على كيفية تكوين هذه الخاصيّة بدقّة لتقليل مثل هذه الأمور: رابط
    - لماذا؟ من الممكن أن يتمكن خصومنا من الوصول إلى أجهزة باستخدام أكوادٍ برمجية ضارة في برنامج نصي تم تنزيله مع صفحة الويب التي نتصفحها؛ في هذه الحالة، يعمل برنامج NoScript على حظر كل الأكواد البرمجية من مواقع الويب غير المعروفة، ما يحمي جهازك من التقاط برمجيات خبيثة وما شابهها.

إدارة الوظائف الإضافيّة والنوافذ المنبثقة عنها

قد يحاول المتربصون بنا خداعنا لتثبيت برامج خبيثة في شكل خصائص إضافية تُضاف على المتصفح. يمكنهم القيام بذلك باستخدام النّوافذ المنبثقة. لذا لا بدّ لنا من ضبط المتصفح لتفادي هذه الحيل والأشراك. بالإضافة إلى ذلك، علينا التّثبّت من تحديث الوظائف الإضافية التي نريدها، وإزالة تلك التي لا نستخدمها، فكما يفسد الطعام القديم، يمكن للأكواد القديمة أن تُضحي ثغرات وخلل برمجي ضار وخطِر. وعليه علينا:

- التّأكد من ضبط متصفح فيَرفُكس لحظر النوافذ المنبثقة وتحذيرنا بشأن أي خاصيّة أو برنامج يُراد تثبيته نتيجة لهذه النوافذ: رابط
- وتحديث الوظائف الإضافية بوتيرة تلقائية كلما توفّرت تحديثات لها: رابط؛ و-إزالة الإضافات غير المستخدمة | رابط

حذف سجل بيانات ومعلومات التّصفح

سجل التصفح الخاص بك هو قائمة بمواقع الويب التي قمت بزيارتها. الخيار الافتراضي في فيَرفُكس هو "تذكر سجل التصفح والتنزيل،"، مما يعني أن فيَرفُكس سيتذكر سجلّات ما نتصفح وننزّل ونبحث عنه، كما سيقبل ملفات تعريف الارتباط من مواقع الويب التي تزورها (تلك الجزئيات المعلوماتية التي تتتبع حركاتنا وسكناتنا عبر الإنترنت). تسمح ملفات تعريف الارتباط للمواقع المُزارة بتسجيل معلومات على أجهزتنا يرسلها فيَرفُكس إليهم وإلى شركائهم من معلنين.

من جهة أخرى، لسجل بيانات التّصفح هذا مزاياه أيضًا، مثلًا سيقترح متصفحك الصفحات التي قمت بزيارتها من قبل، لذلك لا يتعين عليك إعادة كتابة العناوين أو نقلك إلى مواقع ضارة. لكن هناك مقايضات، حيث إن تمكّن شخص ما من الوصول إلى سجل ما نتصفح على الإنترنت، فكأنما وقع على منجمٍ من المعلومات عنّا، وعن الأشخاص الذين نعمل معهم، والأشياء التي كنا نقرأ عنها وتهمّنا. وعليه علينا:

- مسح جميع ملفات تعريف الارتباط: رابط
- تعطيل ملفات تعريف الارتباط للجهات الخارجية: رابط
- إعداد زر أو خيار واحد بالنّقر عليه نمحي كل ملفات تعريف الارتباط وسجّل التّصفح، بكبسة زر كما يقال: رابط
- ضبط متصفح فيَرفُكس بحيث لا يتذكّر شيء من سجلّات تصفحنا أو تخصيص ما يتذكره وما ينساه: رابط
  - كذلك يمكننا حذف سجل التّصفح يدويًا: كيفيّة حذف سجل التّصفح: رابط
- في ذات السّياق، من الجدير أن نفكّر إذا ما كنّا نريد تغيير ما يقترحه المتصفح عند الكتابة في شريط العناوين؛ فذلك أيضًا بمقدورنا:
  - تغيير إعدادات شريط العناوين بحيث لا يقترح صفحات من سجل التصفح أو نتائج أخرى غير مرغوب فيها: رابط
  - إزالة المُقترحات الاستباقية: رابط

إمكانيّة تجنّب إظهار آخر ما تُصفّح عند بدء التشغيل

إذا كنت قلقًا من أنه سيتم الاستيلاء على جهازك أو تفتيشه، فأوقف تشغيل الميزة التي تعرض صفحات الويب التي قمت بفتحها عند آخر إغلاق للمتصفح.

قم بإيقاف ميزة استرجاع الجلسة السابقة: رابط

استخدام التصفح الخاص

يشير "التصفح الخاص" إلى وضعيّة تحول دون تتبع المتصفح لملفات تعريف الارتباط أو حفظ سجل التّصفح الخاص بنا، ويعد استخدامه طريقة سريعة لإخفاء بعض أنشطتنا إذا ضبطنا متصفحنا على أنّه من المقبول الاحتفاظ بسجل ما نتصفحه ونبحث عنه عبر الإنترنت. يمكن لهذه الخاصيّة أن تكون مفيدة جدًا إن كنّا نعيش مع شخص يهدّدنا ويمكنه الوصول إلى أجهزتنا، وعليه ينبغي لنا:

- تعميق فهمنا حيال ما لا يُمكن للتصفح الخاص حمايتنا منه: رابط، بما في ذلك منشوراتنا على وسائل التّواصل الاجتماعي، أو الملفات الّتي تقوم بتنزيلها، أو البرامج الخبيثة الّتي قد يضعها المتربصون بنا على أجهزتنا.
- تشغيل التصفح الخاص لجلسة معيّنة: رابط.
- التّفكير في خيار التّصفح الخاص في جميع الأوقات: رابط.

استخدام متصفح تور (Tor) أو نظام تايلز (Tails) أو الشّبكات الافتراضيّة الخاصّة الموثوقة (VPN)

يتيح لنا استخدام متصفح تور (Tor) أو نظام تايلز (Tails) أو عبر الشّبكات الافتراضيّة الخاصّة الموثوقة (VPN) زيارة الصّفحات الإلكترونيّة دون الكشف عن هويتنا أو موقعنا. في المقابل، إذا سجّلنا الدّخول إلى موقعٍ أو خدمة ما فإنّنا نُشاركها معلومات حساباتنا (وربما معلومات شخصية).
متصفح تايلز هو نظام تشغيل نستخدمه عوضًا عن نظام التشغيل المعتاد لحواسيبنا (نحو ويندوز، أو ماك، أو لينكس) لما يوفره من حماية لاتصالنا بالإنترنت عبر متصفح تور في جميع الأوقات. يتم تشغيله من محرك أقراص وحد نقل وتخزين بيانات متصل بأجهزتنا. يعمل نظام تايلز على مسح سجلّات التّصفح بمجرد بإيقاف تشغيله، ممّا يقلل من احتمالية "أخذ بصمات" أجهزتنا عن طريق المواقع التي نتصفحها، وشبكة الواي-فاي التي نستخدمها، والتطبيقات التي نثبتها على أجهزتنا، وعليه ينبغي لنا:

- مراجعة القسم الثّاني من المحور الثّالث من الفصل الثّاني: "استخدام الشبكات الافتراضية الخاصة" [رابط] بالإضافة لهذا الدليل (رابط) بشأن زيارة المواقع المحظورة، ومتصفح تور، والشّبكات الافتراضيّة الخاصّة، وغيرها من أدوات يمكنها حماية نشاطنا على الإنترنت من المتربصين به.
- وتعميق معرفتنا بنظام تايلز.
- والتّحقق مِمّا إذا كان استخدام هذه الأدوات في سياقنا آمنًا ومشروعًا.

2.4.2| تطبيقات المراسلة الآمنة

يستند محتوى هذا المحور على مادّة "الاتصال الخاص" المتاحة عبر منصّة دليل عدَّة الإسعاف الأوّلي الرّقمي: رابط.
يُمكن لخدمات الدردشة الوصول إلى المعلومات وجمعها عن موقعك، ونشاطك، ومحتواك، ومن نتحدث معهم؛ لذا حري بنا اختيار التّطبيق أو البرنامج الآمن لحماية سلامتنا.

استخدام تطبيقات المراسلة المشفرة تشفيرًا تامًا

توصيات بشأن أدوات الدّردشة ومكالمات الفيديو الآمنة والمُشفّرة تشفيرًا تامًا: رابط، لكن لا بدّ أن نعلم بأن جهات تقديم خدمات الإنترنت أو الهواتف الخاص بك قد تتمكن من الاطلاع على التطبيقات التي نستخدمها (لتجنب ذلك، علينا بالشبكات الافتراضية الخاصة؛ وللمزيد بهذا الخصوص يُمكن مراجعة القسم الثّاني من المحور الثّالث من الفصل الثاني: "استخدام الشبكات الافتراضية الخاصة").

- تطبيق سيغنال (Signal) (يعمل على أنظمة الأندرويد، والآي. أو. إس.، ولينكس، والماك، والويندوز): تطبيق مجاني ومفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة، والصّوتيّة، والمرئية، لكن يتطلب رقم هاتف صالح للتسجيل فيه.
- تطبيق إيليمنت (Element) (يعمل على أنظمة الأندرويد، والآي. أو. إس.، ولينكس، والماك، والويندوز): تطبيق مجاني ومفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة المشفرة تشفيرًا تامًا، ويوفر خاصية مشاركة الملفات للأفراد والمجموعات، يقدّم التّطبيق أيضًا خدمات المراسلة الصّوتية والمرئيّة، بل ويمكن للأفراد والمؤسسات ذات الخبرة استضافات خدمات هذا التّطبيق بنفسها. يستند إيليمنت على معيار الاتصال المصفوفي (Matrix Communication Standard).

- تطبيق دلتا (Delta) (يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز): تطبيق مجاني ومفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة بالاعتماد على جهات تقديم خدمات البُرد الإلكترونيّة لنقل البيانات، يُذكر أنّ دلتا لا يتطلّب إدخال رقم هاتف لاستخدامه على عكس تطبيقات واتس-آب، وسيغنال، وتيليجرام.
- تطبيق واير (Wire) (يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز): تطبيق مجاني (لكن تجاري) ومفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة بالاعتماد على جهات تقديم خدمات البُرد الإلكترونيّة لنقل البيانات، يُذكر أنّ دلتا لا يتطلّب إدخال رقم هاتف لاستخدامه على عكس تطبيقات واتس-آب، وسيغنال، وتيليجرام.
- إذا لم يكن استخدام التطبيقات المشفرة تشفيرًا تامًا ممكنًا، فحريٌّ بنا استخدام الخدمات الموصى بها والمُستضافة على خوادم موثوقة بواسطة مقدمي خدمات موثوقين (مثل Mattermost وRocketChat).
- في ذات السياق، يُمكننا الاطلاع على التوصيات التّالية بشأن الحفاظ على مجهولية الهوية في أثناء تصفح الإنترنت: رابط

تجنب الاحتفاظ بالمعلومات الحساسة التي لم نعد بحاجة إليها

ينبغي لنا التفكير بتلك الرسائل التي قد يعثر عليها شخص إن وصل إلى حساباتنا على خادم بُردنا الإلكترونية أو أجهزتنا. ما الذي قد تكشفه هذه الرسائل عن عملنا، أو وجهات نظرك، أو الجهات الّتي نتواصل معها؟ ينبغي لنا وزن هذه المخاطرة مقابل الاستفادة من إمكانية الوصول إلى بريدك الإلكتروني على أجهزة متعددة. يعد النسخ الاحتياطي لبُردنا الإلكترونية على جهاز مشفر إحدى الطرق للاحتفاظ برسائل البريد وحفظها بأمان، وعليه ينبغي لنا:

- استخدام خاصية الرّسائل المختفية واستخدامها على تطبيقات المراسلة حيثما أمكن ذلك.
- حذف الرسائل حيثما كان ذلك ممكنًا.

2.4.3| مؤتمرات ولقاءات الفيديو الآمنة

يستند محتوى هذا المحور على مادّة "استخدام تطبيقات الدّردشة المرئية والمسموعة على نحو أكثر أمنًا" المتاحة عبر منصّة دليل عدَّة الإسعاف الأوّلي الرّقمي: رابط

استخدم خدمات الفيديو والصوت والنّص المشفّرة تشفيرًا تامًا

إذا لم يكن استخدام التطبيقات المشفرة تشفيرًا تامًا ممكنًا، فحريٌّ بنا استخدام الخدمات الموصى بها والمُستضافة على خوادم موثوقة بواسطة مقدمي خدمات موثوقين.

- توصيات بشأن أدوات الدّردشة ومكالمات الفيديو الآمنة والمُشفّرة تشفيرًا تامًا: (رابط)، لكن لا بدّ أن نعلم بأن جهات تقديم خدمات الإنترنت أو الهواتف الخاص بك قد تتمكن من الاطلاع على التطبيقات التي نستخدمها (لتجنب ذلك، علينا بالشبكات الافتراضية الخاصة؛ وللمزيد بهذا الخصوص يُمكن مراجعة القسم الثّاني من المحور الثّالث من الفصل الثاني: "استخدام الشبكات الافتراضية الخاصة").
  - تطبيق جيتسي (Jitsi) (يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز): تطبيق مفتوح المصدر بإصدارين أحدهما مجاني والآخر مدفوع، يوفر خدمات آمنة

للدردشة الصّوتيّة والمرئية، ويمكن استخدامه على أنظمة لينكس وماك وويندوز عبر المتصفح . (يُجرى الاطلاع على دليلنا لأدوات الدّردشة ومؤتمرات الفيديو الجماعية الآمنة واستخدام المُستضاف منها على خوادم موثوق بها)، جدير بالذكر أنّه يمكن للأفراد والمنظمات التي تتمتع بالخبرة التقنية المناسبة استضافة خدمات جيتسي بأنفسهم.

- يذكر في هذا السّياق دليل فرونت لاين ديفندرز الخاص بهذا التّطبيق، والّذي يضم طيفًا من النّصائح العملية المفيدة لاستخدامٍ آمنٍ لهذا التّطبيق: رابط

- تطبيق بيغ بلو بَتِن (BigBlueButton) : تطبيق مفتوح المصدر بإصدارين أحدهما مجاني والآخر مدفوع، يعمل عبر متصفحات الإنترنت يوفر خدمات آمنة للدردشة الصّوتيّة والمرئية، يُذكر أنّه بإمكان الأفراد والمنظمات التي تمتلك الخبرة التقنية المناسبة استضافة خدمات هذا التّطبيق على خوادمها. صُمِّم هذا التّطبيق لغايات الجلسات التّدريبية عبر الإنترنت وضُفِّرَ بالكثير من المزايا الّتي تُحاكي متطلبات هذا السّياق (وثّم مقاطع فيديو تعليميّة عن كيفيّة استخدامه للمشاركين في الجلسات المنعقدة من خلاله وعبره كما ولنسقي هذه الجلسات والمشرفين عليها).

التّحكم في الأشخاص المتصلين بمكالمات الفيديو والمحادثات

لا تمنع الخدمات عبر الإنترنت الأشخاص من تسجيل الدخول إلى المكالمات أو الدردشات باستخدام أسماء غير أسمائهم. للتأكد من أن كل شخص من يدعي، لا بدّ من التّحقّق من هوياتهم قبل الخوض بأي تفاصيل حسّاسة.

في خضم جائحة الحمّى التّاجية كوفيد19، اكتشف الكثيرون أن من يسعى لإزعاجهم قد يتسلل إلى مكالمات الفيديو الخاصة بهم. تمنح صلاحيات المشرفين في كتم الصوت أو طرد المشاركين الفرصة لإتمام هذه المكالمات دون تدخل، وعليه ينبغي لنا:

- معرفة من نرسل إليه طلب مكالمة أو دعوة للدردشة، بما في ذلك:
  - التّثبّت من أرقام الهواتف أو عناوين البريد الإلكتروني التي نراسلها.
  - الإحجام عن مشاركة الدعوات على وسائل التواصل الاجتماعي العامة.
- قبل البدء بأي مكالمة، لا بدّ أن نلم بأدوات المسؤول أو المشرف التي تتيح لنا كتم صوت المشاركين غير المرغوب فيهم أو حظرهم أو إخراجهم. وبتالي علينا تهيئة هذه الأدوات بحيث لا يتمكن سوى المشرفين من كتم صوت مكالمات الفيديو وحظرها.
- عندما تبدأ مكالمة أو محادثة، لا تفترض أنك تعرف المتصل فقط من خلال قراءة اسمه. ليس من الصعب أن يقوم شخص ما بإدخال اسم شخص تعرفه كاسم المستخدم الخاص به، ويتظاهر بأنه هو، وعليه لا بدّ لنا من
  - التحقق من هويات جميع المشاركين في المكالمة من خلال مطالبتهم بالتحدث أو تشغيل الكاميرا الخاصة بهم.
  - التأكد من هويتهم عبر قناة أخرى (مثل الدردشة الآمنة أو البريد الإلكتروني) من أن الشخص المشارك في المكالمة هو بالفعل من يظهر اسمه على الشاشة.
  - التقاط لقطات شاشة أو سجل المشاركين غير المرغوب فيهم لجمع الأدلة لتحليلها لاحقًا واتخاذ الإجراءات القانونية.
  - طرد أي شخص لا ترغب في وجوده في المكالمة أو المحادثة.
- إذا لم ينجح طرد شخص ما أو حظره، فعليك بإنهاء المكالمة وبدء مكالمة جديدة لا وجود للشخص المزعج فيها. كذلك تحقق مرة أخرى من قائمة أرقام الهواتف أو عناوين البريد الإلكتروني التي

ترسل إليها، للتأكد من صحة نسبتها للأشخاص الذين تريد محادثتهم، واتصل بكل شخص عبر قناة أخرى للتحقّق من هويتهم (على سبيل المثال، عبر مكالمة هاتفية إذا كنت تعتقد أن عنوان بريده الإلكتروني غير صحيح).

تغيير مكالمات الفيديو إلى الميكروفون وتعطيل التفعيل التلقائي للكاميرا

- افترض أنه عند الاتصال، قد يتم تشغيل الكاميرا والميكروفون بشكل تلقائي، لذا تحقق من هذا الإعدادات، وكن حذرًا فيما تظهره وتقوله إلى أن تتثبت من إلغاء تفعيل الكاميرا.
- فكر في تغطية الكاميرا بملصق أو ضمادة لاصقة، وقم بإزالتها فقط عند استخدام الكاميرا.
- فكر في خيار تعطيل الميكروفون والكاميرا من خلال إعدادات الجهاز إن لم نتمكن من إيقاف تشغيلهما خلال استخدام الخدمة قبل الاتصال.

وضع قواعد لالتقاط الصّور خلال مكالمات الفيديو والمشاركة فيها

إذا كان المشاركون في المكالمة قلقين على سلامتهم، فإن تسجيل مشاركتهم في المكالمة قد يعرضهم لخطر تحديد موقعهم وانتمائهم إلى مجموعتك؛ وعليه لا بدّ لك من إرساء قواعد أساسية مسبقًا بشأن الكاميرات والميكروفونات إذا كان ذلك يشكل خطرًا. تذكر أن القواعد الأساسية ليست كفيلة بمنع أي شخص من تسجيل المكالمة.

يمكن أن تضمن اجتماعًا أسلس وأقل إرهاقًا من خلال إرساء القواعد المتعلقة بإيقاف تشغيل الميكروفونات بمجرد التوقف عن الحديث وكيفية تبادل الأدوار، وعليه ينبغي:

- الاتفاق على القواعد الأساسية قبل بدء الاجتماع، بما في ذلك، على سبيل التمثيل لا الحصر:
  - ما إذا كان المشاركون سيستخدمون أسماءهم الحقيقية أم أسماء مستعارة
  - وما إذا كنت ستبقي الكاميرات الخاصة بك قيد التشغيل أم لا
  - وما إذا كان المشاركون سيبقون بميكروفوناتهم قيد التشغيل أو إيقافها عند عدم التحدث،
  - وكيف سيعبّر المشاركون عن رغبتهم في التحدث وإدلاء مداخلاتهم
  - من الذي سيقود الاجتماع
  - من سيقوم بتدوين الملاحظات، وأين، وما إذا كان سيتم كتابة هذه الملاحظات وتوزيعها، وما إذا كان من المقبول التقاط لقطات شاشة لمكالمة الفيديو أو تسجيلها، إلخ.

استخدام سماعات الرأس أو الأذنين

يضمن استخدام سماعات رأس أو سماعات الأذن للحؤول دون تمكّن من يجلس بجوارك من استراق السّمع على محادثتك، لا سيّما ما يقوله الآخرون في المكالمة (على الرغم من أنه سيكون قادرًا على سماعك بالطبع).

التّحقق ممّا يمكن رؤيته وسماعه

هل تعلم أنّ بعض المدافعين عن حقوق الإنسان قدّ تمكّن المتربصين بهم من التّعرف على ماكنهم مما تمكنوا من رؤيته وسماعه في خلفية مكالمات فيديو هؤلاء المدافعين، وعليه لا بدّ لنا من التّالي للحفاظ على أمننا ومن معنا:

- التيقظ لما يظهر في خلفية الفيديو الخاص بنا، ومن وماذا يوجد في الإطار. فقد لا نرغب في الكشف

2.5| حماية البيانات

مُقدِّمة: ما زاد عن حدّه انقلب ضدّه| مبدأ ترشيد جمع البيانات والحد منه

مع تزايد كمية البيانات التي نجمعها ونخزنها، تتعاظم حاجتنا إلى تعزيز حمايتها. فضلاً عن التزاماتنا القانونية بصفتنا منظمات مجتمع مدني بموجب القوانين الوطنية أو الاتفاقيات الإقليمية لحماية البيانات، من الضروري الانتباه لتأثير هذه البيانات علينا وعلى مجتمعاتنا في حالة تسربها أو استغلال خصومنا لها ضدّنا.

- يمكنّنا بناء تصوّر عام عن البيانات التي نحتفظ بها وأين وكيف نحميها عبر بناء خريطة معلوماتيّة: رابط
- كذلك يُمكن تقليل ما نجمع من معلومات بتدبر إذا ما كانت هناك ما يُسوّغ جمعها واستخدامها—تلك المعلومات الّتي نجمعها من خلال الاستطلاعات أو عمليّات تسجيل للمشاركة.
- أيضًا، يُمكن لتصنيف البيانات أن يُعيننا تحديد أي المعلومات الّتي علينا حمايتها وكيف، بتصنيفها مثلًا إلى معلومات عامّة، أو داخلية، أو سريّة، أو باستخدام بروتوكول الإشارة الضّوئيّة (Traffic Light Protocol).

2.5.1| حماية البيانات

يستند محتوى هذا القسم على مادّة "سُبل حماية البيانات الحسّاسة" المتاحة عبر منصّة عُدَّة الأمان، أدوات و ممارسات للأمان الرقمي: رابط
قد تتمكّن الجهات المُخترقة من قراءة بياناتنا أو تعديلها عن بعد—عبر الإنترنت. أمّا إن وضعوا أيديهم على أجهزتنا، فقد يتمكنون من قراءة بياناتنا أو تعديلها بأصابعهم! لذا؛ يُفضّل أن نُحصّن أجهزتنا بعدّة خطوط دفاع لتفادي هذه الخروقات المُحتملة؛ يسوقنا ذلك لتقنيّة تشفير الملفات المحفوظة على أجهزتنا باعتباره أحد أشكال الحماية الفاعلة.
يُعرّف التّشفير بأنّه وسيلة تستخدمها البرمجيات لتشفير معلوماتنا عبر توظيف عمليات رياضيّة معقّدة، ينشأ عن هذه العمليات مفتاح لفك التّشفير لا يملكه سوانا (في شكل كلمة مرور أو مفتاح تشفير). بعبارة أخرى، يُمكننا تشبيه التّشفير بحفظ معلوماتنا في خزانة موصدة بعدّة أقفال لا يملك مفاتيحها سوانا.
فيما يلي جُملةً من الخطوات الّتي يُمكن أن تساعدنا على حماية ما نحفظه من بياناتٍ على أجهزتنا:

خيار حذف البيانات القديمة بدلًا من تخزينها

قد يشكل حفظ البيانات السّرية خطرًا علينا وعلى من نعمل معهم. يقلل التّشفير من هذا الخطر؛ لكنه لا يزيله. تتمثّل الخطوة الأولى لحماية البيانات الحسّاسة بتقليل كمية المعلومات التي تحتفظ بها. ما لم يكن لدينا سبب وجيه لحفظ ملف معين، أو فئة معيّنة من المعلومات في ملف، علينا ببساطة حذفه (لمزيد من المعلومات بشأن كيفية القيام بذلك على نحوٍ آمن، يُمكن مراجعة الفصل 2.5.3 إتلاف البيانات).

هل التّشفير غير قانوني أو مشبوه وفقًا للتشريعات السّارية علينا؟

- في الواقع، تُدرج بعض الدّول التّشفير ضمن اللّامشروعات؛ بالتّالي إن كنّا نعيش في أحد هذه البلدان، قد ينتهي بنا تنزيل برامج التشفير أو تثبيتها أو استخدامها للإدانة والتّجريم، حيث قد تتذرّع أجهزة الشّرطة، أو الجيش، أو المخابرات باستخدامنا لبرامج التشفير لتحري أنشطتنا أو اضطهاد مؤسّساتنا.
- بغض النّظر عمّا تحويه ملفّاتنا المشفّرة، أو بغض النّظر عن قانونيّة ذلك حسب التّشريعات السّارية، فإنّ استخدام برامج التّشفير قد يكون كفيلًا بإثارة الشّكوك حول مستخدمها؛ لذا علينا التّحقّق من كيفية تعامل جهات إنفاذ القانون مع التّشفير في حيث نعيش، كما علينا التّفكير مليًا إذا ما كانت أدوات تشفير البيانات مناسبة لسياقنا.

إن لم يكن التّشفير خيارًا مشروعًا، علينا أخذ البدائل التّالية بعين الاعتبار:

حفظ المعلومات غير الحسّاسة فقط

- إن تعذّر علينا حفظ المعلومات الحسّاسة، يجب علينا التّثبت من حفظ بعض المعلومات غير الحسّاسة، إذ قد تثير الأجهزة الفارغة من أي بيانات ريبة وشكوك خاصّة في خضم المداهمات ومصادرة الأجهزة.

- نقصد بنظام الكلمات الرّمزية أحد أشكال إخفاء المعلومات، بحيث نُخزّن ملفاتنا بشكل طبيعي، لكن باستخدام كلمات رمزيّة لتورية الأسماء والمواقع والأنشطة الحسّاسة وما إلى ذلك.

حفظ البيانات على أقراص مشفّرة غير ثابتة

- يمكننا الاحتفاظ بالمعلومات الحسّاسة في منأى عن حواسبنا عن طريق حفظها على وحدات نقل وتخزين البيانات (USB) أو محرك أقراص ثابت محمول. لكن تجدر الإشارة إلى أنّ مثل هذه الأجهزة عادة ما تكون أكثر عرضة من الحواسيب للفقدان والمصادرة؛ لذا فإن حفظ معلومات حسّاسة وغير مشفّرة عليها ليس بالفكرة السّديدة عادةً.

حفظ المعلومات على حساب سحابي مشفر

- يُمكننا النّظر في خيار خدمات التّخزين السّحابيّة المشفّرة مثل Tresorit لمواجهة ما يساورنا من مخاطر. على حين أنّه يُمكن لهذا الخيار أن يحمي بياناتنا باستخدام التّشفير، وذلك بتخزين بياناتنا على خوادم يصعب على خصومنا الوصول إليها، وإن كان بإمكانهم النّفاذ إلى تلك الخوادم، سيكون لديهم المزيد من الوقت لمحاولة اختراق بياناتنا، يُضاف إلى ذلك، أنهم سيكونون قادرين على اختراق بياناتنا دون أن ندري أو نشعر بذلك.

خيار التّشفير الكامل لأجهزتنا

في حال سرقة أو استيلاء أشخاص على أجهزتنا بغية الاطلاع على ملفاتنا واتصالاتنا، فلا بدّ لنا من وسائل حماية لإيقافهم، وهذا يسوقنا لخيار التّشفير الكامل لأجهزتنا.
قد تحتوي الحواسيب المكتبيّة والمحمولة على خيارات تشفير ضمنيّة. كذلك يمكن أن يوفر برماج فيرا-كربت (VeraCrypt) حماية إضافيّة لملفات معيّنة، كذلك الأمر بالنّسبة لمحركات الأقراص الخارجيّة— أو يمكنّنا اللّجوء لتشفير الجهاز كاملًا، إن ارتأينا ذلك.

- تجدر الإشارة هنا إلى أنّ التّشفير الكامل للقرص لا يعمل إلّا إذا كان جهازنا مُطفأ بالكامل، وليس في وضع السكون (المعروف أيضًا باسم بالتعليق أو الإسبات). إذ إن كان قيد التّشغيل فقد يجد الشخص المستحوذ على جهازنا سهولة أكبر في اختراق ملفاتنا واتصالاتنا.

نظام تشغيل الAndroid

يمكن تشفير معظم الهواتف العاملة بنظام تشغيل Android الإصدار السّادس وما تلاه. للتحقّق من ذلك، علينا الذّهاب إلى الإعدادات ثُم إعدادات الأمان، ثم التّشفير وبيانات الاعتماد، بعد ذلك نبحث عن التّشفير أو تشفير الهاتف. يرجى ملاحظة أنّ خيارات الإعدادات قد تتباين من هاتف لآخر.

نظام تشغيل الآي. أو. اِس (iOS)

تُشفَّر أجهزة الآي-فون (iPhone) افتراضيا بمجرّد تعيين رمز الدّخول: رابط

نظام تشغيل لينكس (Linux)

- للتشفير باستخدام النّظام الضّمني لنظام تشغيل الجهاز:
  - لا يمكننا إتمام التّشفير الكامل للقرص الصّلب إلّا بتثبيت أوبونتو (Ubuntu) على حاسوبنا المحمول للمرّة الأولى، لذا قد نحتاج إلى إعادة التثبيت. لكن قبل أن نفعل ذلك لا بدّ لنا من:
  - الاحتفاظ بنسخة احتياطيّة بجميع بياناتنا، حيث أنّه بمجرد تثبيت نظام تشغيل أوبونتو سيحل محل جميع البيانات المخزّنة على نظام التّشغيل السّابق.
  - نُبق الجهاز متصلًا بالإنترنت كي نضمن الحصول على آخر التّحديثات في أثناء تثبيت نظام أوبونتو. إذا لم نكن متصلين بالإنترنت، سيتعيّن علينا تحديد شبكة لاسلكيّة إن توفرت. كذلك، علينا إنشاء وحدة نقل وتخزين البيانات يُمكن استخدامها على الحاسوب. لإرشادات عن كيفية إنشاء مثل هذه الوحدات، يُمكننا الاطلاع على دليل نظام أوبونتو:
    - كيفيّة إنشاء وحدة نقل وتخزين البيانات يُمكن استخدامها على حاسوب يعمل بنظام ويندوز: رابط
    - كيفيّة إنشاء وحدة نقل وتخزين البيانات يُمكن استخدامها على حاسوب يعمل بنظام ماك أو. اِس. اِكس: رابط
    - كيفيّة إنشاء وحدة نقل وتخزين البيانات يُمكن استخدامها على حاسوب يعمل بنظام أوبونتو: رابط
    - ثم نُفعّل خاصيّة خزنة الملفات المضمّنة لنظام التّشغيل لتشفير قرص حاسوبنا كاملًا من ألفه إلى يائه: رابط
    - يُمكننا الوصول إلى هذه الخاصيّة بتتبع المسار التّالي: إعدادات النظام > الخصوصية والأمن في الشريط الجانبي > خزنة الملفات، ثُمّ نفعّلها لتشفير قرص الحاسوب بذات كلمة المرور الّتي نستخدمها لتسجيل الدّخول.

نظام تشغيل ماك (Mac)

- أولًا نصل حاسبونا بمقبس كهربائي كي نضمن ألّا يكف عن التّشغيل في أثناء التّثبيت.
- اتباع الاشرادات التالية للتشفير باستخدام Filevault

نظام تشغيل ويندوز (Windows)

إن كانت حواسيبنا تعمل بنظام ويندوز، يُمكننا تشفير أقراصها كما يلي:
التّشفير باستخدام خاصيةBitLocker المُضمَّنة لنظام التّشغيل: رابط
لتشفير الأجهزة القديمة، يُمكننا الإفادة من المعلومات الواردة في الرّابط.
إذا قفزت أمامنا رسالة مفادها "لا يمكن لهذا الجهاز استخدام الوحدة النمطية للنظام الأساسي الموثوق به،" فذلك يعني أن حاسبونا يفتقر لوحدة نمطيّة للنظام الأساسي الموثوق به (Trusted Platform Module) المستخدمة للتشفير. مع ذلك، يمكننا من خلال تعديلات التكوين التّالية، لا يزال من الممكن استخدام BitLocker على الحواسيب الّتي تفتقر لوحدة نمطيّة للنظام الأساسي الموثوق به:

- الخطوة الأولى: نختر ابدأ ثم نتوجه إلى تشغيل، ثم نكتب GPEDIT.MSC في مربع فتح، ثم ننقر فوق موافق. ستظهر لنا نافذة أخرى ننقر على محرّكات نظام التّشغيل.
- الخطوة الثّانية: الآن نختار بنقرتين اثنتين على "المطالبة بخطوات مصادقة إضافيّة عند بدء التّشغيل،" ما سيقودنا إلى نافذة جديدة. (ملاحظة: ثمّ خيار للمطالبة بخطوات مصادقة إضافيّة عند بدء التّشغيل لا نريد المطالبة بها (خادم ويندوز 2008 وويندوز فيستا).
- الخطوة الثّالثة: نختار "تفعيل" مع التّثبّت من أنّ الخيار المفعّل هو خيار تفعيل BitLocker دون وحدة نمطيّة للنظام الأساسي الموثوق به متوافقة معه، وهو الخيار الّذي يتطلّب كلمة مرور أو رمز لبدء التّشغيل يُحفظ على وحدة نقل وتخزين البيانات، ثُم ننقر موافق.
- الخطوة الرّابعة: نغلق نافذة محرّر المجموعة.
- الخطوة الخامسة: تشغيل تشفير الأجهزة: رابط

خيار تشفير بعض ملفاتنا

قد يكون من المفيد ترك الملفات غير الحسّاسة على جهازنا غير مشفّرة، بحيث إذا تم تفتيش جهازنا، لا يبدو جهازنا مشبوهًا لأنه يحتوي على ملفات واتصالات يوميّة عاديّة. في هذه الحالة، نُشفّر بعض ملفاتنا ونترك بعضها الآخر غير مشفّر.
أنظمة تشغيل لينكس، وماك، وويندوز
تحميل برنامج فيرا-كربت
كيفية استخدام فيرا-كربت

التّفكير بخيار المُجلّد(ات) المخفي(ة)

بتشفير معلوماتنا نحول دون تمكّن غيرنا من قراءتها، لكنّ ذلك لا ينفي استحالة تمكّن أحدهم من الاطلاع على بياناتك المشفّرة، رغم أنّنا اتخذنا خطوات لحمايتها. قد يحاول هذا الخصم بعد ذلك تخويفنا أو ابتزازنا أو استجوابنا أو تعذيبنا لحملنا على فك هذا التشفير. يمنحنا برنامج فيرا-كربت الفرصة لتجنب هذه المخاطر عن طريق إنشاء "مجلد مخفي." يمكننا فتح مجلد فيرا-كربت المخفي باستخدام كلمة مرور مختلفة عن تلك التي نستخدمها عادة. بهذه الحالة، إذا تمكّن متسلّل لديه تقنيات متقدّمة من الوصول إلى ملفاتنا المشفّرة "غير المخفيّة" لن يتمكّن من إثبات وجود ملفات مخفية.
تعمل تقنية الفيرا-كربت بإخفاء معلوماتنا المشفّرة في صورة بيانات مخفية أخرى أقل حساسيّة (مثل ملفات الموسيقى أو المستندات العادية)، بحيث ينزع عنها صفة الغرابة. يعتبر بشكل عام من المستحيل معرفة ما إذا كان المجلد المشفّر يحتوي على مجلد مخفي أم لا. لذا، إذا سرق أحد المتطفلين مفتاحنا،

أو أحالنا إلى المحكمة، أو أرهبنا كي نتخلّى عن كلمة المرور الخاصة بنا، فسوف يجد مواد "تمويهية" مقنعة، ولكن ليس المعلومات التي نحميها بواسطة الملفّات المخفيّة.
يُشبه استخدام تقنية الفيرا-كربت خزنة مقفلة بقاعٍ زائف، حيث لا يعرف أحد أن خزنتنا تحتوي على حجرة مخفية. يتيح لنا ذلك إنكار احتفاظنا بأي أسرار خلاف ما وضعنا بين أيدي خصمنا، وقد يساعد في حمايتنا في المواقف الّتي يتعين علينا فيها الكشف عن كلمة المرور خاصّتنا. يمنحنا هذا فرصة للفرار من المآزق الّتي تنشي على احتمالات خطرة. مع كل ذلك، إن قُبض علينا وعُثر على الخزنة فشكوك خصومنا ستزيد.
أمر آخر، قد يكون خصمنا على علمٍ ببرنامج فيرا-كربت ومقدرته على إخفاء المعلومات؛ بصيغة أخرى، ليس هنالك ما يضمن أنّ خصمنا سيسلّم لنا بمجرّد أن نُعطيه مفتاح البوابة الأولى! تجدر الإشارة إلى أن الكثير من الأشخاص يستخدمون فيرا-كربت دون اللجوء للمجلدات المخفية.
يجب علينا أيضًا التأكد من عدم الكشف عن المجلد المخفي عن طريق الخطأ عن طريق تركه مفتوحًا أو السماح للتطبيقات الأخرى بإنشاء اختصارات للملفات التي يحتوي عليها.

حماية محرك الأقراص المشفّر الخاص بنا

إلغاء التّثبيت

عندما يتم تركيب مجلد ڤيراكربت خفي، بمعنى آخر، عندما نلج إلى محتويات مجلد مخفي، فإن بياناتنا تكون معرضة للخطر. أبقه غير مثبت عندما لا نقوم بقراءة أو تعديل الملفات الموجودة بداخله بشكل فعال.
إذا كنّا نحتفظ بوحدة تخزين مشفّرة على وحدة نقل وتخزين البيانات، علينا تَذَكُّر أنّ مجرد فصل وحدة النّقل والتّخزين لن يخفي رمز الوحدة من النّظام بمجرد الخروج منها، بل قد يؤدي قطع الاتصال إلى إتلاف ملف الصوت الموجود على الوحدة، لذا لا بدّ لنا من إلغاء تثبيت المحرك في ڤيراكربت أولًا، ثم إخراج الوحدة من نظام التشغيل، وصولًا إلى فصل الجهاز عن الحاسوب. يُذكر هنا أنّ إلغاء تحميل وحدة النّقل والتخزين يتطلّب إغلاق جميع الملفات التي تم النّفاذ إليها. لذا، إذا عدّلنا مستندًا أو اِطّلعنا على صورة، ينبغي لنا إغلاق تلك الملفات أو إغلاق البرامج قبل إلغاء التّثبيت. نصيحة: لا بدّ من التّدرّب على ذلك مرارًا لاعتياد القيام به بسهولة في حالة الطّوارئ.

علينا فصل مُحرّك الأقراص قبل

- أن نبتعد عن أجهزتنا لأي فترة من الوقت؛ فذلك يضمن عدم ترك ملفاتنا الحسّاسة في متناول المتسللين الفعليين أو البعيدين.
- وضع حواسيبنا في وضعيّة السكون (المعروف أيضًا باسم "التعليق المرحلي" أو "الإسبات")، وذلك إمّا عن طريق تحديد هذا الخيار أو عن طريق إغلاق جهاز الحاسوب المحمول.
- السّماح لشخص آخر بالتعامل مع حاسوبنا، مثلًا عند المرور عبر نقطة تفتيش أمنية أو معبر حدودي، من المهم أن نقوم بفصل جميع وحدات التخزين المشفّرة وإغلاق حاسوبنا إغلاقًا تامًا.
- وصل وحدة نقل وتخزين بيانات أو أي جهاز تخزين خارجي آخر غير موثوق به، بما في ذلك أجهزة الأصدقاء والزّملاء.

إياك ووصل مُحرّك الأقراص المشفر الخاص بك على جهاز لا تثق به

بناء على مجاز الخزنة المقفلة، وبغض النّظر عن مدى قوّة خزنتنا، فلن يفيدنا كثيرًا إذا تركنا بابها مُشرّعًا. لذا علينا بهذه الخطوات لحماية محرّكات الأقراص الخاص المُشفّرة الخاصّة بنا. يُمكننا اللّجوء إلى المشتغلين بمحال ومراكز التقانة وتصليحات الأجهزة الموثوق بها.

ربما قام أحد المتربصين بينا بتثبيت برامج ضارة للتجسس على جهاز لا يقع تحت سيطرتنا، مثل جهاز حاسوب في مقهى إنترنت، بحيث يعملون على سرقة كلمات المرور الخاصّة بنا للوصول إلى محرّكات الأقراص المشفّرة أو المواد الحسّاسة الأخرى المحفوظة على أجهزتنا.

الاستفادة من خدمات محال أجهزة تقانة المعلومات ومراكز التّصليح الموثوقة

عندما نحصل أو نبتاع جهازاً مستعملاً، أو نُرسل جهازنا للتصليح، فإنّنا نُعطي خصومنا فرصة للاطلاع على ملفاتنا. لسوء الحظ، قد تحمل الأجهزة المستعملة برامج ضارة أو برامج تجسس، لذا من الأفضل شراء جهاز جديد إن أمكن. من المعروف أحيانًا أن بعض محلات الإصلاح تتجسس على الأجهزة أو تنسخ بياناتها وتبيعها. لذا علينا ألّا نقصد أي مراكز تصليح لا نثق بخدماتها.

- إذا اشترينا جهازًا مستعملًا، لا بدّ أن نلجأ لشخصٍ نثق به لتنظيفه والتحقق من خلوه من أي برامج خبيثة.
- إن ساورك شك بأن شخصًا ما قد يكون لديه النّفاذ أو الموارد أو الدافع لاستهدافك عن طريق تثبيت برامج خبيثة على جهازك قبل شرائه، فلا بدّ من تجنّبه واختيار وكيل معتمد عشوائيا.

2.5.2| النسخ الاحتياطيّة واستعادة البيانات

يستند محتوى هذا القسم على مادّة "النّسخ الاحتياطية سبيلًا لاستعادة المعلومات المفقودة" المتاحة عبر منصّة عُدَّة الأمان، أدوات و ممارسات للأمان الرقمي: رابط
ثمَّ مقولة شائعة بين متخصصي خدمات الدّعم الحاسوبي مفادها أنّ "فقدان بياناتنا شرّ لا بدّ منه، لكن السّؤال متى." إن سُرقت أجهزتنا أو استولى عليها أحدهم أو تَلِفت، فإنّ ذلك لا ينفي حاجتنا للولوج إلى ما لنا فيها من مستندات مهمة. في هذا السّياق، يُشكّل التخطيط المسبق عاملًا مهمًّا لتقليل الخسائر. للخروج بتخطيط سديد يُمكننا الاستفادة من الخطوات التّالية:
كذلك يُمكننا الاستفادة من محور "ضاعت بياناتي" في دليل عدَّة الإسعاف الأوّلي الرّقمي: رابط

استعادة المعلومات المحذوفة أو المفقودة

عندما نحذف ملفاً ما فإنّنا لا نعود نراه لكنّه لا يتبخر من جهازنا. حتى بعد إفراغ سلّة المحذوفات أو سلّة المهملات، يمكن عادةً العثور على الملفات الّتي حذفناها على القرص الصلب. لمعرفة كيف يمكن أن يؤدي ذلك إلى تعريض أماننا للخطر، يُمكنك الاطلاع على القسم الثّالث من المحور الخامس من الفصل الثّاني (2.5.3) إتلاف رابط البيانات.
لكن أحيانًا يكون بعض الشّر خيراً، فقد نحذف ملفًا مهمًا دون قصد ويكون ذلك لصالحنا. مؤخرًا بات شائعًا تمكين البرامج لخيار استعادة الملفات المحذوفة.

جميع الأجهزة

بادئ ذي بدء لا تعمل هذه الأدوات إن كتب جهازنا بيانات جديدة فوق البيانات المحذوفة. بتالي علينا التّوقّف عن استخدام جهازنا إلى أن ننتهي من استعادة ملفّاتنا أو اللّجوء إلى شخص آخر للقيام بذلك نيابةً عنّا. قد تسفر مواصلة استخدامنا لجهازنا عن الكتابة فوق الملفات التي فقدناها وتجعل استرجاعها ضربًا من المُحال. كلما طالت فترة استخدامنا لحاسوبنا قبل محاولة استعادة المفقودات، قلّت احتمالية نجاتها واسترجاعها.
لهذا الغرض، يُمكننا استخدام النسخة المحمولة من أداة مثل Recuva بدلاً من تثبيتها. قد يؤدي تثبيت البرنامج إلى الكتابة على الملف الذي نحاول استعادته عن طريق الخطأ.

أنظمة تشغيل لينكس، وماك، ووينـدوز

يُمكننا تجريب أداتي TestDisk وPhotoRec https://www.cgsecurity.org/wiki/؛ يُمكنك الاطلاع على الدّليل الكامل للأداة الأولى عبر الرّابط.

ويندوز

يُمكننا تجريب أداة Recuva

إنشاء خطة للنسخ الاحتياطيّة

للتخطيط المسبق للإبقاء على نسخ احتياطيّة من بياناتنا، علينا بالخطوات التّالية:

تنظيم المعلومات

قبل إنشاء خطة النسخ الاحتياطي، علينا نقل كافّة المجلدات الّتي تحتوي على المستندات الإلكترونية التي ننوي عمل نسخة احتياطيّة منها في مكان واحد، مثلًا داخل مجلد "الوثائق" أو "وثائقي".

تحديد أين وما هي المعلومات الخاصة بك

الخطوة الأولى لبناء خطّة ناجعة للنسخ الاحتياطية هي تحديد المكان الرّاهن لمعلوماتنا الشخصية ومعلومات العمل. بريدنا الإلكتروني، على سبيل المثال، قد يتم تخزينه على خادم مزود البريد الإلكتروني الخاص بنا، أو على حواسيبنا، أو في كلا المكانين في ذات الوقت. بطبيعة الحال، قد يكون لدينا العديد من البُرد الإلكترونيّة.

ثم هناك مستندات مهمة على الحواسيب التي نستخدمها في المكتب أو في المنزل: مثل مستندات معالجة النصوص، والعروض التقديمية، وملفات PDF، وجداول البيانات. من جهة أخرى، تخزّن أجهزتنا، سواء الحواسيب أو المحمولات، قوائم الجهات الّتي نتصل بها، وسجلات الدردشة، وإعدادات البرامج الشخصية، وجميعها قد تندرج في خانة البيانات الحسّاسة.

ربما نكون قد قمنا أيضًا بتخزين بعض المعلومات على وسائط غير ثابتة مثل وحد نقل وتخزين البيانات أو محركات الأقراص الثابتة المحمولة أو الأقراص المضغوطة أو أقراص الدي. في. دي إذا كان لدينا موقع ويب، فقد يحتوي على مجموعة كبيرة من المقالات التي كتبناها على مدار سنين طِوال. أخيرًا وليس آخِرًا، لا بدَّ ألّا ننسى المعلومات غير الرّقميّة، مثل الدّفاتر الورقية، والمذكرات، والرّسائل.

تحديد النّسخ الأوّليّة والنّسخ المكرّرة

عند إجراء نسخ احتياطيّة من الملفات، ينبغي أحيانًا استخدام القاعدة 1-2-3، إي علينا الاحتفاظ بثلاث نسخ على الأقل من أي معلومات، في مكانين على الأقل، مع نسخة واحدة على الأقل في مكان مختلف عن النّسخة الأصليّة.

قبل البدء في عمل النسخ الاحتياطية، حريٌّ بنا تحديد أيّ الملفات التي جمّعناها تندرج ضمن خانة النسخ الأوّليّة وأيُّها يندرج ضمن خانة النسخ المكرّرة. يجب أن تكون النسخة الأوّلية هي الإصدار الأحدث من ملف معين أو مجموعة ملفات معيّنة؛ بعبارة أخرى يجب أن تكون النّسخة الّتي سنبني على ما وصلت إليه إذا كنّا بحاجة تحريرها أو تحديثها أو تعديلها. ومن الواضح أن هذه الجزئية لا تنطبق على الملفات التي لدينا نسخة واحدة منها فقط، لكنها مهمة جدًا بالنّسبة لأنواع أخرى من المعلومات.

أحد السيناريوهات الكارثية الشائعة تحدث عند الاحتفاظ بنسخة احتياطية من النسخ المكررة من مستند مهم، حين تُفقد النسخة الأساسية نفسها أو تُتلَف قبل أن يتم تحديث النسخ المكرّرة. على سبيل المثال، لنفترض أنك سافرت لمدة أسبوع لتحديث نسخة من جدول بيانات مهم مخزّن على وحدة نقل وتخزين بيانات، لا بدّ من اعتبار تلك النّسخة بأنّها الأساسية، لأنها أحدث من النسخ الاحتياطية التي لربما تكون/ين قد أن أنشتها في المكتب.

علينا توثيق مكان جميع النّسخ الأولية والمكرّرة من المعلومات المحدّدة أعلاه. سيساعدنا ذلك في توضيح احتياجاتنا والبدء في تحديد سياسة النسخ الاحتياطيّة الأنسب لنا. يقدّم لنا الجدول أدناه مثال مبدئي، إذ قد تكون قوائمنا أطول بكثير، وتحتوي على بعض أجهزة التخزين مع أكثر من نوع بيانات أو أنواع بيانات مخزنة على أجهزة متعددة.

نوع البيانات	أوّلية/مُكرّرة	جهاز الحفظ/التّخزين	مكان الحفظ
ملفّات بحثيّة	أوّليّة	مُحركّ قرص الحاسوب	المكتب
انتهاكات حقوق الإنسان: ملف الشّهادات	مكرّرة	وحدة نقل وتخزين بيانات	بحوزتي
قواعد بيانات البرامج (صور، وسجل عناوين، ورزنامة العمل، إلخ)	أوّليّة	مُحركّ قرص الحاسوب	المكتب
بعض الوثائق الّتي تمّت مُشاركتها	مكرّرة	الخادم الخاص بالمكتب	المكتب
بضع الوثائق الإلكترونيّة	مكرّرة	قرص صلب	المنزل
البريد الإلكتروني وجهات التّواصل عبر البريد الإلكتروني	أوّليّة	حساب الGmail	الإنترنت
رسائل نصيّة وسجلات جهات الاتصال	أوّليّة	الهاتف المحمول	بحوزتي
المطبوعات (عقود، وفواتير، إلخ)	أوّليّة	دولاب مكتبي	المكتب

يُمكننا أنّ نستشف من الجدول أعلاه التّالي:

- المستندات الأكثر أمانًا في حالة تعرض الحاسوب المكتبي لأعطال، هي تلك الموجودة على وحدات نقل وتخزين البيانات، بالإضافة إلى المستندات المشتركة على الخوادم. هذه الطريقة تضمن بقاء النسخ المكررة من المستندات محفوظة ومتاحة حتى في حال تعطل القرص الصلب للحاسوب. كما يسهم استخدام الأقراص المضغوطة وتخزينها في مكان آمن مثل المنزل في توفير طبقة إضافية من الحماية للبيانات.
- ليس لدينا نسخة غير متصلة بالإنترنت من رسائل البريد الإلكتروني أو سجل العناوين، لذلك إذا نسينا كلمة المرور الخاصة بنا (أو إذا تمكن شخص ما من تغييرها بغية الأذيّة)، سنفقدها.
- ليس لدينا نسخ من أي بيانات على هواتفنا المحمولة.
- ليس لدينا نسخ مكرّرة، رقميّة أو ماديةٌ، من المستندات المطبوعة مثل العقود والفواتير.
- في ضوء القائمة المرجعية الموصى بها في هذا القسم، يجب أن نكون قد قمنا بإعادة ترتيب أجهزة التخزين وأنواع البيانات والنسخ الاحتياطية بطريقة تجعل معلوماتنا أكثر مقاومة للكوارث. على سبيل المثال:

نوع البيانات	أوّلية/مُكرّرة	جهاز الحفظ/التّخزين	مكان الحفظ
ملفّات بحثيّة	أوّليّة	مُحركّ قرص الحاسوب	المكتب
ملفّات بحثيّة	مكرّرة	وحدة نقل وتخزين بيانات	المنزل
انتهاكات حقوق الإنسان: ملف الشّهادات	أوّليّة	مُحركّ قرص الحاسوب	المكتب
انتهاكات حقوق الإنسان: ملف الشّهادات	مكرّرة	وحدة نقل وتخزين بيانات	المنزل
قواعد بيانات البرامج	أوّليّة	مُحركّ قرص الحاسوب	المكتب
قواعد بيانات البرامج	مكرّرة	محرّك قرص خارجي	المنزل
البريد الإلكتروني وجهات التّواصل عبر البريد الإلكتروني	أوّليّة	حساب الGmail	الإنترنت
البريد الإلكتروني وجهات التّواصل عبر البريد الإلكتروني	مكرّرة	نسخة احتياطية بواسطة أداة ثندربرد محظوظة على حاسوب المكتب	المكتب
رسائل نصيّة وسجلات جهات الاتصال	أوّليّة	الهاتف المحمول	بحوزتي

نوع البيانات	أوّلية/مُكرّرة	جهاز الحفظ/التّخزين	مكان الحفظ
رسائل نصيّة وسجلات جهات الاتصال	مكرّرة	مُحركّ قرص الحاسوب	المكتب
رسائل نصيّة وسجلات جهات الاتصال	مكرّرة	نسخة احتياطية على شريحة أمن رقمي	المنزل
المطبوعات (عقود، وفواتير، إلخ)	أوّليّة	دولاب مكتبي	المكتب
الوثائق المسوحة	مكرّرة	محرّك قرص خارجي	المنزل
نسخ من كافّة الوثائق	مكرّرة	الخادم الخاص بالمكتب	المكتب

عملًا بقاعدة ثالوث النّسخ: نجد في الجدول الجديد ثلاث نسخ من المعلومات: على الحواسيب، وخادم المكتب، والمنزل، في مكانين، ونسخة واحدة على الأقل خارج المكتب.
بمجرد الانتهاء من كتابة القائمة المرجعية، يكون الوقت قد حان لعمل النسخ الاحتياطية.

الاحتفاظ بنسخ احتياطية على أجهزتنا الخاصّة... في خطوات

نحفظ النسخ الاحتياطية على أداة نقل وتخزين محمولة كي يتسنى لنا نقلها إلى مكان آمن. تعد محركات الأقراص الصلبة الخارجية أو أقراص الدّي. في. دي. أو وحدات نقل وتخزين البيانات من الخيارات الممكنة لهذا الغرض. يستخدم بعض الأشخاص الأقراص المدمجة أو أقراص الدّي. في. دي لهذا الغرض، نظرًا لأن خطر الكتابة على النسخة الاحتياطية وفقدان النسخة الاحتياطية أقل. قد تكون الأقراص المضغوطة الفارغة رخيصة بما يكفي للسماح لنا باستخدام قرص جديد في كل مرة نحفظ بها نسخة احتياطيّة جديدة.

إذا احتفظنا بنسخ احتياطية لجهازنا المحمول على حاسوبنا، فلا بدّ أن تكون الخطوة التالية أن نحفظ تلك النّسخة الاحتياطية على جهاز تخزين خارجي. كما علينا ضبط إعدادات أجهزتنا للاحتفاظ بنسخ احتياطيّة على نحوٍ تلقائي.
نظرًا لأن ملفاتنا غالبًا ما تحتوي على معلومات أكثر حساسية، فمن المهم أن نقوم بحماية ملفاتنا التي تم نسخها احتياطيًا باستخدام التشفير. يمكننا معرفة كيفية القيام بذلك باستخدام الأدوات المضمنة في نظام التشغيل مثل BitLocker أو FileVault أو LUKS في القسم الأوّل من المحور الخامس من الفصل الثّاني (2.5.1) حماية رابط البيانات كما بالرّجوع إلى دليل ڤيراكربت: رابط

نظام تشغيل لينكس
تشتمل معظم إصدارات نظام لينكس على أداة نسخ احتياطي. يحتوي أوبونتو على أداة مدمجة تسمى Déjà Dup تسمح لنا بعمل نسخة احتياطيّة من ملفاتنا وتشفيرها، للمزيد بهذا الخصوص، يُمكن مراجعة دليل استخدام خاصيّة Déjà Dup عبر الرّابط.

نظام تشغيل ماك
يُمكننا عمل نسخ احتياطية على محرّك أقراص خارجي باستخدام أداة Time Machine

نظام تشغيل ويندوز
يُمكننا عمل نسخ احتياطية على محرّك أقراص خارجي باستخدام خاصيّة ويندوز للنسخ الاحتياطي:
رابط

النّسخ الاحتياطي باستخدام التّقنيات السّحابية كخيار؟
عندما نسمع شخصًا يتحدّث عن خدمات محوسبة "سحابية" علينا التّفكر في "حواسيب أشخاص آخرين". تعمل الخدمات السّحابية مثل Google Drive، وCloud Dropbox، وNextCloud على حفظ نسخنا الاحتياطيّة وغيرها من البيانات على خوادم (حواسيب) تلك الشّركات أو مقدمي هذه الخدمات، ما يعني أن خصمنا يحتاج إلى فيض من الوقت للوصول إلى تلك الأجهزة دون أن نلحظ تسلله (على عكس الأجهزة الّتي بحوزتنا، إذ من المرجح أن نلحظ نشاطًا مشبوهًا)؛ لذا حري بنا الاحتفاظ بنسخة محليّة من بياناتنا القيّمة.
إذا كان هناك احتمال قوي بأنّ أجهزتنا أو مساحة العمل الخاصة بنا عُرضة للإتلاف، أو قد أنّ نسخنا الاحتياطية عُرضة للسلب، فمن المنطقي تشفير بياناتنا ثم تخزينها في خدمات سحابية موثوقة.
في هذا السّياق، علينا أن نُفكّر في اللّجوء لمقدمي خدمة يمكنهم تشفير بياناتنا نيابةً عنّا (تسمى خدمات التشفير الجامع المانع (End-to-End) أو خدمات المعرفة الصفرية (Zero Knowledge)) أو تشفير ملفاتنا بنفسنا ثم الاحتفاظ بنسخ احتياطيّة منها باستخدام التّقنيات السّحابيّة.
حماية ملفاتنا قبل حفظها باستخدام الخدمات السّحابية
إن ساورنا قلق حيال إمكانية وصول شخص ما (مثل المتسللين أو جهات تقديم الخدمة) إلى الملفات التي نحتفظ بها في السُحُب الحافظة، يمكننا حمايتهم بالتشفير.

- يُمكننا تحميل بِرماج Crypomator لحماية ملفّاتنا (رابط) الّتي نريد حفظها في سُحب الحفظ.
- أو يُمكننا استخدام برنامج كريبت-فيرا لإنشاء مجلّد مشفّر ثُم حفظه في سُحب الحفظ.

الخدمات السّحابية المشفّرة
إذا قرّرنا الاحتفاظ بملفاتنا باستخدام التّقنيات السّحابية، ينبغي لنا استخدام أحد خيارات التّشفير التالية الّتي تضمن المعرفة الصفريّة والتّشفير الجامع المانع:

- ميغا (أوّل 15 غيغا مجانيّة ثُم ينبغي الدّفع) رابط
- سِنك (أوّل 5 غيغا مجانيّة، بعد ذلك ينبغي الدّفع) رابط
- سبايدِر أوك (مساحات مدفوعة) رابط
- ترِسورِت (مساحات مدفوعة) رابط

عمل نسخ احتياطيّة باستخدام التقنيات السّحابية من خلال الأدوات المُضمّنة في نُظم التّشغيل

نظام تشغيل الأندرويد
- غوغل درايف

نظام تشغيل الآي. أو. اِس.
- آي-كلاود

نظام تشغيل ماك
- آي-كلاود

نظام تشغيل ويندوز
- وون درايف

الاحتفاظ بنسخ احتياطيّة من بُردنا الإلكترونيّة
- يمكننا استخدام برنامج عميل البريد الإلكتروني نحو برنامج ثَندِربِرد لمعاينة بريدنا الإلكتروني وعمل نسخ احتياطيّة بوتيرة دوريّة على أجهزتنا. يشرح دليل استخدام ثَندِربرد (رابط) بالتفصيل كيفية إعداد تثبيت البرنامج لاستخدام عنوان بريدنا الإلكتروني الحالي، وتنزيل بريدنا الإلكتروني، وربما حذفه من الخادم. توفر معظم خدمات البريد الإلكتروني إرشادات بشأن كيفية تثبيت برامج أخرى لتلقي بريدنا (لهذا الغرض يُمكننا البحث في إعدادات بريدنا الإلكتروني للحصول على تعليمات بشأن بروتوكول مكتب البريد (POP3) لحذف بريدنا الإلكتروني من الخادم، أو بروتوكول الوصول إلى رسائل الإنترنت لإبقائه على الخادم.)

عمل نُسخ احتياطية من الهاتف الذكي وحفظها على الحاسوب
لعمل نسخة احتياطية من جهات الاتصال والرسائل النصية والإعدادات والبيانات الأخرى الموجودة على هاتفنا المحمول، يُمكننا توصيل جهازنا الذّكي بحاسوبنا الخاص من خلال كابل وحدات نقل وتخزين البيانات، وقد نحتاج أيضًا إلى تثبيت برنامج من الموقع الإلكتروني للشركة المصنعة لهاتفنا.

نظام تشغيل الأندرويد
- ننقل ملفاتنا من جهازنا الأندرويد إلى حاسوبنا: رابط
- إذا واجهنا صعوبة في عمل نسخة احتياطية لكافّة أنواع المعلومات من هاتفنا الأندرويد إلى حاسبونا، يُمكننا اللّجوء إلى خدمات غوغل السّحابيّة من خلال الأدوات المُضمّنة في أجهزتنا: رابط، لكن علينا التّنبّه بأنّ معلوماتنا ستُحفظ على خادم تابع لشركة غوغل.

نظام تشغيل الآي. أو. اِس.
- عمل نُسخ احتياطيّة من محمولنا إلى حاسوبنا: رابط، شريطة ألّا ننسى تشفير النّسخة الاحتياطية المحليّة بكلمة مرور خاصّة.

مسح المستندات المطبوعة وعمل نسخ احتياطيّة منها

- نستطيع أيضًا، إن أمكن، عمل نسخ ممسوحة (مصوّرة) من كافّة أوراقنا المهمة، ثُم نعمل نسخة احتياطيّة من المواد الممسوحة أو الصّور مع المستندات الإلكترونيّة الأخرى، على النّحو الّذي سبقت مناقشته أعلاه.

جدولة النّسخ الاحتياطي

لإجراء نسخ احتياطي لجميع أنواع البيانات المذكورة أعلاه، لا بدّ لنا من جُملةٍ من البرامج والعمليات. تأكد من تخزين كل نوع بيانات في موقعين منفصلين على الأقل.

التّدرّب على استعادة البيانات

- بمجرّد الاحتفاظ بنسخ احتياطية، علينا إجراء اختبار للتأكد من أنّنا نعرف كيفية فتح الملفات واستخدامها مرة أخرى، فهذه العمليّة محكومة بخواتيمها، أي أنّ الغاية تكمن في استعادة المفقود، لا في إجراءات النسخ الاحتياطي بحد ذاته!

وضع إجراءات لزملاء العمل

- إذا كنّا نعمل في مكتب، علينا أن نكتب الإجراءات ومشاركتها مع جميع الموظفين لضمان قيامهم بالاحتفاظ بنسخ احتياطيّة للملفات على نحوٍ موثوق وآمن. كذلك لا بدّ من الإبلاغ المخاطر الّتي قد تنجم عن فقدان بياناتنا لقدرتنا على القيام بأعمالنا. في هذا السّياق، من المفيد العمل معًا لرسم شبكة كتلك المذكورة أعلاه لتحديد جميع البيانات التي يتم تداولها في مكاتب عملنا.

عِدةّ من اِعتِبَارات أُخَر

عندما نضع خطة للإبقاء على نسخ احتياطيّة، علينا مقاربة الأمر من منظارٍ أوسع: كيف يمكننا التعافي من كارثة فقد البيانات ومواصلة العمل؟ لا ينبغي أن تقتصر خطتنا على ملفاتنا فحسب، بل يجب أن تشمل أيضًا ما يلي:

- البرامج التي نستخدمها، وتراخيص استخدامها
- كيفية استبدال المعدات في حالة فقدانها، أو إتلافها، أو مصادرتها؟
- الإبقاء على مكان لمواصلة العمل منه في الأزمات.
- يُذكر في هذا السّياق، أن التّخطيط لهذا الغرضٍ قد يقتضي تكريس مخصّصات ماليّة لتعافي من تبعات فقدان البيانات والمعدّات، لذا يُمكننا مثلًا تخصيص بند لهذه المسألة ضمن منحة تمويل أعمالنا.

2.5.3| إتلاف البيانات

يستند محتوى هذا القسم على مادّة "سُبل إتلاف البيانات" المتاحة عبر منصّة عُدَّة الأمان، أدوات وممارسات للأمان الرقمي: رابط
يستخدم الهاتف أو الحاسوب ذاكرته كشخصٍ يسعى لحفظ محتوى ورقة؛ فيكتب بقلم الرصاص، ويجمع الملفات التي نطلب منه حذفها (مثل الملفات المؤقتة أو الملفات الموجودة في سلة المهملات أو سلة المحذوفات). وعندما يحتاج إلى مساحة أكبر، فإنّه يمحو جزءًا من المكتوب على الورقة في الكومة المخصصة للحذف ويكتب على ذلك الجزء من الورقة كرّة أخرى بيانات لملفات جديدة.
عندما نسحب ملفاً إلى سلة المهملات ونفرغها، فإن الهاتف أو الحاسوب لا يزيل ذلك الملف فعليًا، فالأمر أشبه بإزالة الملصقات من خزانة الأرشيف مع ترك الملفات داخلها. إذ أنَّ "حذف" ملف ما هو بمثابة إعلام وإخبار لهاتفنا أو حاسوبنا بأنّه يمكن استخدام المساحة التي كان يشغلها الملف المحذوف لغيره. حتى يقوم الجهاز بحفظ ملف آخر في تلك المساحة، وبالتّالي يُمكن لمن يستطيع الوصول إلى الجهاز والأدوات المناسبة معاينة الملف بعد حذفه.
تتميّز الأدوات التي نوصي بها بأنها تمكّنا من مسح أكثر من الملصقات والتسميات، فهي تكتب خربشةً على كل كلمة عدة مِرار إلى أن يتلاشى أي أثر للملف الأصلي. يتفق خبراء الأمن على أن "مسح" المساحة غير المستخدمة في هاتفنا أو حاسوبنا بهذه الطريقة كفيل بمنع المتسلل من قراءة ملفاتنا المحذوفة.
لكن ثمَّ استثناء كبير لهذا، ففي جميع الهواتف والحواسيب الحديثة خطر يكمن في محركات الأقراص الأحدث التي تسمى محركات الأقراص الصّلبة الثّابتة (Solid State Drive) ففيها تقنية تحول دون مسح محتوياتها بالكامل، وتُعرف هذه الخاصيّة توزيع التّلف (Wear Leveling). لمزيد من المعلومات عن تحديات مسح محرّكات الأقراص الصّلبة الثابتة: رابط لتعسير استعادة ما نمسحه عن محرّكات الأقراص الصّلبة الثابتة، ينبغي لنا تشفير هذه الأقراص (ينبغي إدراج رابط للقسم الأوّل من المحور الخامس من الفصل الثّاني (2.5.1)) بأسرع ما يُمكن، لا سيّما إذا أردنا التّخلّص منها؛ من الضّروري أيضًا تشفير محرّكات الأقراص قبل إعادة استخدامها.
لكن تأمين أدوات الحذف لن يحذف الملفات ما لم نحذفها أو نوجّه الجهاز أو الأدوات بحذفها الّتي ينبغي أن نتعامل معها بكثير من الحذر، إن كنّا نتعامل مع هذه الأدوات للمرّة الأولى، علينا اتباع هذه الخطوات بدقّة لحذف الملفات بأمان وفعاليّة. هناك عدة طرق لمسح البيانات الحسّاسة من أجهزتنا. يمكننا مسح ملف واحد فقط، أو محتويات سلة المهملات، أو المساحة الفارغة على محرك الأقراص، أو محرك الأقراص بأكمله.

إزالة آثار أنشطتنا على أجهزتنا

ينبغي لنا محو آثار أنشطتنا على أجهزتنا بإزالة سجل الأنشطة عن الجهاز والتّصدّي لأي برمجيات خبيثة للحفاظ على جودة أداء أجهزتنا. من الصّعب العثور على هذه الملفات وإزالتها بأمان، وهذا ما يسوقنا إلى السّطور التّالية الّتي تُخبرنا أكثر عن هذه الملفات.
تحتفظ متصفحات الويب الّتي نستخدمها نصوص، وصور، وملفات تعريف الارتباط، ومعلومات الحسابات، وسجل المواقع الإلكترونيّة الّتي نزورها، والبيانات الشخصية المستخدمة لملء نماذج التسجيل عبر الإنترنت. يُضيء القسم المخصّص لتصفح Firefox على المزيد عن تلك البيانات، وكيفيّة حذفها في كثير من الأحيان.

تحفظ أجهزتنا والتّطبيقات الموجودة عليها نُسخًا مؤقتة من الملفات التي نعمل عليها، بحيث إذا تعطل الجهاز أو انقطع التيار الكهربائي، لا نفقد كل شيء. مثلًا إذا حذفنا الملف الذي نعمل عليه، فإنّ ما يُحذف هو النّسخة الحالية منه، لكن جهازنا يُبقي على الملفات المؤقتة الأقدم منه بطرق يصعب العثور عليها وإزالتها دون أدوات خاصة. تحفظ التطبيقات والأجهزة أيضًا كافّة أنواع الاختصارات الأخرى لتسهيل حياتنا، بما في ذلك ما تنسخه إلى الحافظة.

- في ضوء ما تقدّم، ينبغي لنا وضع جدول زمني منتظم لمحو المضامين غير المستخدمة من ذاكرة جهازنا على نحوٍ آمن، لضمان إزالة الملفات الحسّاسة عن أجهزتنا، أو محركات الأقراص الثابتة، أو شرائح الذّاكرة، أو وحد نقل وتخزين البيانات، أو بطائق الذّاكرة القابلة للإزالة (شرائح الأمن الرّقمي) من الكاميرات، أو الهواتف المحمولة، أو مشغلات الموسيقى المحمولة، وأي جهاز آخر يحفظ معلومات حسّاسة.

نظام تشغيل الأندرويد

يُمكننا استخدام برنامج CCleaner لأنظمة تشغيل الأندرويد لإزالة الملفات المؤقتة والمخفيّة.

نظام تشغيل لينكس

يُمكننا استخدام برنامج BleachBit لنظام تشغيل اللينكس لإزالة الملفات المؤقتة والمخفية، يُمكننا أيضًا الاطلاع على أدلّة استخدام البرامج.

نظام تشغيل ماك

يُمكننا استخدام الملفات والمجلدات المُخصّصة تُوجد هذه الخاصيّة في برنامج CCleaner لنظام تشغيل الماك لإزالة الملفات المؤقتة والمخفيّة.

المحو الفردي للملفات بأمان

نظام تشغيل لينكس

يُمكننا استخدام BleachBit باتباع الخطوات المدرجة في الدّليل الإرشادي.

نظام ويندوز

يُمكننا استخدام برنامج Eraser
أو برنامج BleachBit باتباع الخطوات المبيّنة في الدّليل الإرشادي.

إزالة المعلومات التّعريفيّة من صورنا وسائر ملفاتنا

قد تبدو مسألة حماية معلوماتنا التّعريفيّة أمرًا بسيطًا ينقضي بتمويه للوجوه الظّاهرة في الصّورة أو تغطية التّفاصيل الحسّاسة أو الأماكن الظّاهرة. إلّا أنّ الأمر ليس بهذه السّهولة، فمن لديه الملف قد يستطيع ما نحاول إخفاءه إن لم نُحكِم التمويه بطريقة محدّدة، وهذا يسوقنا إلى تطبيق Obscuracam الّذي يساعدنا على إحكام تمويه صورنا بأمان.

تحتوي الصور على معلومات أكثر ممّا نراه، إذ تحتوي كافة الملفات على كمية صغيرة من المعلومات عن كيفية إنشائها ومكانه. تسمى هذه المعلومات البيانات الوصفية. يمكننا عادةً إلقاء نظرة على بعض البيانات التّعريفيّة للملف على حاسوبنا بالنّقر بزر الفأرة الأيمن على الملف واختيار "خصائص" أو "الحصول على معلومات."

قد تتضمن بعض البيانات التعريفيّة موقعنا أو الجهاز الذي تم إنشاء الملف به: معلومات يمكن أن يستخدمها شخص يعاين الملف للتعرف علينا. لتفادي ذلك يُمكننا الاستعانة ببرامج Scrambled Exif، وMetaX، وExifcleaner لمسح البيانات التعريفية بأمان. للمزيد من المعلومات عن البيانات التّعريفيّة وكيفيّة تخفيف ملفاتنا منها، يُمكن الاطلاع على هذه المقالة.

- يمكننا استخدام تطبيق Obscuracam
- يمكننا استخدام تطبيق Scrambled Exif
- يمكننا استخدام تطبيق MetaX
- يمكننا استخدام تطبيق Exifcleaner
- في هذا السيّاق، من المفيد الاطلاع على هذه المقال بشأن إخفاء المعلومات المُضمّنة للصور والحصول على تقنيّات إضافية

محو بيانات جهاز بالكامل

عند إقدامنا على مسح بيانات محرّك أقراص صلبة بالكامل، يتعيّن علينا تشغيل نظام تشغيل حاسوبنا من محرّك أقراص مختلف لأن برنامجًا مثل Eraser لا يُمكنه مسح الجهاز بالكامل إن كان في وضع التّشغيل، وهما يستدعي إزالة محرك الأقراص المُراد محو بياناته من حاسوبنا وتحويله إلى محرك أقراص صلبة خارجي.

خطوات تنطبق على كافّة الأجهزة

- إغلاق جميع التّطبيقات غير الضّروريّة؛
- قطع الاتصال بالإنترنت، أو إيقاف تشغيل شبكة الواي فاي أو فصل كابل الإنترنت، وفقًا ما تقتضيه الحاجة؛
- الحفاظ على نسخة احتياطيّة مشفّرة من ملفاتنا المهمة، على النّحو الّذي سبق مناقشته في دليلنا، تحديدًا بشأن كيفية التعافي من فقدان المعلومات؛ (يرجى مراجعة القسم الثّاني من المحور الخامس من الفصل الثّاني (2.5.2) النسخ الاحتياطيّة واسترجاع البيانات)
- قد يُفضّل أيضا البدء بمسح الملفات المؤقتة في متصفحنا؛ (يُرجى مراجعة القسم الأوّل من المحور الرّابع من الفصل الثّاني (2.4.1) التصفح الآمن)
- ثُمَّ اتباع الخطوات أدناه وفقًا لكل جهاز ونظام تشغيل:

الهواتف

- التأكّد من تشغيل التّشفير الكامل للقرص، إن أمكن، على أن نُراجع إضاءات القسم الأوّل "خيار التّشفير الكامل لأجهزتنا" من المحور الخامس من الفصل الثّاني "حماية البيانات" قبل الإقدام على ما في أجهزتنا من بيانات.

نظام تشغيل الأندرويد

أولًا نبدأ بإعادة ضبط المصنع، ثُم نُثبّت تطبيق Extirpater، لمباشرة محو كل أثر متبق في شريحة الذّاكرة، من المفيد في هذا السّياق مراجعة القسم الثّالث " إزالة آثار أنشطتنا على أجهزتنا" من المحور الخامس من الفصل الثّاني "إتلاف البيانات."

نظام تشغيل الآي. أو. اِس

لمحو بيانات جهازنا بأمان علينا اتباع التّعليمات في الرّابط.

أجهزة الكمبيوتر

- من غير الممكن للجهاز أن يمحو جميع بياناته بالكامل، لا بدّ لنا من تشغيل حاسوبنا من محرك أقراص خارجي للقيام بذلك.
  - ثمّ عدّة خيارات أحدها إزالة محرك الأقراص الصّلبة من حاسوبنا، والتّعامل معه باعتباره محرك أقراص خارجي، وتنظيفه باستخدام حاسوب آخر.
    - للحصول على إرشادات حيال كيفيّة فك القرص الصّلب، يُمكننا البحث على "إزالة القرص الصّلب" ثُمّ نتوجه إلى طِراز ونموذج الحاسوب على موقع iFixit.
    - ثُم نضع محُرّك الأقراص المُزال في حاضنة (حاوية) الأقراص الصّلبة المخصّصة لتخزين ونقل البيانات.
- يُمكننا التّفكير بخيار برمجية DBANJI، للكتابة فوق القرص بأكمله. قد يستغرق ذلك بعض الوقت، كما سنحتاج لتنزيل DBAN وتشغيله من محرك أقراص نقل وتخزين بيانات فارغ. لسوء الحظ، من الصّعب ضمان مسح محرك الأقراص بالكامل على الحواسيب الأحدث الّتي تستخدم الأقراص الصّلبة الثّابتة (Solid State Drives). مع ذلك لا يزال بإمكاننا بمحو المستطاع باتباع الخطوات التّالية.
- بمجرد مسح القرص بأكمله، علينا التّفكير في إعادة تثبيت نظام التشغيل.
- في خضم ذلك، لا بدّ ألّا ننسى ضبط الإعدادات بما يضمن التّشفير للقرص كاملًا.

نظام تشغيل ماك

- في أجهزة Mac القديمة التي تحتوي على شرائح Intel يمكننا مسح محرك الأقراص الثابتة لدينا بأمان باستخدام أداة القرص أو مساعد المسح.
- أمّا على أجهزة الماك المدعمة برقاقات الأقراص الصّلبة الثّابتة، فعلينا بالتّالي:
  - أولًا نفعّل التّشفير الكامل للقرص المُراد حذفه (رابط) لكي نضمن أن تبدو محتوياته بلا معنى لأي شخص لا يملك كلمة مرور الجهاز.
  - ثانيًا نتبع الإرشادات التّالية لمسح القرص الصّلب الثّابت باستخدام أداة القرص (رابط).

نظام تشغيل ويندوز

- نصل القرص الّذي نريد مسحه بحاسوب مُدعّم ببرماج Eraser.
- ثُمّ نمحي كل شيء على القرص الخارجي؛
- بعد ذلك نستخدم برماج Eraser لمحو كل مساحة غير مخصّصة على القرص، علمًا أنّ ذلك قد يستغرق ليلة كاملة نظرًا لبطء هذه العملية.

ماذا نفعل حال بيع حاسوبنا أو هاتفنا القديم أو إعطائه لغيرنا أو التّخلّص منه

كما قلنا سابقًا، تتطلب عملية مسح القرص وقتاً ليس بالهين، ومن غير السائغ إعطاء الجهاز دون قرصه، لكن عند بيعه أو التّخلص منه، فلا مناص من أخذ الاحتياطات التّالية كي لا نُسلّم ملفّات حسّاسة لشخص آخر.

- مسح الجهاز بالكامل باستخدام الإرشادات المذكورة أعلاه.
- إزالة محركات وحدات نقل وتخزين البيانات، أو الأقراص المدمجة، أو أقراص الدّي. في. دي. أو شرائح الأمن الرّقمي، أو شرائح الاتصال، أو أجهزة دونجل، أو الأجهزة الصغيرة الأخرى التي قد يتم إدخالها أو توصيلها بجهازنا.
- الإحجام عن إعطاء المالك الجديد القرص الصلب؛ إن كان ذلك ممكناً، أمّا إن تعذّر ذلك، فلا مناص من اتباع التعليمات الخاصة بكيفية مسح القرص قبل ذلك.
- الإتلاف الفعلي للقرص بعد مسحه إن كان المراد التّخلص من الجهاز. يمكن القيام بذلك عن بخرقه بعدّة مسامير أو باستخدام المثقاب؛ لكن إيّاك وحرق القرص أو تعريضه للأحماض، أو وضعه في الميكروويف. تجدر الإشارة إلى أنّ الإتلاف الفعلي للقرص الخيار الأكثر أمانًا دائمًا.
- يمكن أيضًا الاحتفاظ بمحرك الأقراص بعد مسحه ما زال في حالة جيدة لإعادة استخدامه لاحقًا في جهاز جديد أو كمحرك أقراص صلبة خارجي لنا.
- فيما يلي طيف من الإرشادات التالية الّتي يُمكن اعتمادها كثبت تحقّقي إضافي عند القيام بالخطوات الّتي أدرجناها في القسم الخاص بمسح بيانات جهازنا بشكل آمن، أعلاه:

نظام تشغيل الاندرويد

- للأجهزة العاملة بنظام الأندرويد، يُمكننا اتباع الإرشادات التّالية (رابط) وذلك لإزالة الجهاز المُباع أو المُتخلَّص منه من قائمة الأجهزة المرتبطة بحسابتنا على الفضاء الرّقمي.
  - واتباع الإرشادات التالية لضمان مسح الجهاز بأكمله وبأمان (رابط)، وذلك لتجهيز الهاتف للتخلّص منه بأمان، بما في ذلك الإرشادات الخاصّة بضمان مسح الجهاز كاملًا وبأمان.

نظام تشغيل لينكس

- للأجهزة العاملة بنظام لينكس، ينبغي لنا اتباع الإرشادات التّالية (رابط) وذلك لإزالة الجهاز المُباع أو المُتخلَّص منه من قائمة الأجهزة المرتبطة بحسابتنا على الفضاء الرّقمي.
  - واتباع الإرشادات أعلاه لضمان مسح الجهاز بأكمله وبأمان.

نظام تشغيل ماك

- للأجهزة العاملة بنظام ماك، ينبغي لنا اتباع الإرشادات التّالية (رابط)؛ وذلك لإزالة الجهاز المُباع أو المُتخلَّص منه من قائمة الأجهزة المرتبطة بحسابتنا على الفضاء الرّقمي.
  - واتباع الإرشادات التالية لضمان مسح الجهاز بأكمله وبأمان (رابط)، وذلك لتجهيز الهاتف للتخلّص منه بأمان، بما في ذلك الإرشادات الخاصّة بضمان مسح الجهاز كاملًا وبأمان.

نظام تشغيل ويندوز

- للأجهزة العاملة بنظام ويندوز، ينبغي لنا اتباع الإرشادات التّالية (رابط)؛ وذلك لإزالة الجهاز المُباع أو المُتخلَّص منه من قائمة الأجهزة المرتبطة بحسابتنا على الفضاء الرّقمي، بما في ذلك:
  - اتباع الإرشادات التالية لضمان مسح الجهاز بأكمله وبأمان (رابط)، وذلك لتجهيز الهاتف للتخلّص منه بأمان.
  - واتباع الإرشادات الخاصّة بضمان مسح الجهاز كاملًا وبأمان.

إتلاف الأقراص المدمجة والدّي. في. دي. قبل التّخلّص منها

حتى لو كان القرص المدمج أو قرص دي. في. دي. يتيح لنا حفظ بيانات إضافية عليه (أي إذا كان قابلاً لأن يحفظ عليه بيانات مرّة أخرى)، فمن الأفضل إتلافه، إذ أنّه من الصعب للغاية مسح محتويات الأقراص المدمجة والدّي. في. دي بالكتابة على ما فيها من بيانات.
قد تكونون قد سمعتم قصصًا عن استرجاع معلومات من أقراص مدمجة أو أقراص الدي. في. دي بعد تقطيعها إلى قطع صغيرة. رغم أنّ هذا ممكن، إلّا أن إعادة بناء المعلومات بهذه الطريقة يتطلب قدرًا هائلًا من الوقت والخبرة؛ لذا فإن الأمر متروك لتقديرنا إذا ما كان هناك حولنا شخص قادر ومستعد لبذل الموارد المطلوبة لإعادة بناء قرص بعد أن أضحى شظايا متناثرة.
لهذا الغرض علينا:

- استخدام مقص قوي لتقطيع الأقراص المدمجة أو أقراص الدّي. في. دي. غير المرغوب فيها وتحتوي على معلومات حسّاسة؛ وذلك لضمان تفتيتها إلى قطع صغيرة.
- من الممكن استخدام بعض آلات تمزيق الورق خيار لتقطيع الأقراص المدمجة أو أقراص الدّي. في. دي. لكن علينا التّثبت بأن جهاز التقطيع المُختار قادر على ذلك قبل مباشرة تقطيع أقراصنا إربًا!
- أخيرًا نتخلّص من حطام القرص في عدّة أماكن بعيدة عن منازلنا أو مكاتبنا لجعل إعادة تجميعها ضربًا من المحال.

تخلص من القطع في مواقع مختلفة بعيدًا عن منزلك أو مكتبنا لتجعل عملية إعادة الإعمار أكثر صعوبة.

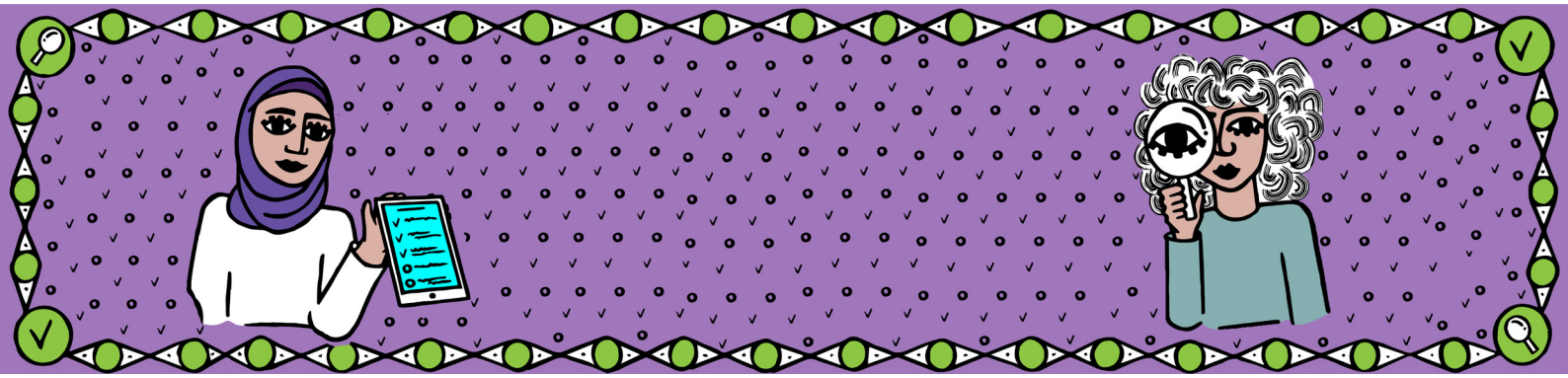
متقدم: إزالة ما تبقّى من آثار المعلومات المحذوفة في هواتفنا الذّكيّة

نوصي بمسح كل المساحة "الفارغة" على أجهزتنا بوتيرة دوريّة.
قد تبقى بعض آثار المعلومات المحذوفة في شريحة الذّاكرة بعد إعادة ضبط هواتفنا وفقًا لإعدادات المصنع؛ لذا:

- لنستخدم برنامج Extirpater لحذف كل ما سبق أن حذفناه باستخدام برنامج CCleaner أو بعد ضبط المصنع، ذلك لضمان أن يكون الحذف نهائيًا. تجدر الإشارة في هذا السّياق أنّ هذا

3| إدارة مخاطر الأمان الرّقمي

تُقدِّم المقاربة المنهجة والجماعيّة لإدارة المخاطر أفضل السُّبل وأنجعها لمواجهة التّهديدات الرّقميّة المتزايدة الّتي يوجهها المجتمع المدني أو المنظّمات الإعلاميّة والنّشطاء والإعلاميون/ات—بدءًا من تقييم المخاطر الّتي تنشي عليها التّهديدات الرّقميّة، بما في ذلك تحليل السّياق وبتقييمات المخاطر الموجّهة، فضلًا عن الخروج بمؤشّرات لرصد الهجمات الرّقميّة (قبل وقوعها في الوضع المثالي) مرورًا بالتّخطيط الاستراتيجيّ لإعداد خطط الأمان (بما يُرجّح أن تتضمّنه من سياسات الأمان الرّقمي، والإجراءات، والإرشادات، إلخ.) وصولًا إلى بناء مسارات سير العمل وروتينيّات ممارسات الأمان الرّقمي الجيدة (على النّحو المشار إليها في الفصل الثّاني: أدلّة الأمان الرّقمي) كما وإجراءات الاستجابات الطّارئة والبنى الهيكليّة لهذه الإجراءات—بالاستناد إلى كافّة هذه المكوّنات يُمكنّنا خلق قدر أكبر من المرانة في التّصدّي للتهديدات الرّقميّة. ضمن هذا الإطار يغطّي هذا الفصل الخطوات التّالية:



- **3.1 | تقييمات مخاطر التّهديدات الرّقميّة**
  - الأمن السيبراني | تقييمات المخاطر عبر الإنترنت
  - النّماذج
  - تقييمات المخاطر السيبرانية لمنظمات المجتمع المدني والمؤسّسات الإعلاميّة
  - تقييمات المخاطر السيبرانية عبر الإنترنت للأفراد (من مدافعين/ات عن حقوق الإنسان وعاملين/ت في حقل الإعلام والصّحافة)
- **3.2 | سياسات وإجراءات الأمان السيبراني**
- **3.3 | التخطيط للاستجابة للحوادث والحالات الطارئة**
- **3.4 | متابعة الأمور الطّارئة: التّعافي، والعنايّة التّالية، واستقاء العبر والدّروس**
- **3.5 | توثيق انتهاكات الحقوق الرّقميّة**

3.1| تقييم مخاطر التّهديدات الرّقميّة

مُلخّص القسم: يُطلعنا هذا القسم على سُبل تحديد المخاطر وإجراء تحليل المخاطر خطوة بخطوة ومعرفة العوامل الّتي ينبغي لنا أخذها بعين الاعتبار.

المُخرجات:

باستكمال هذا الفصل واتباع إرشاداته سنتمكّن من:

- التعرّف على الأمن السيبراني
- والتّمييز بين التهديد، ومواطن الضعف، والمخاطر؛
- والوعي بدائرة التّهديدات؛
- وفهم الأصول والجهات الفاعلة في سياق الأمن السّيبراني والقدرة على تحديدهما؛
- وحساب المخاطر واحتمالية وقوعها وخطورتها بالنّسبة لعملنا؛
- والإلمام باستراتيجيات تخفيف المخاطر على اختلافاتها والقدرة على تطبيقها؛
- والتخطيط للحماية وإعداد خطط طوارئ؛
- تحديد مختلف المخاطر الكامنة بمحيط التّشغيل وبيئته:
- بالإضافة لما سبق، يعرّفنا هذا الفصل على مختلف العوامل التي قد تؤثر على سلامتنا.

الأمن السيبراني | تقييم المخاطر عبر الإنترنت

تعد عمليّة تقييم المخاطر في مجال الأمن السيبراني عاملًا حاسمًا في تحديد الثغرات الكامنة في بنية الأمان التّحتيّة كما في التّوزيع الاستراتيجي للموارد لتخفيف المخاطر المحتملة.

تُمِّد تقييمات المخاطر السّيبرانيّة مؤسّسات المجتمع المدني، والصحفيين/ات، والمدافعين/ات عن حقوق الإنسان بنظرة ثاقبة على وضعهم الأمني بتمكينها لهم من تحديد نقاط الضعف والثّغرات التي يمكن استغلالها من المتربصين، وبالتّالي استباق المخاطر بتخصيص الموارد اللّازمة لمواجهتها ضمن إطار أمان أقوى وأكثر مَرَانة.

تُشكّل تطبيقات الويب غالبًا هدفًا للتهديدات السيبرانية لما تنطوي عليه من مواطن ضعف متأصلة في بُناها. في هذا السّياق، تُساعد تقييمات المخاطر الشّاملة المُحاكة خِصِّصًا لتطبيقات الويب على فهم المخاطر التي تواجهها هذه التّطبيقات وتُمكِّن تنفيذ الاستراتيجيات التّخفيفيّة المنشودة، كما تُعزّز هذه الخطوة من أمان تطبيقات الويب بتقييم ومعالجة ما يتربص بها من مخاطر، عدا ما لها من أثر في الحد من الوصول غير المصرّح به وانتهاكات البيانات والأنشطة الخبيثة الأخرى.

بإيجاز، تعتبر تقييمات المخاطر السيبرانية عاملًا حاسمًا في تشكيل المشهد الرّقمي، لما تؤدّيه من وظيفة استباقية تُحدِّد مواطن الضّعف، وتُسهم في تخصيص الموارد بكفاءة، وتخفيف المخاطر المحتملة. بتعبير آخر تؤدّي هذه التّقييمات دورًا أساسيًا في تقوية تدابير الأمان والحماية من التهديدات السيبرانية ضمن إطار تطبيقات الويب والحضور الرّقمي والمتصل بالإنترنت.

التّهديدات، مواطن الضّعف والمخاطر

يمكن تعريف الفروق بين التّهديدات، ومواطن الضّعف، والمخاطر كما يلي:

تُعرّف **مواطن الضّعف** بأنها أي نقطة ضعف في نظام، أو عمليّة، أو طريقة عمل منظمة أو فرد، بأي أنها بمثابة انكشافنا على الهجمات والأضرار. بعبارة أخرى هي عيوب أو نقاط ضعف في النظام التي يمكن إصلاحها بمُجرّد تحديدها. تشمل هذه المواطن قدرتنا على منع هذا الضّعف أو التقليل منه. إذا كانت قدرتنا على التعامل مع هذه المواطن أكبر من حجم الضعف نفسه، فلا تُعْتَبَر بالضرورة نقطة ضعف؛ أمّا إن فاقت مواطن الضّعف قدرتنا على التعامل معها، فلا مناص من اعتبارها عيوبًا بالنظام لا بدّ لنا من تصويبها.

أمّا **التّهديد**، فهو أي شيء يعرّض ناسنا وأشيائنا للخطر، أو يعيق عملنا، أو يسفر عن ضروبٍ أخرى من الضّرر (نحو الإضرار بالسّمعة)، يُعزى هذا النّوع من التّهديدات إلى شخص آخر يُمكننا تحديده لكن لا يقع ضمن نطاق سيطرتنا وتحكمنا.
تُشير **المخاطر** إلى مآل استغلال تهديد لأحد مواطن الضّعف، بعبارة أخرى: مواطن الضعف + التهديد = المخاطر

تنطوي المخاطر على احتمالية حدوث أمر ذي أثر ما على ناسنا، وأشيائنا، ومنظمتنا، أو عملنا.

تعريف المخاطر

يوسّع تعريف المخاطر الّذي وضعته المنظّمة الدّوليّة للتوحيد القياسي مفهوم المخاطر من دائرة إمكانية الإضرار أو التّسبب بخسارة إلى إحداث "التباس في أهداف المنظّمة،" ما يتعدّى السّلبيات ليشمل الآثار الإيجابيّة أيضًا (المنظّمة الدّولية للتوحيد القياسي، 3100:2009). بصيغة أخرى، يدمج هذا التّعريف مفهوم "الفرصة" ضمن بوتقة المخاطر.
يمكن تقسيم المخاطر التي يواجهها أي شخص إلى ثلاثة أنواع بناءً على:

- الهوية (الملف الشخصي): من العمر، والجنس، والمؤشرات الدّينية، والعرق، والميول الجنسيّة، إلخ.
- والمهنة: مثل الصحفيين/ات، والناشطين/ات، والعاملين/ات في المجال الإنساني.
- البيئات الشخصيّة والمهنيّة: نحو المواقع الجغرافيّة المعرضة للكوارث الطبيعيّة، والاضطرابات والقلاقل المدنية، والعداء تجاه الصحفيين/ات.

في عالم الأمن السيبراني، تبرز الضرورة المُلحة لتقييم المخاطر المتعلقة بشبكات الاتصال وأنظمة الأمان وكشف نقاط الضعف.

تقييم الشّبكة	تقييم الأمان	تقييم مواطن الضّعف
• الأنظمة الدّاخلية • خطط استرداد النسخ الاحتياطية • أدوار الكوادر • استقرار الأنظمة (من تحديث، وأداء، وما إلى ذلك) • تخليص النّظام مِمّا به من ضوضاء • سياسات الاستخدام	• سطح الانكشاف للهجمات السّيبرانيّة • نقاط الدخول • عادات المستخدمين/ات • سياسات الأمان • إجراءات الموارد البشرية • الأثر القانوني	• عيوب التطبيقات • عيوب نظام التشغيل • عيوب النظام الحاسوب • المنافذ والعمليات والخدمات المُفعّلة • قاعدة البيانات • الأخطاء البشري (التكوين، الميزات، التصيد الاحتيالي)

تعتمد معظم المنظمات التّعريفات التّالية:

- التهديد هو خطر أو مصدر محتمل للأذى أو الخسارة؛
- المخاطر هي احتماليات وآثار التّعرّض للتهديد؛
- إدارة المخاطر هي نظام موضوعي لتوقع المخاطر وتقييمها والتأهب لها بهدف الحد من آثارها.

تقييم المخاطر

تُعد التقييمات المتواترة لمخاطر الأمان السيبراني ضرورة لا غنىً عنها لتحديد الأصول الأكثر عرضة للتهديدات، وتقييم الخسائر المحتملة التي قد تتمخض عن استغلال هذه المخاطر، عدا تحديد أولويات تدابير تخفيف آثار المخاطر الأكثر إحاطة برسالة المنظمة.

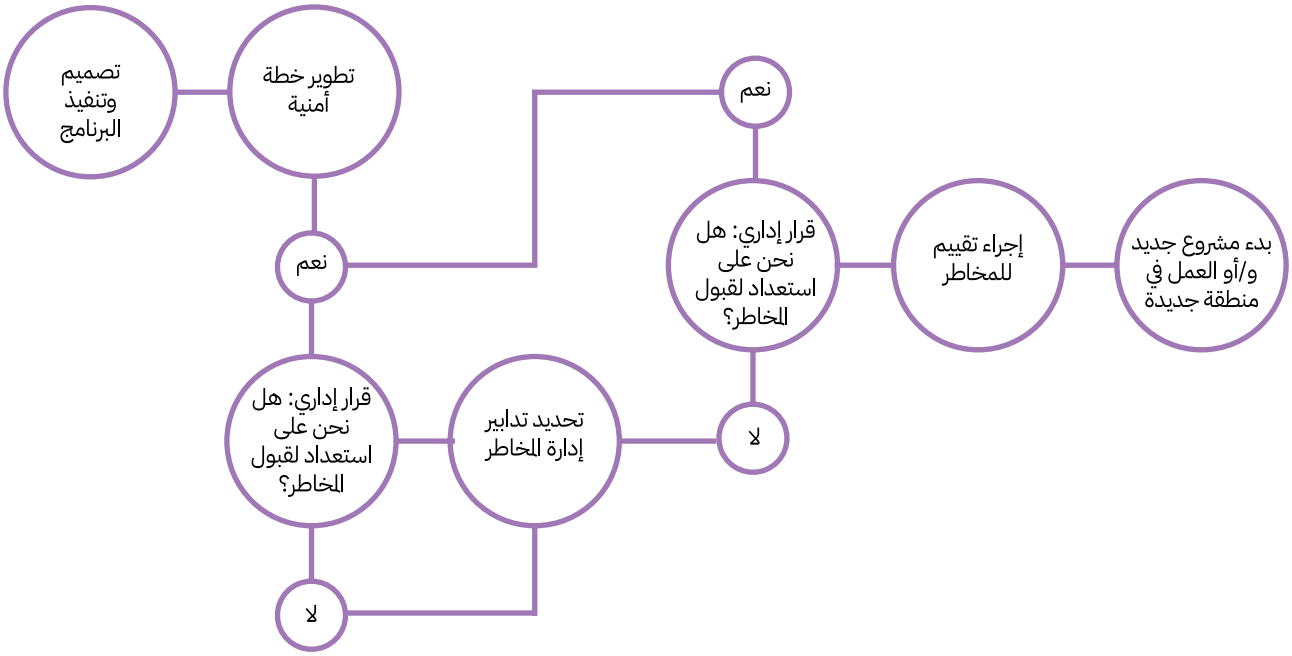
يشكّل تقييم المخاطر عملية لا بدّ من فريق لإكمال دائرتها، أي أكثر من شخص. تتضمن هذه العملية تحديد الأهداف، والتعرف على المخاطر، وتقييمها، وتطوير الأهداف، ورصد المخاطر وتحقيق الأهداف والتواصل بشأنها. في ذات السياق، يقدّم تقييم المخاطر نظرة ثاقبة على المخاطر التي قد تتعرض لها منظّماتنا، وبرامجنا، والأهم من ذلك، الأشخاص عند تواجدهم في موقع محدد. يعتبر تقييم المخاطر الأمنية جزءًا لا يتجزأ من تصميم وتنفيذ البرامج والحضور المستدامين على الإنترنت، عدا أنّه الخطوة الأولى في رحلة إعداد تدابير الأمان والسلامة الرّقميّة الضروريّة لمنظّماتنا.

من المهم تذكر أن هذا الأداة تستخدم لإثراء صناعة القرارات واتخاذها، فضلًا عن إدماج المعلومات المستقاة من تحليل سياق منظماتنا ومناطق عملها، تلك الخطوة المهمّة في إجراء تقييم شامل لمخاطر الأمان.

على الرغم من أهمية دور مديري الأمان والنقاط المركزية في قيادة عملية تقييم المخاطر، يظل من الضروري أن تشمل هذه العملية طواقم الإدارة العليا وأصحاب المصلحة المحليين، وبخاصة فرق البرامج، لجمع أكبر قدر ممكن من المعلومات وتعدد الآراء حيال المخاطر المتنوعة التي تحيط بالموظفين في بيئة عملهم. يفضي هذا النهج التشاركي إلى تقييم شامل ومتكيف، يمكن أن يسهم في تحديد

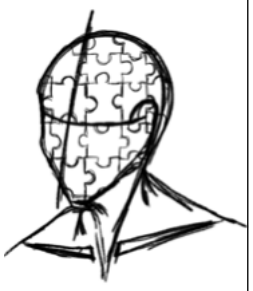
الإجراءات الواجب اتخاذها للقضاء على المخاطر أو تخفيفها أو السيطرة عليها، وتحديد الأولويات بناءً على درجة تأثير هذه المخاطر واحتمالية وقوعها.

في حالة الاستجابة للطوارئ، قد يكون من الصعب إجراء تحليل وتقييم شاملين للسياق ولمخاطر الأمان لتحديد التهديدات المحيطة بمنظمتنا، لما تقتضيه هاتان العمليتان من بحث ووقت كاف في بيئة العمل.



في خضم استجابة منظمتنا لحدث طارئ، يمكننا البدء بإجراء تقييم سريع لمخاطر الأمان خلال المراحل الأولية للتأهب أو عند تطوير برنامج جديد. يتبع ذلك دمج نتائج هذا التقييم في استراتيجية البرنامج الشاملة وتصميمه. مع مرور الوقت وتوفر مزيد من المعلومات، يمكننا تعزيز التحليل وتحديثه باستمرار.

يُمكن إجراء تقييمات مخاطر الأمان في أي مرحلة باعتبارها جزءًا لا يتجزأ من عملية التقييم الأوسع للبرامج. تتضمن هذه التقييمات ثلاث خطوات أساسية: أولًا، تحديد التهديدات ثانيًا، تقييمها، ثالثًا، تطوير استراتيجيات فعّالة للتخفيف من المخاطر وآثارها.

1. تحديد الأهداف	2. تحديد التهديدات	3. التقييم	4. التطوير	5. الرّصد والمتابعة والتغطية التّقريريّة
				
ما هي أهداف المشروع أو البرنامج أو الحملة، قبل وبعد تحقيقها؟	تحديد التهديدات التي تواجه منظّمتنا، وكوادرها، ومجتمعها	تقييم التهديدات وتحليل مستوى المخاطر في منظمتنا (مواطن ضعفها)، وتحديد الأولويات، ومستوى الإقدام على المخاطرة والاستراتيجيّة ذات الصّلة.	تطوير استراتيجيات لتقليل المخاطر المحيطة بمنظّمتنا ومواطن ضعفها من خلال التخفيف من المخاطر.	ينبغي ألّا نتوقف عن تحسينها وتعقبها، ورصدها بالتّقارير، ومشاركتها، ووتيرة مشاركتها ومراجعتها وأطرها الزّمنيّة.

الخطوة الأولى: تحديد الأهداف

أهداف ما قبل التنفيذ	أهداف ما بعد التنفيذ
• فهم البيئة؛ • الوفاء بالتفويضات الخارجية، أي المتطلبات القانونية؛ • تقليل القلق الداخلي؛ • الإجراءات الوقائية؛ • الالتزامات الاجتماعية لخلق وعي بالمخاطر، مثل الموافقة المسبقة.	• بقاء المنظمة أو الأشخاص، أو كلاهما؛ • استمرارية عمليات المنظمة؛ • بدء وتحسين الوظائف التشغيلية مثل سلامة الأفراد، وجمع التبرعات، واستقرار المنظمة؛ • الالتزامات المجتمعيّة.

الخطوة الثّانية: تحديد التهديدات

ينطوي العمل في بيئات تحفها المخاطر على تهديدات قد تلحق الضرر بنا قبل حتى بدء أي عمليات من قبل منظماتنا. تتنوع هذه المخاطر التي قد تؤثر سلبًا على قدرة منظماتنا في تقديم برامجها.

تشمل الخطوة الثانية من عملية تقييم مخاطر الأمان تحديد مجموعة واسعة من التهديدات ضمن السياق الذي تنشط فيه منظمتنا، والتي قد تشكل خطرًا على مكونات البرمجيات والأجهزة الداعمة لعملياتنا، وبالتالي على مواردنا البشرية.

في عصرنا الرقمي، تستلزم شبكات الاتصال، أجهزة التوجيه، والمفاتيح، وقواعد البيانات، وموارد الخوادم، والتطبيقات الخارجية وغيرها، جهدًا دقيقًا لتحديد التهديدات. يُعد إجراء تقييم المخاطر خطوة جوهريّة في تحديد وجرد جميع الأصول، سواء كانت خارجية أو داخلية، بما في ذلك أجهزة الشبكة. يمكن لكل من هذه الأصول أن تشكل خطرًا على أماننا، وبعضها يحمل درجة خطورة أعلى من غيرها. يهدف تحديد التهديدات في الأمن السيبراني إلى الوصول إلى فهم دقيق لجميع الأصول المعلوماتية الحيوية وتحديد الأخطاء البشرية المحتملة في المناطق التي تكون فيها هذه الأخطاء مرجحة، مما يمكننا من التخفيف من هذه المخاطر والتوعية بها.

الخطوة الثّالثة: تقييم التهديدات

بعد تحديد أنواع التهديدات التي قد تواجهها منظمتنا، سواء في البيئة التشغيلية أو في حضورها على الإنترنت، تأتي الخطوة التالية في عملية تقييم مخاطر الأمان، وهي تقييم كل تهديد وتصنيف مستوى المخاطر الذي يمثله للمنظمة. سيمكننا هذا التقييم الدقيق من تحديد الأولويات وتطوير تدابير ملائمة للتخفيف من المخاطر. يتضمن تقييم التهديدات المحتملة للمنظمة فحص كل تهديد بعناية وتحديد مدى تأثيره والعواقب المحتملة له.

التحليل وتحديد الأولويات

ما هو التهديد؟

للإجابة عن هذا السّؤال، لا بدّ لنا من إعداد قائمة بجميع التهديدات التي يمكننا تحديدها في البيئة التّشغيليّة، مثل رسالة المنّظمة، ووظائفها، وخدماتها الحسّاسة، وصورتها، وسمعتها.

أين يكمن التهديد؟

لا بدّ لنا من التّحلي بالتّحديد والدّقة في الإجابة عن هذا السّؤال، وتحديد مواقع التهديد، بما في ذلك البت إذا كان التهديد مقصورًا على منطقة أو أكثر، أو عله يمتد عبر منطقة بأكملها.

من أو ما الذي في خطر؟

للإجابة عن هذا السّؤال، علينا التّفكير في جميع الأشخاص والأشياء المحتمل تعرضها للخطر، مثل:

- الكوادر الدّولية
- الكوادر المحليّة
- أعضاء المجتمع
- الملفات الشخصية والسمعة في الفضاء الرّقمي
- المعلومات الشخصية للداعمين أو المتبرعين
- الصحفيون/ات
- الشّركاء

ما أثر أو آثار التّهديد؟

للإجابة عن هذا السؤال لا بدّ لنا من التّفكير في سيناريوهات مختلفة وتأمل الأثر المحتمل والنتائج الممكنة للتهديد. كذلك ينبغي لنا تحديد مدى خطورة تلك الآثار على منظّمتنا أو مواردنا البشريّة.

للإجابة عن هذا السؤال، علينا الغوص في سيناريوهات متعددة والتأمل في الأثر والنتائج المحتملة لكل تهديد. من المهم أيضًا تقييم مدى خطورة هذه الآثار على منظمتنا ومواردنا البشرية. تتباين التهديدات والمخاطر باختلاف سياقات التشغيل وتشمل عوامل مثل الموقع الجغرافي، وضعف الكوادر، والحضور في الفضاء الرّقمي والملف العام. عند العمل في موقع جديد، حري بنا الاستفادة من البيانات المستخلصة من تدخلات سابقة ومعلومات من المصادر المحلية لتحديد التهديدات المحتملة. كما يجب أن نأخذ في الاعتبار كيف يمكن أن يتغير مستوى الأمان لكل تهديد وفقًا للسياقات المختلفة.

يعتمد اختبار الاختراق على استخدام تقنيات تشابه تلك التي يستخدمها المخترقون لتحديد مدى صعوبة أو سهولة استغلال الثغرات الأمنية في نظامنا. بمجرد إتمام الفحوصات الدقيقة واختبار الاختراق، سنحصل على تقرير مفصل يبرز جميع الثغرات التي حُدِّدَت، مع توفير معلومات إضافية لكل ثغرة. يمثل هذا التقرير مصدرًا قيمًا يساعدنا في تحديد الأولويات ومعالجة الثغرات الأمنية المكتشفة، مما يسهم في تحسين الأمان الشامل لأنظمتنا.
بعد تقييم التهديدات التي تواجه منظماتنا، تأتي الخطوة التالية التي تتمثل في تصنيف كل تهديد لتحديد مستوى المخاطرة المرتبطة به. يعتمد تصنيف المخاطر على مزيج من احتمالية وقوع الحادث وشدة تأثيره. نستخدم طرقًا متنوعة لتصنيف المخاطر، مثل استخدام مقياس مرقم من 1 إلى 5 أو الترميز بالألوان، لإظهار مستويات مخاطر الأمان من منخفضة جدًا إلى عالية جدًا. في هذا الإطار، يُعد استخدام المعلومات المستقاة من تقارير الحوادث الأمان السابقة أمرًا مهمًا لدعم تصنيفاتنا. نظرًا لأن التقييم يكون ذاتيًا، فإن الحصول على دعم من خبراء خارجيين أو على الأقل إجراء مناقشات داخل الفريق يُعد بمثابة تحقق من واقعية التصنيفات. أمّا لتقدير الاحتمالية، فمن المفيد التحقق من وقوع المخاطرة المحددة في منظمات مماثلة أو كيفية تقييمه تلك المنظّمات لاحتمالية تحقّق المخاطرة. في إطار عملنا مع مستويات المخاطر ومصفوفة المخاطر، يُوصى بمراجعة التصنيفات بانتظام.

الخطوة الرّابعة: تخفيف المخاطر

يُعد تطوير تدابير التخفيف، أو العلاج والتّحكّم، خطوة ضروريّة لضمان أن منظمتنا قد بذلت كل ما يُعقل من جهد لتقليل المخاطر قبل الشروع في استخدام كوادرها، ومواردها، وسمعتها في أي إجراءات؛ لما يمثل ذلك من عامل جوهري في إطار واجب العناية الذي نتحمله.

من النادر القضاء على المخاطر قضاءً تامًّا، لكن يمكن لمنظمتنا اتخاذ خطوات محددة لتقليص تعرضها لها. مع أخذ مدخلات أصحاب المصلحة في الحسبان لتوسيع فهم المخاطر، تظهر أيضًا الفائدة المضافة في تحديد التدابير التي يمكن اتخاذها للتخفيف من المخاطر، وتلك التي أثبتت فعاليتها، والإجراءات التي لم تنجح في الماضي. يجب أن تركز هذه التدابير أو "تدابير التخفيف" على الوقاية (لتقليل احتمالية تحقّق الخطر) والتخفيف (من الأثر في حالة وقوع الخطر)، ربما من خلال التجنب، والردع، أو الحماية، أو كل هذه الخيارات أو بعضها.

من المفيد أخذ هذه الإرشادات بعين الاعتبار لتطوير تدابير تخفيف مخاطر الأمان الّتي قد تساور منظّمتنا:

الاحتمالية ما هي احتمالية حدوث الخطر؟					
تقريبًا مؤكّدة 5	متوسطة 5	مرتفعة 10	مرتفعة جدًا 15	شديدة 20	شديدة 25
محتملة 4	متوسطة 4	متوسطة 8	مرتفعة 12	مرتفعة جدًا 16	شديدة 20
متوسطة الاحتمال 3	منخفضة 3	متوسطة 6	متوسطة 9	مرتفعة 12	مرتفعة جدًا 15
غير محتملة 2	منخفضة جدًا 2	منخفضة 4	متوسطة 6	متوسطة 8	مرتفعة 10
نادرة 1	منخفضة جدًا 1	منخفضة جدًا 2	منخفضة 3	متوسطة 4	متوسطة 5
	ضئيلة 1	طفيفة 2	بارزة 3	كبيرة 4	شديدة 5
	الأثر / النتيجة ما مدى خطورة النتائج في حال حدوث الخطر؟				

علينا أن نضمن توافق تدابير التخفيف مع استراتيجيتنا الشاملة لإدارة مخاطر الأمان. الهدف الأساسي من إدارة مخاطر الأمان هو تمكين منظمتنا ومواردنا البشرية من الاستمرار في المشاركة وتنفيذ البرامج على الرغم من مستويات المخاطر. لذا، يتعين علينا ضمان التطابق بين تدابير التخفيف واستراتيجية إدارة مخاطر الأمان المرعية لدى منظمتنا، سواء كانت قائمة على القبول، أو الحماية، أو الردع.

كما ينبغي **تحديد الأولويات لهذه التدابير بناءً على تقييم المخاطر، مع التركيز على نتائج تقييم مخاطر الأمان،** معتمدين على تحليل دقيق لكل تهديد من حيث احتماليته وتأثيره وكيفية ترابطهما مع تصنيف مستوى مخاطر الأمان. فمثلًا، إذا أشار تقييم المخاطر إلى أن التهديد معين غير محتمل ولكنه سيكون ذا تأثير شديد إذا وقع، فإن التدابير التي تركز فقط على تقليل الاحتمالية لن تُسهم بفعالية في تقليل وطأة المخاطر الكلية.

يهدف وضع تدابير الوقاية الفعالة إلى تقليل احتمالية تحقق التهديد، من الضروري لمنظمتنا تحديد الإجراءات الوقائية التي يمكن اعتمادها لمنع أو خفض احتمالية وقوع التهديد.

بالمثل، يجب علينا **تحديد تدابير الاستجابة التي تعزز استعداد منظمتنا وقدرتها على التعامل مع التهديدات بما يساعد في تخفيف آثارها.** يُعتبر وضع تدابير الاستجابة أمرًا حيويًا خاصةً في التعامل مع التهديدات غير القابلة للوقاية مثل الكوارث الطبيعية، أو تداعي البنية التحتية، أو التحديات السياسية. مثال على ذلك تطوير أنظمة التحذير المبكر أو استخدام المؤشرات الموثوقة للإشارة إلى تصاعد مثل هذا الضّرب من المخاطر.

فيما يلي بعض المؤشرات الشائعة الّتي تدل على وقوع خرق في الأمان السيبراني:

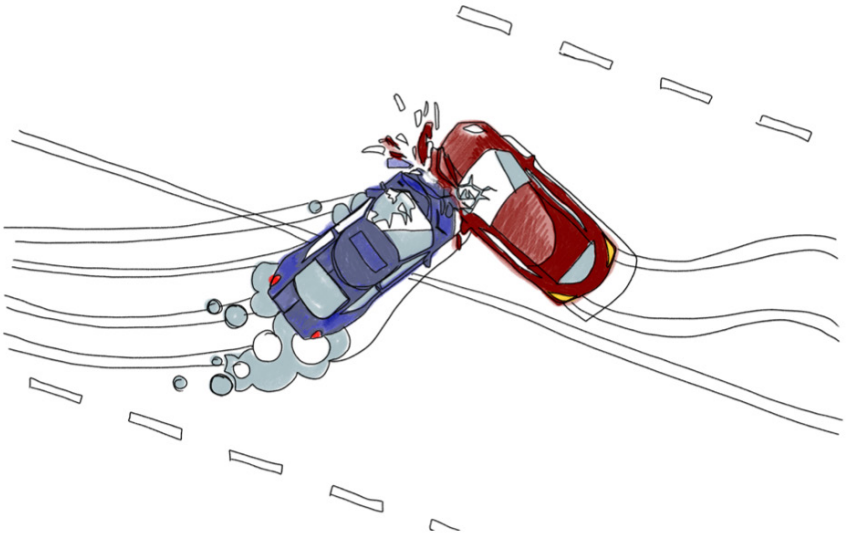
- سجلات خادم الويب التي تُظهر استخدام أداة فحص الثغرات
- تهديد من مجموعة يشير إلى أن هجومًا سيبرانيًا وشيكًا (برمجيات الفدية)
- نشاط مستخدم/ة غير عادي
- قفل حسابات المستخدمين/ات بشكل غير متوقع
- تنبيهات من برمجيات مكافحة الفيروسات/البرمجيات الخبيثة
- انحراف غير عادي عن تدفقات حركة الشبكة النموذجية
- تغييرات في التكوين لا يمكن تتبعها إلى تحديثات معروفة

تطوير تدابير التخفيف بالتعاون مع منظمات شريكة

إذا كانت منظمتنا تعمل بشراكة مع منظمات محلية أو دولية لتنفيذ المشاريع، أو تختار العمل مع منظمة محلية كوسيلة لتقليل تعرضها للمخاطر، فمن المهم التعرف معًا على المخاطر التي قد تؤثر على كلتا المنظمتين وإيجاد طرق لتخفيف هذه المخاطر معًا.

تحديد المستوى المقبول من المخاطر المترسبة

بعد تطبيق التدابير المناسبة للسيطرة على المخاطر المحددة في تقييم مخاطر الأمان الخاص بنا أو تقليلها، سيظل هناك بعض المخاطر التي تبقى والتي تسمى بالمخاطرة المتبقية أو المترسبة. من المهم لمنظمتنا تحديد ما إذا كان مستوى المخاطرة المتبقية مقبولًا ولن يحول دون تمكن منظمتنا من تحقيق أهدافها وتقديم برامجها بأمان.



*يلقي الفصل الأوّل| التهديدات الرّقمية: المؤشّرات، والوقاية، والاستجابة] نظرة عامة على التهديدات المغطاة في هذا الدليل.

الخطوة الخامسة: الرّصد والمتابعة والتواصل

من خلال تأسيس ممارسة راسخة لإجراء تقييمات المخاطر بانتظام، ترتقي منظمتنا إلى مستوى أكثر تقدمًا في استعدادها للتعامل بكفاءة مع حوادث الأمان السيبراني. يساهم هذا النهج في تعميق فهم أهمية الاستثمار في تدابير الأمان السيبراني والفوائد الملموسة لاستثمارات مثل تقييمات الثغرات واختبار الاختراق. مع وجود فهم واضح للخسائر المحتملة المرتبطة بمخاطر الأمان، يصبح تخصيص الموارد اللازمة للتخفيف من هذه المخاطر قرارًا أوضح وأكثر استنارة، مما يؤدي إلى تبني منهج استباقي ومتين في حماية الأصول الرقمية لمنظمتنا.

الرّصد والمتابعة	النّشر والتّواصل
• التّواصل المنتظم؛ • تحديد الوتيرة الدّالة على الموثوقية؛ • فعالية؛	• التحسين والتقييم؛ • التعقب؛ • التقارير؛

3.1.1| تقييمات مخاطر الأمان السيبراني لمنظمات المجتمع المدني والمؤسّسات الإعلاميّة

على مدى العقدين الماضيين، ومع التقدم المتسارع في تقنيات الاتصال، خاصةً في الفضاء الرقمي، شهدنا تحولات كبيرة في طبيعة التهديدات السيبرانية والرقمية. هذا التطور دفع قادة منظمات المجتمع المدني لتوسيع نظرتهم العالية، متحملين مسؤوليات تنظيمية على المستويات الوطنية (أو الإقليمية) والعالية (ديسيه، 2012).

في مجال الأمان السيبراني والمخاطر الرقمية، رأينا توسعًا في دور قادة منظمات المجتمع المدني، حيث تجاوزوا الحدود التقليدية لمسؤولياتهم. أصبحوا الآن يؤدّون دورًا مركزيًا في مواجهة التحديات الاقتصادية والاجتماعية والبيئية، مُساهمين بشكل متزايد في الحوكمة العالمية (ديسيه، 2012). يُبرز هذا التحول الدور الأساسي لقادة هذه المنظّمات في حمايها من كثيب التهديدات التي يفرضها المشهد الرقمي الّذي لا ينفك يتطوّر ويتغيّر.

بفضل نهجهم الاستباقي في مجال الأمان السيبراني وقدرتهم على التكيف مع المخاطر المستجدة، تتمكن منظمات المجتمع المدني من التنقل في العالم المعقد والمتشابك للتقانة. من خلال مواكبتهم لأحدث التطورات، يضمن قادة هذه المنظمات تطبيق تدابير فعالة لحماية والأفراد، والمنظمات، والأمم من التهديدات السيبرانية والاضطرابات المحتملة في البنية التحتية الرقمية. كما أكد ديسيه في عام 2012 الدور الوازن والمتنامي لقادة منظمات المجتمع المدني في مواجهة المخاطر الرقمية، مشيرًا إلى دورهم الفعّال في تشكيل المشهد العالمي للأمان السيبراني.

يمكن لقادة منظمات المجتمع المدني الاستفادة من عدة مزايا عن طريق إجراء تقييمات المخاطر السيبرانية. تتضمن هذه المزايا تلبية المتطلبات التشغيلية والرّسالة، تعزيز المرانة الشاملة والموقف الأمني السيبراني للمنظمة، والوفاء بالتزامات حيال الحفاظ على أمان الفضاء السيبراني.
يُوصى بأن يقوم قادة منظمات المجتمع المدني بإجراء تقييمات دورية للأمان السيبراني، تتوافق مع الاحتياجات التشغيلية لمنظماتهم، لتقييم وضعها على هذا الصّعيد. من خلال هذه التقييمات، تُنشئ المنظمات قاعدة بيانات أساسية من معايير الأمان السيبراني، على أن تُوظَّف هذه الأخيرة مقياسًا مرجعيا للتقييمات المستقبلية، مما يساعد على استمراريّة التحسين في وضع الأمان السيبراني والمرانة مع إظهار التقدم المحرز.
يُمكن إجراء هذه التقييمات باستخدام الموارد الداخلية للمنظمة أو بالاستعانة بمساعدة خارجية. على سبيل المثال، قد تُجري المنظمات تقييمات لثغرات أمانها السيبراني بفحص سجلاتها داخليًا وإجراء تدقيقات لشبكاتها في الفضاء الرّقمي.

وضع موازنات الأمان الرّقمي وإدارة مخاطر الأمان الرّقمي

إذا كنا جديين في التعامل مع الأمان الرقمي وإدارة المخاطر كمنظمة، فمن الضروري تخصيص موازنة لتدابير الوقاية والاستجابة المحتملة. يمكن تحقيق الأول من خلال إدراجه في موازنات المشاريع، وقد أصبح العديد من المانحين مستعدين لتضمين هذه التكاليف في تمويلهم. أما التدابير اللاحقة، فهي تتطلب عادةً نوعين من التمويل:

- تمويل أولي للإسعافات الأولية الرقمية (الأنشطة التي تديرها مواردنا الداخلية).
- تمويل طويل الأمد للطوارئ أو الأزمات الممتدة، وهذا قد يشمل دعمًا ماليًا خارجيًا من منظمات مثل ديجتال ديفندرز أو غيرها.

من الأهمية بمكان الاعتراف بوقت الفريق المستغرق في تأدية مهام الأمان الرقمي وإدارة المخاطر، سواء للوقاية أو للاستجابة. الأمان الرقمي وإدارة المخاطر ليستا مجرد مهمة صغيرة إضافية، بل هما طيف واسع من المهام التي تحتاج إلى تنسيق ودمج مستدام في موازنة الفريق وممارساته.

المصدر: تكلفة إدارة مخاطر الأمان الرّقمي للمنظمات الأهليّة (بالإنجليزيّة) رابط

3.1.2| تقييم مخاطر الأمان السيبراني في الفضاء الرّقمي للأفراد (للمدافعين/ات عن حقوق الإنسان والصحفيين/ات)

تُواجه منظماتنا في العالم الرقمي تهديدات متعددة مثل اختراق الحسابات، ومصادرة الأجهزة، والرقابة والمراقبة، والرّصد والمتابعة المفرط، وهي أمور قد تتعارض مع حقوق الإنسان. بوصفنا مدافعين/ات عن حقوق الإنسان، غالبًا ما نكون هدفًا رئيسيًا للخصوم والمعارضين.

يواجه المدافعون/ات عن حقوق الإنسان والصحفيون/ات تحديات خاصة في سياق عملهم، حيث يتعرضون غالبًا لاستهداف مكثف من مناهضي وخصوم رسائلهم. يمكن أن يُترجم هذا الاستهداف في شكل تهديدات لسلامتهم الجسدية والنفسية، بالذّات عند تغطية قضايا حسّاسة في مجال حقوق الإنسان. تتحول القضايا التي يسلطون الضوء عليها أحيانًا إلى مصادر خطر مباشر على أمنهم وسلامتهم.

يُعد الاهتمام باحتياجات الأمان وتجارب المدافعين/ات عن حقوق الإنسان مطلبًا لا غنى عنه لبناء مجتمعات رقمية ديمقراطية تُعطي الأولوية للأمان والمرانة. إذ يمثل هذا النهج خطوة أساسية نحو تعزيز مجتمعات تحترم الحقوق وتوفر بيئة آمنة للجميع.

أصبحت الحاجة إلى تقييم المخاطر أكثر أهمية الآن أكثر من أي وقت مضى بالنسبة للصحفيين/ات والمدافعين/ات عن حقوق الإنسان. فقد أتى الإعلان المتعلق بالمدافعين عن حقوق الإنسان وإنشاء ولاية المقرر الخاص بشأن وضعهم لتلبية حاجة التّطرق لدورهم والاعتراف بأهميته في تعزيز احترام

حقوق الإنسان، وأيضًا لتسليط الضوء على خطورة ومدى الانتهاكات التي يتعرضون لها. تعكس هذه الخطوات الاعتراف بالحاجة إلى حماية ودعم الصحفيين/ات والمدافعين/ات الحقوقيين في مساهمتهم الجوهرية لتحقيق وتعزيز حقوق الإنسان.

من الضروري الإشارة إلى أن التركيز المفرط على السياسات والممارسات التقييدية كوسيلة لتحقيق الأمان قد ينطوي على مخاطر. قد يؤدي هذا النهج إلى تقييد حقوق الإنسان والحريات، مما قد يؤدي إلى تطبيق تدابير غير متوازنة أو غير كافية. تمتلك الدول القدرة على استغلال القوانين والممارسات المتعلقة بالأمان السيبراني تحت ذريعة ردع الجرائم أو مكافحة الإرهاب، مما يتيح لها زيادة تحكّمها بالمواطنين والمواطنات.

دروس عمليّة

من الضروري أن يستخدم جميع أفراد منظمتنا ذات تصنيفات مخاطر الأمان السيبراني لضمان توحيد البيانات باختلاف السياقات. وفي حالة التعاون مع منظمات شريكة، يجب علينا مشاركة وفهم المعايير المشتركة لمستوى مخاطر الأمان السيبراني.

لا يُعد تقييم المخاطر مجرد عملية علمية دقيقة، بل إنه يأخذ في الاعتبار السياق التشغيلي وهشاشة الكادر وعوامل أخرى (مثل الخبرة). ومن هنا، يكتسب تقييم المخاطر المُجرى بالتعاون مع الفريق الميداني قيمة خاصة.

أظهر استطلاع أجرته فيريزون في عام 2022 درسًا عمليًا مهمًا؛ حيث وُجد أن الغالبية العظمى من خروقات البيانات (82%) كانت نتيجة خطأ بشري. يُبرز هذا المُعطى أهمية الاستثمار في البرامج التدريبية والتوعوية الشاملة في الأمان السيبراني للكوادر والموارد البشريّة. من خلال تعليم الكادر أفضل الممارسات والمخاطر المحتملة وكيفية التخفيف منها، يمكن للمنظمات تقليل احتمالية الأخطاء البشرية التي قد تسفر عن خروقات بياناتيّة، مما يعزز مرانة الأمان السيبراني للمنظمة إلى حد بعيد.

يشكل تشغيل موقع إلكتروني للتجارة الإلكترونية تحديًا كبيرًا، خاصةً عندما يتعلق الأمر بمعالجة عمليات الدفع والتعامل مع بيانات بطاقات الدفع الحساسة. في ظل خطر اختراق بوابات الدفع، من الضروري توجيه موارد إضافية نحو تعزيز أمان هذه البوابات في منظمتنا. باتخاذ هذا الإجراء، نضمن حماية معلومات الدفع للعملاء بكفاءة، مما يساهم في الحفاظ على الثقة في منصتنا وسلامتها.

إذا كانت منظمتنا تخزن معلومات شخصية يمكن استخدامها لتحديد هوية العملاء، فمن المهم أن نعي الخطر المتمثل في هجمات الحقن. للتصدي لهذا التهديد، يجب أن نولي أهمية قصوى لتدابير التحقق القوية من البيانات المدخلة. من خلال تطبيق بروتوكولات متينة للتحقق من البيانات المدخلة، نستطيع تقليل احتمالية نجاح هجمات الحقن إلى حد بعيد، مما يساعد في حماية سلامة وخصوصية معلومات العملاء.

يمكن أن تؤثر عوامل مثل الجنسية، والعرق، وهوية النوع الاجتماعي، والخبرة على مستوى هشاشة الصحفيين/ات في منطقة معينة. في بعض الحالات، قد يواجه الصحفيون/ات الدوليون مخاطر أقل مقارنةً بالصحفيين/ات المحليين، أو العكس.

من الدروس القيمة المستفادة من بيئة تطوير البرمجيات والعمليات (DevOps)، التي تتسم بنظام عملياتي رشيق وديناميكي، هي الحاجة إلى تقييم المخاطر باستمرار. من المهم التعرف على المخاطر المرتبطة بالأكواد في كل مرة تُوَظَّف في الإنتاج. بتبني هذا النهج الاستباقي، تستطيع المنظمات تحديد الثغرات المحتملة بحثاثة واتخاذ خطوات فورية لتخفيف المخاطر، مما يضمن موثوقية وأمان أنظمتها خلال دورة التطوير والتوظيف.

موارد

- فرونت لاين ديفندرز، كتاب العمل الخاص بالأمن: خطوات عمليّة للمدافعين عن حقوق الإنسان الّذين يواجهون الأخطار: رابط
- منظّمة ألونا للدعم النفسي والاجتماعي (Aluna-Psicosocial، Risk Assessment in Human Rights Defense: Methodological Guide from the Psychosocial Approach [تقييم المخاطر في مضمار الدفاع عن حقوق الإنسان: دليل منهجي من المنظور النفسي الاجتماعي] رابط
- إنتر نيوز، Safer Journo: Digital Security Resources for Trainers of Journalists - Chapter 1: Understanding and evaluating digital risk [موارد الأمان الرّقمي لمدربي الصّحفيين/ات: الفصل الأوّل فهم المخاطر الرّقميّة وتقييمها،] رابط
- أكاديمية دويتشه فيله، Threat Modeling Guide: How to identify digital risks in international development projects [دليل نمذجة التهديدات: كيفية تحديد المخاطر الرّقمية في مشاريع التنمية الدولية،] رابط
- Holistic Security Manual: Explore - Context and risk analysis [الدّليل الشّامل في الأمان الرّقمي: استكشاف وتحليل السياق والمخاطر،] رابط
- التدريبات المتاحة عبر منصّة توتم التّعلّمية الإلكترونيّة: رابط
- تحليل المخاطر: رابط
- نمذجة المخاطر: رابط
- توفر وكالة الأمان السيبراني وأمان البنية التحتية (CISA) أدوات وخدمات سيبرانية مجانية ودون التزام بمشاركة النتائج، مثل أداة تقييم الأمان السيبراني (CSET ®).
- الشبكة الدولية للصحفيين، لسلامة الصحفيين/ات وحمايتهم: ثلاث نصائح
- الشبكة الدولية للصحفيين، نصائح الأمان الرّقمي للصحفيين
- لجنة حماية الصّحفيين، مجموعة أدوات الأمن الرقمي
- توصي منصّة سايف-كوم (SAFECOM) باستخدام الدّليل بالتعاون مع إطار الأمان السيبراني (CSF) من المعهد الوطني للمعايير والتكنولوجيا (NIST)، الّذي يقدّم منظارًا شامل عن الخطوات الأساسيّة لتقييم المخاطر السيبرانيّة.
- مؤسّسة التّخوم الإلكترونيّة، الدّفاع عن النّفس من المراقبة وأدواتها.
- تعتبر وكالة الأمان السيبراني وأمان البنية التحتية مصدرًا لتقييم القدرات الحالية للمرونة، وتحديد

طرق لتحسين المرانة، ووضع الخطط للتخفيف من آثار التهديدات المحتملة لها، أي المرانة.

- منظّمة بِن أمريكيا (PEN America)، Online Harassment Field Manual [التّحرّش الإلكتروني: دليل ميداني].
- فرونت لاين ديفندرز، عُدَّة الأمان: أدوات و ممارسات للأمان الرقمي، التّقانة التّكتيكيّة.
- السّلامة المادّيّة والجسديّة
- لجنة حماية الصحفيين، PPE Guide [دليل معدات الحماية الشخصية].
- مراسلون بلا حدود واليونسكو، دليل السلامة للصحفيين: دليل عملي للصحفيين في المناطق المعرضة للخطر.
- الصّدمات
- موارد مركز دارت للصحافة والصدمة.
- مركز دارت لمنطقة آسيا والمحيط الهادئ وتحالف ثقافة السلامة، Leading Resilience: A Guide for Editors and Newsroom Managers [المرانة القياديّة: دليل للمحررين ومديري غرف الأخبار.]
- موارد ومصادر مؤسّسة ذَا سِلف-اِنفِستِغايشِن (The Self-Investigation).
- المساعدة القانونيّة
- منظّمة مِيديا دِفْنس، الدّفاع الطّارئ.
- أدلّة لجان المراسلين لحريّة الإعلام.
- قسم الاستشارة القانونية لديوان المراسلين الاستقصائيين والمحررين المستقلين (Freelance Investigative Reporters and Editors)
- قسم الدعم القانوني لشبكة القانونيّة للصحفيين المعرضين للخطر (Legal Network for Journalists at Risk).

النّماذج

تحديد التهديدات والمخاطر ومسحها:

ماذا نقصد بالتّهديد؟

لنُعد قائمة بجميع التهديدات التي يمكننا تحديدها في بيئة عملنا:

_____
_____
_____
_____

أين تكمن التهديدات؟

علينا تحديد مكامن التهديدات بدقة، بحيث نبت ما إذا كانت هذه التهديدات تقتصر على منطقة بعينها أو عدة مناطق، أو لربما تمتد على نطاق منطقة بأكملها.

_____
_____
_____
_____

من أو ما الذي يتعرض للخطر؟

علينا التفكير في كافّة الأشخاص والأشياء المحتمل تعرضها للخطر، مثل:

الكوادر الدولية
الكوادر المحلية
أفراد المجتمع
المركبات
المواد الإغاثة

_____
_____
_____
_____

ماذا نقصد بالأثر؟

يتطلب منا ذلك تقييم الآثار المحتملة والنتائج المترتبة على هذه التهديدات، بحيث نقيّم مدى خطورة التأثير على منظمتنا.

على سبيل المثال، مثل فحص مدى خطورة تأثير تهديد سرقة السيارات على أمان الفريق وأصول المنظمة.

_____
_____
_____
_____

مصفوفة المخاطر

ما هي احتمالية الحصول على الفائدة؟ الاحتمالية	الفائدة						الخطورة						ما هي احتمالية حدوث الخطر؟ الاحتمالية
	تقريبًا مؤكّدة 5	جيدة 5	جيدة جدًا 10	كبيرة 16	ممتازة 20	ممتازة 20	شديدة 25	شديدة 20	مرتفعة جدًا 15	مرتفعة 10	متوسطة 5	تقريبًا مؤكّدة 5	
	محتملة 4	جيدة 4	جيدة 8	جيدة جدًا 12	كبيرة 16	ممتازة 20	شديدة 20	مرتفعة جدًا 16	مرتفعة 12	متوسطة 8	متوسطة 4	محتملة 4	
	متوسطة الاحتمال 3	محدودة 3	جيدة 6	جيدة 9	جيدة جدًا 12	كبيرة 16	مرتفعة جدًا 15	مرتفعة 12	متوسطة 9	متوسطة 6	منخفضة 3	متوسطة الاحتمال 3	
	غير محتملة 2	منخفضة جدًا 2	محدودة 4	جيدة 6	جيدة 8	جيدة جدًا 10	مرتفعة 10	متوسطة 8	متوسطة 6	منخفضة 4	منخفضة جدًا 2	غير محتملة 2	
	نادرة 1	منخفضة جدًا 1	منخفضة جدًا 2	محدودة 3	جيدة 4	جيدة 5	متوسطة 5	متوسطة 4	منخفضة 3	منخفضة جدًا 2	منخفضة جدًا 1	نادرة 1	
		ضئيلة 1	طفيفة 2	بارزة 3	كبيرة 4	شديدة 5	شديدة 5	كبيرة 4	بارزة 3	طفيفة 2	ضئيلة 1		
		أثر إيجابي					أثر سلبي						
		الأثر / الفائدة إلى أي حد يمكن أن تكون النتائج ممتازة في حالة حدوث التأثير؟					**الأثر / العاقبة** ما مدى خطورة النتائج في حال حدوث الخطر؟						

الفئات	المخاطر التي تم تحديدها	الاحتمالية	الأثر	المخاطر الفعلية	تدابير التخفيف	الاحتمالية	الأثر	المخاطر المتبقية	المالك	حالة تنفيذ تدابير التخفيف	ملاحظات

قراءات إضافيّة:
مسرد منصّة توتم التّعلّمية الإلكترونيّة

3.2| سياسات وإجراءات الأمان الرّقمي

بعد تحديد التهديدات الرقمية المحتملة في أنشطتنا، يمكننا الشروع في وضع خطط الأمان الرقمي أو بروتوكولات الأمان ضمن إطار سياسات وخطط الأمان. هذه الخطط، سواء كانت رسمية وموثقة أو غير رسمية وقائمة على التفاهمات المشتركة، يجب أن نتعامل معها كوثائق دينامية قابلة للتحديث المستمر. كذلك ينبغي للتسمية المعتمدة لهذه الوثائق أن تُستمَد من ثقافة الفريق أو المنظمة والوثائق الإرشادية المتاحة، ومن الضروري اختيار أسماء تتوافق مع ثقافة المنظمة لتسهيل الفهم والتنفيذ الفعال لهذه السياسات والإجراءات.
يمكننا تنظيم خططنا واتفاقيات الأمان الرقمي بأي طريقة تناسب أسلوب عملنا، سواء بناءً على نوع الأنشطة، أو مناطق عملنا، أو المسؤولين، أو أيام الأسبوع، أو أي معيار آخر. بغض النّظر عن الطريقة، لا بدّ للخطط أن تشمل بعض العناصر الأساسية:

- سياسة الأمان الرقمي: توضح هذه السّياسة الأهداف والأشخاص المشمولين.
- إجراءات التشغيل القياسية: تشمل هذه الإجراءات كلمات المرور، وأمان السفر، والاتصالات، والمعلومات.
- أدلة أو إرشادات الأمان الرقمي: تشمل هذه المراجع أدلة أدوات إدارة كلمات المرور، والمصادقة الثنائية، وصيانة الأجهزة.

تختلف طريقة ترتيب وتنظيم وثائق الأمان الرقمي من مؤسسة لأخرى. تفضل بعض المؤسسات وجود سياسة أمان رئيسة واحدة تشمل جميع الوثائق الأخرى المتعلقة بالأمان الرقمي، تليها إجراءات التشغيل القياسية للأمان الرقمي أو أمان المعلومات. هذا التنظيم يعكس الثقافة التنظيمية الخاصة بكل مؤسسة، إلى جانب الممارسات والمصطلحات المستخدمة فيها. وفيما يلي تفصيل عن محتوى هذه الهيكلة الوثائقية إن جاز التعبير.

سياسة (ومدونة السلوك)

تُعرف السياسة بأنّها بيان يعبر عن النوايا ويُطبَّق كإجراء أو بروتوكول، وغالبًا ما تُعتمد السّياسات من هيئة الحوكمة داخل المؤسسة. تبين السياسة الأطراف المعنية، والأدوار والمسؤوليات بشكل عام، وتتضمن ملخصًا لإجراءات التشغيل القياسية المرتبطة بإدارة مخاطر الأمان الرقمي. تُحافظ هذه الوثائق على البساطة قدر الإمكان وتُراجع سنويًا أو حسب الحاجة، حيث تُعدّها الأمانة العامة أو مدير/مستشار/منسّق الأمان الرّقمي، بينما تتولّى الجمعية العامة أو مجلس الإدارة أو الإدارة العليا مهمّة القرارات المرتبطة بها.

إجراءات التشغيل المعياريّة

تُستخدم إجراءات التشغيل المعيارية كطرائق محددة ومرعيّة لأداء عمليات محددة أو في حالات خاصة. تحدد هذه الإجراءات الأشخاص المعنيين والأدوار والمسؤوليات بتفصيل جم. يجب توفر إجراءات تشغيل قياسية لجميع المجالات والعمليات التي تحتاج إلى تنظيم، بما في ذلك أمان المعلومات، والسفر، وتقييم المخاطر، وقدرات الشركاء، وأجهزة تقانة المعلومات، إلخ. من المهم أيضًا وجود إجراءات

للحالات الرقمية الطارئة ومراجعتها بانتظام. يجب الحرص على عدم زيادة عدد الإجراءات لتجنب الإرهاق، وتُراجع سنويًا أو حسب الحاجة، على أن يُعهد بتحديثها لمدير/مستشار/منسق الأمان، بينما يُبت بالقرارات المتعلقة بها من طرف فريق الأمان أو الإدارة العليا.

الأدلّة أو الإرشادات المحدّدة حسب الموضوع أو السّياق

توفر الإرشادات والأدلّة المواضيعيّة أو السيّاقيّة تعليمات تفصيلية للتعامل مع مواقف أو أعمال معينة مثل تقانة المعلومات والاتصالات وإدارة الحوادث، وإعداد التّقارير. يمكن لأي شخص في المنظمة يرى الحاجة لإرشادات معينة صياغتها، ويتم الاتفاق عليها من الجهة المختصة. تشمل هذه الإرشادات قوالب وخطط طوارئ وتعليمات تكنولوجيا المعلومات. يُشدد على ضرورة وجود إرشادات واحدة فقط لكل مجال، ويتم تحديثها دوريًا. تُراجع هذه الإرشادات حسب الحاجة، يُعد هذه الإرشادات فريق الأمان أو المديرين، او الكادر العام، ويتولّى فريق/مستشار/مديري الأمان مهمّة التّقرير بشأن هذه الإرشادات على المستوى المركزي.

ملاحظات عامة بشأن السّياسات والإجراءات

من الضروري التأكد من التناسق الداخلي بين السياسة/مدونة السلوك وإجراءات التشغيل القياسية والإرشادات في المؤسسة. يجب ضمان أن تشتمل إجراءات التشغيل والإرشادات على إشارات متبادلة عند الضرورة، خاصةً في حال وجود تداخل أو ترابط بينهما، مثل العلاقة بين أمان المعلومات وأمان السفر وتقييم قدرات الشركاء والمخاطر. من المهم أيضًا تحديد التّاريخ والجهة المسؤولة عن تقرير بشأن كل وثيقة.

أدوات وموارد متاحة عبر الإنترنت لإعداد وثائق الأمان الرّقمي

بينما يمكننا إعداد وثائق الأمان الرّقمي الخاصة بنا بشكل مستقل وفقًا لإجراءات العمل الداخلية والوثائق الأمنية الموجودة لدينا، يمكننا أيضًا استخدام قوالب وأدوات وموارد متاحة عبر الإنترنت مثل:

- أداة الحفاظ على أمان المنظّمات من خلال صناعة السياسات المُؤتمتة، وهي أداة بسيطة تُمكّن منظّمات المجتمع المدني من بناء سياسات أمان أفضل وأمتن: رابط
- أكاديمية دويتشه فيله، فاحص التّهديدات، أداة مُتاحة عبر الإنترنت تُساعدنا على تحديد التّهديدات السيبرانيّة والخروج بتوصيات سياساتيّة لحماية مؤسّساتنا الإعلاميّة: رابط
- تقارير العملاء: أداة تخطيط الأمان للحفاظ على بياناتنا بأمان من خلال خطّة أمان مُحاكة خصيصًا لسياقنا: رابط
- الأمان أوّلًا: تطبيق الشّمسيّة، القوائم التّحقق والتدقيق: رابط

الموارد

- Holistic Security Manual: Creating security plans and agreements [دليل الأمان الشامل: إنشاء خطط واتفاقات الأمان]: رابط
- فريق مساعدو الأمان الرقمي باكساس ناو، Basic guide to help organizations create and implement a security policy [دليل أوّلي لمساعدة المؤسّسات على إعداد سياسات الأمان وتنفيذها،] رابط

- المعهد الوطني الديمقراطي، Cybersecurity Handbook For Civil Society Organizations: A guide for civil society organizations looking to get started on a cybersecurity plan [دليل الأمان السيبراني للمنظمات المدنية: دليل موجه للمنظمات المدنية الراغبة في تطوير خطة للأمن السيبراني،] رابط

3.3| الاستجابة للحوادث والطوارئ

على الرغم من جهودنا الكبيرة في تقييم المخاطر والتخطيط الأمني لتقليل احتمالية تحول التهديدات الرقمية إلى حوادث، وللحد من تأثير الهجمات والحوادث الرقمية، من الضروري أن نكون مستعدين للاستجابة للحوادث الرقمية. قد تتحول هذه الحوادث إلى طوارئ أو أزمات، اعتمادًا على نوع الحادث وقدرتنا على الاستجابة. من الأهمية بمكان أن يكون لدينا إجراء واضح وتدفق عمل للتعامل مع الحوادث الرقمية، بما في ذلك الإبلاغ عنها، توثيقها، الاستجابة لها والتعلم منها.
هناك ثلاثة عناصر رئيسة للاستجابة لحوادث الأمان السيبراني:

1. توثيق ومشاركة الحوادث (أي الإبلاغ عنها)
2. والاستجابة للحادث
3. والمتابعة والتعلم (إدارة المعرفة)

في حالات الطوارئ أو الأزمات، يشمل العنصر الثاني مكونًا خاصًا بالأزمات أو الطوارئ.
في خطوة الاستجابة للحوادث الرقمية، يتم عادةً إشراك الأشخاص المسؤولين عن بنية تقانة المعلومات وصيانتها داخل المنظمة. وعلى أساس تقييم هؤلاء الأشخاص، يقرر مستوى الإدارة المعني الاستعانة بفريق استجابة الحوادث أو ما يماثله للتعامل مع الوضع.

خطط الاستجابة للحوادث

استنادًا إلى التهديدات التي قد نواجهها في أثناء الأنشطة، لا بدّ من وضع خطط للاستجابة للحوادث لتمكين القيام برد حثيث دون الحاجة إلى اتخاذ قرارات معقدة. تتضمن خطط استجابة الحوادث إجراءات تشغيل قياسية تحدد مسؤوليات الأشخاص (مثل فرق الاستجابة للحوادث)، والموارد المستخدمة، والإجراءات العامة، وزمن إنهاء الحادث. كما ثمَّ حاجة لإرشادات محددة لأنواع مختلفة من الحوادث الرقمية مثل خرق الحسابات، وفقدان البيانات والأجهزة، والهجمات الرقمية على البنية التحتية أو المواقع الإلكترونية، والتحرش الرّقمي.

فرق الاستجابة للحوادث

لضمان فعاليّة الاستجابة للحوادث، لا بدّ لنا من اعتماد على عضو واحد فقط كنقطة مركزيّة للأمان، بل تشكيل فريق يتمتع أعضاؤه بصفات متنوعة مثل على سبيل الذّكر لا الحصر:

- القدرة على اتخاذ القرارات: تأتي عادةً من الإدارة.
- الخبرة التقنية: للتعامل مع مسؤوليات تقانة المعلومات.
- القدرة على تنسيق الاستجابة للحوادث: تُعزى للنقاط الأمان المحورية.
- القدرة على المساعدة في توثيق الاستجابة: لتسهيل التنسيق وعمليات التعلم.

من أجل الاستجابة الفعالة للحوادث، من المهم عدم الاعتماد فقط على عضو فريق واحد مسؤول بحيث يشكل نقطة مركزية فيما يتعلّق بالأمان، بل تشكيل فريق يضم أعضاء يتمتعون بالصفات التالية:

- القدرة على اتخاذ القرارات (الإدارة).
- الخبرة التقنية (للتعامل مع مسؤوليات تقانة المعلومات).
- القدرة على تنسيق الاستجابة للحوادث (النقاط الأمان المحوريّة).
- القدرة على المساعدة في توثيق جميع خطوات الاستجابة لتسهيل التنسيق المتغير وعمليات التعلم.

وفي بعض الأحيان، قد نحتاج إلى إشراك طرف داخلي أو خارجي يتمتع بالقدرة على تقديم الدعم العاطفي لفريق استجابة الحادث.

من المهم تخصيص وقت كافٍ لأعضاء فرق الاستجابة للحوادث للتأهب والتّهيؤ، وبالتّالي أداء أدوارهم بنجاعة. خلال الطوارئ الرّقميّة، لا بدّ من تفريغ هذه الكوادر من أي مهام أخرى. إذا تطور حادث إلى طارئ أو أزمة جرّاء مدته أو آثاره، فلا بدّ للفريق من العمل على نحو مستدام وتنظيم العمل بنوبات دوريّة. من الضروري أيضًا توفير فترات راحة لأعضاء الفريق للحؤول دون استنفاد طاقتهم وتجنب إرهاقهم، مما يساعد في منع حدوث أزمة داخلية إضافية ناتجة عن الإجهاد الشديد.

3.4| متابعة الحوادث: التعافي والرعاية اللاحقة واستقاء الدّروس

حتى بعد استعادة الأنظمة والبنية التحتية الرقمية للعمل وصد الهجمات الرقمية، قد تظل هناك تأثيرات عاطفية ونفسية أخرى تحتاج إلى معالجة. من الضروري الاهتمام بهذه التّبعات فور انتهاء الحادث، أو الطّارئ، أو الأزمة، وقد تستمر هذه الحاجة على المدى الطويل.

الرعاية العاطفية

إن التعامل مع الآثار العاطفية (ردود الفعل العاطفية للصدمة، والإرهاق، والإنهاك، والنّزاعات الداخلية، إلخ.) والمؤسسية (مثل إعادة بناء الثقة في البنية التحتية الرّقمية والمسؤوليات، إلخ) للحوادث يتطلب رعاية واحترافية. من الضروري عدم الاكتفاء بالحلول الفردية مثل تقديم الدعم المالي للعلاج، بل يجب التركيز على الرعاية الجماعية، تحمل المسؤولية الجماعية، واتخاذ خطوات مشتركة للتعافي ومعالجة الآثار المستمرة كفريق واحد.

تمويل الرعاية اللّاحقة

لضمان توفير رعاية لاحقة فعّالة، من الضروري إما تخصيص جزء من الموازنة مسبقًا لهذا الغرض، أو العمل على تأمين الوصول إلى شبكات التمويل التي يمكن أن تدعم الاحتياجات المالية بعد الحوادث الطارئة.

اتساق الدّروس وإدارة المعرفة

من الصّعب تعلّم الدروس في خضمّ الأزمات والطّوارئ إذ يُضحي بقاؤنا جُل هم أجهزتنا العصبيّة وبؤرة تركيزها. مع ذلك، من المهم تخصيص وقت لتحليل ومعالجة الأسباب الكامنة خلف الأزمات والطّوارئ، وتقييم فعالية استجابتنا لها، وآثارها الجانبية وكيفية التخفيف منها.، عدا ما ننوي تحسينه لمعالجة ما قد يستجد من حوادث. علينا أيضًا مراجعة جميع الوثائق بعد الأزمة، وجمع الإفادات الإغنائيّة للمتأثرين المباشرين وغير المباشرين (بالمباشرين نُشير مثلًا إلى فريق الاستجابة لحوادث الأمان السيبراني، والشّركاء؛ وبغير المباشرين نشير مثلًا إلى أعضاء الفريق الّذين تولّوا مهام إضافيّة للأخذ من حمل فريق الاستجابة الطّارئة أو ما شابه ذلك).

ولإكمال دائرة استقاء الدّروس علينا بالخطوات الأساسيّة التّالية:

- إعداد خطط تنفيذية لجميع خطوات تحسين الأمان الرّقمي وإدارة المخاطر.
- ومراجعة وتحديث جميع الوثائق ذات الصلة بأماننا الرّقمي وإدارة المخاطر.

3.5| توثيق الانتهاكات الرّقميّة

يتسند محتوى هذا المحور إلى الإرشادات العامّة على موقع Acoso.online، بالذّات بشأن كيفية الإبلاغ عن الانتهاك والحفاظ على الأدلة، يُذكر أن هذه الإرشادات متاحة عبر الرابط. أفاد المحور أيضًا من مادّة توثيق الانتهاكات الرّقميّة الطّارئة ضمن عدّة الإسعاف الأوّلي الرّقمي (سَتُنشر قريبا).

مع تزايد الهجمات الرقمية، من الضّروري توثيق هذه الحوادث لعدة أسباب وأهداف، بما في ذلك:

- استعادة وتعزيز القدرة على التّحكّم في أثناء الهجمات وبعدها.
- الاستعداد للتعامل مع التهديدات والهجمات المستقبليّة، وذلك من خلال تقييم المخاطر والتخطيط الأمني.
- طلب المساعدة من جهات موثوقة.
- الإبلاغ عن الحوادث إلى منصات التواصل الاجتماعي والفرق التقنية.
- تدعيم القضايا القانونية أو طلب الحماية من الأجهزة الأمنية.
- تدعيم التّقارير الجنائيّة.

من الضّروري الإدراك بأنّ توثيق العنف الرّقمي المُقترف بحقنا أو بحق سوانا ليس بالعملية السهلة، بل هو عملية مرهقة عاطفيًا وقد تردّنا في بعض الحالات إلى مربّع الصّدمة مجدّدًا. لذا يُنصح بألّا نخوض عمليّة التّوثيق بمفردنا، بل الاستعانة بفريق داعم أو مجتمع مساند لاجتياز الأعباء العاطفيّة لهذه العمليّة. إذا كنا نستعد لتوثيق عنف رقمي مُورس بحقّنا، يمكن اختيار شخص آخر موثوق أو محترف لتولي هذه المهمّة لتقليل الضّغط العاطفي الّذي يُمكن أن يقع علينا.

خطوات ينبغي لنا اتباعها عند التّوثيق:

- توثيق أكبر قدر ممكن من التفاصيل، بما في ذلك التفاعلات مع المهاجمين والتأثيرات العاطفية والجسدية لهذه التفاعلات. لهذا الغرض يُمكننا استخدم سجل رقمي أو مستند نصّي، وقد يكون من المفيد أيضًا استخدام تقويم منفصل عبر الإنترنت لتتبع الأحداث.
- ينبغي أن يشتمل كل سجل لحادثة رقمية على تاريخ ووقت وقوعها، عناوين البريد الإلكتروني للمهاجمين والرّوابط ذات الصّلة، كما وأسماء المستخدمين الضّالعين، ونوع الهجوم. يمكن

الرجوع إلى مثال هيكل الأدلة المتاح عبر Acoso.online. (يمكننا الاطلاع على مثال هيكلة الأدلة في موقع Acoso.online).

- يتعين علينا أن نُحتفظ بمجلد خاص لحفظ لقطات الشاشة للرسائل والصور التي يرسلها المعتدون أو تلك التي تظهر آثار ما نتعرض له أو نشهده من هجمات رقميّة. كذلك يمكننا البحث في الإنترنت عن كيفية أخذ لقطة شاشة تتوافق مع نوع وطراز جهازنا ونظام التشغيل الخاص به، مثل سامسونغ غلاكسي اِس.21. لحفظ صورة معينة، يمكن الضغط مطولًا على الصورة في الهاتف المحمول أو استخدام زر الفأرة الأيمن على الحاسوب، أو استخدام مفتاح التحكم على جهاز ماك أو مفتاح القائمة المنسدلة في ويندوز، لاستخدام خيار "حفظ الصورة باسم".
- عند أخذ لقطات الشاشة للتوثيق، يجب التأكد من تضمين الساعة والتاريخ المعروضين على الجهاز في الصورة. هذا الإجراء يوفر إطارًا زمنيًا دقيقًا للحادثة. بالمقابل، ينبغي الحذر لتجنب ضم معلومات حساسة غير مرتبطة بالحادثة، مثل رسائل شخصية أو بيانات خاصة، والتي قد تشكل خطرًا إذا ما تمت مشاهدتها أو توثيقها.
- عند توثيق مواقع الويب، فمن الأهمية بمكان التأكد من ظهور عنوان الصفحة (URL) في لقطة الشاشة. فهذا التّفصيل مهم لتوثيق موقع الحادثة، بالذّات في حالات التحرش أو الهجمات الرّقمية، حيث يسهل على المحترفين التقنيين والقانونيين تحديد الموقع وفهم سياق الحادثة.
- عند توثيق الرسائل الإلكترونية، ينبغي التركيز على التّرويسة الخاصة بكل بريد إلكتروني، لما تحويه من معلومات مهمّة عن المرسل وآلية الإرسال (مثل العناوين والأختام على الرّسائل الورقيّة). يمكن لحفظ هذه المعلومات إعانة الأشخاص الذين يحاولون مساعدتنا. نجد في الرّابط المضمّن بهذا النّص إرشادات بشأن كيفية عرض وحفظ ترويسات الرسائل الإلكترونية.
- أما بالنسبة لتوثيق مقاطع الفيديو، فمن المهم توفير قرص صلب خارجي (أو محرك أقراص، أو وحدة لنقل البيانات، أو فلاش) لحفظها. يمكن استخدام خيار "الحفظ باسم"، أو تسجيل الشاشة، أو استخدام ملاحق تحميل الفيديو (Video DownloadHelper) في المتصفح لهذا الغرض.
- عند حفظ المعلومات التي وُثِّقَت، ينبغي اتخاذ الاحتياطات الضرورية لضمان سلامتها. من المستحسن أيضًا حفظ النسخ الاحتياطية على الجهاز نفسه بدلًا من الإنترنت أو خدمات التخزين السّحابي. كذلك يُنصح باستخدام تقنيات التشفير وتخزين البيانات في مجلدات مخفية أو أقسام متعدّدة من محرك الأقراص الصلبة. هذا يقلل من مخاطر فقدان هذه السجلات أو تعرضها للكشف.

عند التعامل مع الهجمات الرقمية القائمة على النوع الاجتماعي، من المهم:

- طلب الدعم من جهة أو شخص نثق به مساعدتنا؛ إذ قد تُثير عمليّة التّوثيق ذكريات موجعة؛ لذا من الممكن أن نطلب من صديق أن يجمع الأدلّة، وبتالي تخفيف وطأة صدمة التّجربة وآثارها. من المهم أيضًا أن نجد شخصًا يلازمنا ويساعدنا ألّا نُهمل تغذيتنا ويساعدنا على أخذ قسطا من النّوم والرّاحة، ويستمع إلينا إن أردنا البوح بمخاوفنا، واستعادة إحساسنا بالأمان. نجد في الرّابط المُضمّن لهذا النّص جُملة من النصائح الإضافية عن سُبل طلب المساعدة من العائلة أو الأصدقاء.

- من المهم أيضًا تذكير النفس بأن حذف الأدلة لا يعني أنّ الحادثة لم تحدث.
- إن إعداد جدول زمني لتوثيق كافّة الأحداث المتعلّقة بالهجمات الرقمية يُعتبر خطوة مهمة. يتضمن هذا الجدول كل ما نستطيع تسجيله، من المعلومات التّقنية إلى المشاعر الشّخصيّة، مما يساعد في رسم صورة شاملة لسلوك المعتدين والمخاطر التي نواجهها، بالإضافة إلى التداعيات التقنية والأشخاص الضّالعين. من الضّروري أن نقرر ما الّذي سنسجله من هذه المعلومات وكيف، وأن نضع استراتيجية لكيفية التعامل مع هذه العملية.
- عند طلب المساعدة في المدرسة، أو العمل، أو من كادر الموارد البشرية:
- ينبغي لنا أن نضع في اعتبارنا أنه عند طلب المساعدة من مؤسسة، ليس من الضروري مشاركة المواد الشخصية إن لم نرغب في ذلك.
- نجد في الرّابط المُضمّن لهذا النّص جُملة من النصائح الإضافية بشأن التحدث مع صاحب العمل عمّا قد نوجهه من مضايقات.
- وهنا نجد بعض الإرشادات لأصحاب العمل بشأن ممارسات التّحرّش والمضايقات الّتي يُمكن أن تحدث في أماكن العمل ويُمكن مشاركتها مع أرباب العمل، هذه الإرشادات صادرة عن منظّمة بِن أمريكيا (PEN America).

عند توثيق الانتهاكات والإبلاغ عنها لدى منصات التواصل الاجتماعي وفرق العمّل المختصّة الأخرى:

- عند الرغبة في الإبلاغ عن الانتهاكات أو المضايقات التي تحدث على منصّات التّواصل الاجتماعي، يُمكننا العثور على روابط صفحات الإبلاغ الخاصة بالعديد من هذه المنصات عبر موقعي Security in a Box و Acoso.online. هذه الروابط تسهل عملية الوصول إلى الإجراءات المناسبة للإبلاغ وتقديم الشكاوى بشكل مباشر وفعّال.
- يمكننا البحث عن روابط صفحات الإبلاغ للعديد من منصات التواصل الاجتماعي المعروفة على موقعي عُدَّة الأمان: أدوات وممارسات للأمان الرقمي وموقع Acoso.online.
- من المهم أن نكون جاهزين لمشاركة الأدلة التي جمعناها في سجلنا الرقمي، مثل روابط الصفحات، ولقطات الشاشة، والصور، مع المنصات ومزودي خدمات الإنترنت وشركات التكنولوجيا. هذه الأدلة ستمكنهم من تقديم المساعدة بفعالية أكبر.

عند التّوثيق ضمن إطار قضايا قانونيّة:

- علينا النظر بعناية في ما إذا كنا نريد المضي قدمًا في رفع قضية. من المهم تقييم المخاطر المحتملة المرتبطة بمثل هذه الخطوة، بما في ذلك التعرض لأخطار إضافية. يجب أيضًا أن نأخذ في الاعتبار الوقت والجهد اللازمين لمتابعة الإجراءات القانونية وما إذا كانت لدينا الموارد والقدرة على تحمل هذا العبء.
- عند التعامل مع التهديدات الرقمية والتوثيق لأغراض قانونية، من الضروري أن نقوم ببحث دقيق في الإجراءات القانونية المتبعة في بلدنا ومنطقتنا. هذا البحث سيساعدنا في فهم الخطوات القانونية المطلوبة وكيفية إعداد الأدلة بشكل يلائم المتطلبات القضائية.
- في حالة اتخاذ قرار برفع دعوى قضائية بشأن المضايقات الرقمية، يُعتبر طلب الحفاظ على البيانات من المنصات أو مزودي خدمات الإنترنت خطوة مهمّة. عادةً، يُمكن لهذه الجهات الاحتفاظ بالبيانات المتعلقة بالمضايقات لفترة محددة، قد تمتد لبضعة أسابيع أو شهر. من المهم الاطلاع

على الإرشادات المتاحة من منظمات مثل Without My Consent، التي توفر معلومات مفصلة بشأن كيفية تقديم طلبات الحفاظ على البيانات والدعاوى القضائية للتعامل مع هذه الحالات.

عند التوثيق للتقارير الجنائية:

- عند التعرض لتهديدات رقمية دقيقة، كبرمجيات التجسس أو الرسائل الإلكترونية الخبيثة، يُفضل جمع أدلة تقنية مفصلة. من الضروري حفظ ملفات السجل من الهواتف والحواسيب، والتحقق من علامات EXIF في الصور لمعرفة تفاصيل مثل مكان وزمان التقاطها. تُعد المرفقات الخبيثة في الرسائل الإلكترونية أيضًا مصدرًا قيمًا للأدلة. يُنصح بتوخي الحذر وعدم فتح هذه المرفقات مباشرةً، والاستعانة بخبير تقني للتعامل معها بأمان. عند التعامل مع المرفقات الإلكترونية المشبوهة، يجب تجنب فتحها أو النقر عليها تحت أي ظرف. يُمكن لخبير تقني موثوق أن يساعد في التعامل مع هذه المرفقات بأمان وتحويلها للتحليل. كما يُفيد تنزيل صفحات الويب بأكملها أو الاحتفاظ بها كنسخة احتياطية لتوفير أدلة مفصلة لمن يسعى لمساعدتك. ذا كانت الصفحة التي تعرضنا فيها للمضايقات متاحة للعامة ويمكن الوصول إليها بدون الحاجة لتسجيل الدخول، فإحدى الخطوات التي يمكننا اتخاذها هي إدخال عنوان الصفحة في أرشيف الإنترنت Wayback Machine لحفظها. هذا يتيح لنا العودة إلى الصفحة المحفوظة في ذلك التاريخ في المستقبل إذا لزم الأمر.

قراءات إضافيّة

- Chayn.co: Collecting Evidence - How To Build A Domestic Abuse Case Without A Lawyer [جمع الأدلة - كيفية بناء قضية تعنيف منزلي بدون محام] | رابط
- PEN America - Documenting Online Harassment [توثيق التحرش عبر الإنترنت] | رابط

4| الحصانة النفسية في مواجهة الاعتداءات الرّقميّة

يُمكن للاعتداءات والتّهديدات الرّقميّة وغيرها من ضروب الإساءات الإلكترونيّة أن تطوّق النّفس بطيفٍ من المشاعر والانفعالات الهشة، نحو الذّنب، والعار، والقلق، والغضب، والحيرة، والضّعف، وصولًا إلى خوفٍ على الصّحّة النّفسيّة والبدنيّة—لكن حِدّة حضور هذه المشاعر ضمن فريق قد تتباين.

ليس هنالك طريقة "صحيحة" لاختبار الإنسان لمشاعره؛ فحالة الإنسان أو شعوره بالهشاشة وما يعتبره معلوماتٍ شخصيّة يختلف من شخصٍ لآخر، فالمشاعر كلها مُبرّرة، بعبارةٍ أخرى، لا داعٍ للقلق حيال صوابيّة ردّة فعلك الشّعوريّة.

إنّ أوّل ما يجب تذكره في الحالات الطّارئة والعاجلة تجنّب إلقاء اللّوم على الذّات أو على أفراد الفريق، قد نرغب في التّواصل مع شخصٍ نثق به يُمكنه مساعدتنا أو فرقينا في تدارك الظّرف الطّارئ الّذي نمر به، سواء من النّاحية التّقنيّة أو العاطفيّة.

للحدّ من الاعتداءات عبر الإنترنت لا بدّ لنا من جمع معلومات تفصيليّة عن الاعتداء، بيد أنّ ذلك لا يعني بالضّرورة أن نجمع تلك المعلومات بأنفسنا، يُمكننا إسناد تلك المهمة إلى شخصٍ نثق به وبإمكاننا أن نطلب دعمه من خلال اتباع الخطوات المذكورة في هذا الموقع، أو بتخويله للدخول إلى حساباتك أو أجهزتك لجمع المعلومات المطلوبة، كذلك يُمكنك التّواصل مع من تثق به للحصول على الدّعم العاطفي أو التّقني خلال هذه العمليّة.

في حال احتياجنا أو فريقنا لدعمٍ عاطفيٍّ للتعامل مع طارئٍ رقمي (أو متابعة)، يُمكنّنا اللجوء إلى البرنامج المجتمعي للصّحة النّفسية التّابع لتيم كوميونيتي للحصول على الخدمات النّفسية على الأمد الطّويل وبأشكالٍ، ولغاتٍ، وسياقات مختلفة.

موارد

أعظم ما نملك: توصيات ونصائح للحفاظ على الصّحة النّفسية الشخصية للنشطاء
العناية بالذّات للتمكّن من مواصلة الدّفاع عن حقوق الإنسان
موارد للرفاه وإدارة الضغط النفسي
الرّعاية الذّاتية لضحايا التّحرّش
النّساء في فضاء الإنترنت: الرعاية الذاتية
عافية الفرد والمجتمع
عشرون طريقة لمساعدة من يتعرضون إلى التّنمّر عبر الإنترنت
مشروع مَرَانة حقوق الإنسان
منصّة توتم التّعلّميّة الإلكترونيّة، "العناية بالصّحة النّفسية" (ينبغي التّسجيل للالتحاق بالتّدريب)
منصّة توتم التّعلّميّة الإلكترونيّة، "الإسعافات الأوّليّة النّفسية" (ينبغي التّسجيل للالتحاق بالتّدريب)

قراءة إضافيّة

مساقات منصّة بلوم للتّعلّم والتّعافي من الصّدمات في فضاءٍ خاصٍ وداعم (ينبغي التّسجيل للالتحاق بالتّدريب)
استجابة الفريق والزّملاء للتهديدات
التّواصل بشأن الأمان ضمن إطار الفرق والمنظّمات
استجابة الأفراد للتهديدات
استجابة الفريق والزّملاء للتهديدات
التّواصل بشأن الأمان ضمن إطار الفرق والمنظّمات

5| مسرد مصطلحات

[استُقي هذا المسرد من مسرد منصّة توتم التّعلّمية الإلكترونيّة بتصرّفٍ جُزئي]

يُقصد **بالحماية من البرامج الخبيثة**—أو ما يُعرف بالبرمجيات المُضادّة للفايروسات—برامج حاسوبيّة تُستخدم للحؤول دون تثبيت أو تسلل البرمجيات الخبيثة أو رصدها، وإزالتها.

يُقصد **بالأصول** أيّ بيانات، أو جهاز، أو أي مكوّن آخر يُتيح أي أنشطة معلوماتيّة أو ذات صِلة بها، علمًا أنّ الأجهزة، والبرامج، والمعلومات السّريّة من أبرز الأمثلة على الأصول الّتي تشمل المصادر أيضًا.

يُقصد **بالنّسخة الاحتياطية** نُسخةً من بيانات الحاسوب تُحفظ في مكانٍ آخر يُلجأ إليها لاسترجاع البيانات الأصليّة في حال فقدانها.

يُشار **بالخليوي المؤقّت** إلى نوعٍ من الهواتف المحمولة مُسبقة الدّفع الّتي لا ترتبط بعقدٍ مع شركة اتصالاتٍ، وعادةً ما يُصار للتخلّص منها بعد استخدامها.

يُقصد بمفهوم **عزل المعلومات** أي إجراء، أو عمليّة، أو سياسة تحدّ الوصول إلى المعلومات بأكبر قدر ممكن من الكفاءة والعملية، وقد يشمل ذلك غربلة عدد الأفراد المُتاح لهم الوصول إلى هذه المعلومات.

يُقصد بمفردة **جهاز** ضمن هذه المساق جهازًا متصلًا بالشّبكة أو جهازًا إلكترونيًا يُستخدم للاتصال بالإنترنت أو بشبكات الهواتف المحمولة، يشمل هذا التّعريف أجهزة الحاسوب الثّابتة والمحمولة، والهواتف المحمولة والذّكيّة، والسّاعات الذكيّة، وأجهزة التّلفزة ذكيّة، أو أيّ آلةٍ مُتصلة بالإنترنت.

يُقصد بمصطلح **التشفير** العمليّة الّتي تُحوّل بها المعلومات إلى رموزًا سريّة تُخفي معانيها ومدلولاتها الفعليّة.

يُشير مصطلح **تشفير الملفات** إلى عمليّة تشفير ملفات بعينها باستخدام مفاتيح خاصّة ومستقلة عن سائر مكوّنات الجهاز تتطلّب رموزًا خاصّة لفكّها واستخدام الملف المُشفّر.

يُشير مفهوم **التّشفير الكامل للقرص الصّلب** إلى تشفير القرص الصّلب للجهاز كاملًا مُكمّلًا بما في ثناياه من بياناتٍ، وملفّات، وأنظمة تشغيل، وبرامج، وذلك باستخدام مفتاح تشفير موحّد.

يُشار بتعبير **مزوّد خدمات الإنترنت** إلى الشّركة الّتي توفّر خدمة الوصول إلى الإنترنت.

يُقصد **بالبرمجيات الخبيثة** برامج الحاسوب الّتي، عند تشغيلها على الحاسوب، تُسفر عن عواقب غير مرجوة—وغالبًا ضارّة.

يشير مصطلح **نظام التّشغيل** إلى البرمجيات الوسيطة بين المكوّنات المادّيّة للحاسوب والمستخدم/ة.

يُشير اسم **مدير كلمات المرور** إلى تطبيق برمجي يعمل كخزنة لحفظ وحماية كلمات المرور الخاصّة بمختلِف حسابات المستخدم على الإنترنت وسائر خصائص الأمان.

يُقصد **بالتّصيّد** استدراج شخص لكشف بياناته الخاصّة عبر إرسال رسالة تبدو وكأنها من شخصٍ أو جهةٍ موثوقة.

يُقصد بمفردة **الاحتماليّة** ضمن هذا المساق، مدى إمكانيّة تحقق تهديد معين أو احتمال حدوثه.

تعني **برامج الفدية** تلك البرمجيات الّتي تُطالب الضّحية بدفع فدية لاستعادة ملفاته بعد أن شفّرتها هذه البرمجيات الخبيثة.

يُقصد **بجهاز التّخزين غير الثّابت** أي جهاز يُستخدم لتخزين البيانات ونقلها من جهازٍ لآخر، مثل وحدات نقل وتخزين البيانات (USB)، أو أقراص التّخزين الثّابتة الخارجيّة، والأقراص الضّوئيّة.

تُشير مفردة **المخاطر** ضمن هذا المساق الخطر النّاجم عن استغلال تهديد ثغرة أمنيّة.
يُقصد **بالمضامين المشبوهة** الدسائس التي تتوارى خلف واجهة تجارية، والتي تهدف في جوهرها إلى النصب والاحتيال.
يُقصد **بالخطورة** مدى خطورة أو جسامة شيء ما.
يُشار **بالتلصص** إلى سرقة البيانات الشّخصيّة، نحو رمز فك قفل الشّاشة أو الرّمز التّعريفي، وذلك باختلاس النّظر على شخص خلال استخدامه لحاسوبه، أو محموله، أو الصّرّاف الآلي، أو ما ماثل ذلك من أجهزة إلكترونيّة تُستخدم في الأماكن العامّة.
يُشار بتعبير **برمجيات التّجسّس** إلى نوعٍ من البرمجيات الخبيثة الّتي تُلملم سرًّا معلوماتٍ عن شخصٍ أو مؤسّسة. تمتاز هذه البرمجيّات بتصميمٍ يُتيح التّحكّم الجزئي أو الكلّي في تشغيل جهاز الضّحيّة دون علمٍ منها أو إذن.
يُشار **بالجهة المتربصة** إلى الشّخص، طبيعيًا كان أم معنويًا، أي فرد أم منظّمة أو هيئة حكوميّة تريد الحصول على ما لدى المستخدم من أصول.
يُقصد **بالتّهديد** كُل ما قد يعرّض النّاس للخطر، أو يعرقل عملهم، أو يُسبّب ضروبًا أخرى الضّرر.
يعني مصطلح **نمذجة التّهديدات** تحديد مختلِف أشكال المخاطر وتبويبها وتطوير تدابير للحد منها ومن آثارها.
يُقصد **بفايروس** البرمجيات الضّارة الّتي تستنسخ نفسها عن طريق تعديل برامج الجهاز الأخرى وتضمينها ببرمجيتها (أي برمجية لفايروس)، وما أن تتم عمليّة الاستنساخ تُضحي المناطق المتضررة مصابة بهذه الفايروسات.
يُشار بمواطن الضّعف أي نقاط انكشاف في نظامٍ، أو عمليّة، أو طريقة عمل فردٍ أو مؤسّسة.
يُقصد **باختراق الحسابات** الأفعال الّتي تنطوي على الوصول إلى معلوماتٍ مخزّنة على أجهزة رقميّة—حواسيب، وهواتف ذكيّة، وأجهزة لوحيّة، وشبكات—دون موافقة أصحابها بغية استلال معلوماتٍ خاصّة، أو اعتراض اتصالات محدّدة، أو تعديل معلومات بعينها.
يطلق مصطلح **بروتوكول الاتصال** على عملية تبادل الآراء والمعلومات بشأن المخاطر بين الأطراف المعنيّة باتصالات أو مخابرات المخاطر، أمّا إدارة المخاطر، فتشير إلى التّدابير الاستباقيّة لتقييم التّهديدات والمخاطر والسّيطرة عليها لمنع حوادث الاختراق، أو الشّكوك، والأخطاء. إلى جانب تقويم المخاطر، تعدّ هذه التّدابير من الرّكائز الأساسيّة لاتخاذ قرارات متزنة، نحو تقليل المخاطر. باعتبارها جزء لا يتجزأ من أُطر الأمان، فإن هذه العناصر تُحدّد الجهة المُتصل بها، ووتيرة وكيفية تغطية الإعلاميين والإعلاميات للأخبار ونقلها لغرفة الأخبار من الميدان. ولا بدّ من الإلمام بالخطوات الّتي يجب اتخاذها في حالة فقدان الاتصال مع أحد أفراد الفريق الإعلامي أو الفريق بقضه وقضيضه، وكيفية التّصرف إن تعثرت محاولات استعادة الاتصال.
يُشار **بتحليل السّياق** إلى مقاربة سياق ما لتحديد ما ينطوي عليه من تهديدات ومخاطر، وقد يتم ذلك باستخدام سلسة من الأسئلة يُراد منها ترسيم سياق ما.
يُقصد **بعملية مسح المُتسبّبين بالمخاطر** جُملةً من الخطوات تُساعد على تحديد أبرز مصادر الخطر في قصّة أو سياقٍ ما، وتشمل هذه الخطوات تحليل الأطراف المتأثرة بالخبر بما في ذلك مصالحهم، وما يمثلونه من صِفات، وما لهم من تأثير.
تعني الجريمة المنظّمة فعلًا إجراميًا ترتكبه مجموعة من الأشخاص، ثلاثة فأكثر، بحيث يعملون معًا لاقتراف جريمة أو أكثر لتحقيق ربحٍ اقتصادي أو مادّي.

يُذكر في هذا السّياق إلى الخلط الشّائع بين **اصطلاحي الجريمة المنظّمة والمنظّمات الإجراميّة**، حيث يشير المصطلح الأوّل إلى مجموعة من الأشخاص يعملون في فعلٍ إجرامي نحو الاتجار بالمخدّرات أو البشر، أو الخطف، أو القتل، أو غير ذلك من الجرائم الخطرة. من جهة أخرى، يُقصد بالمنظّمة الإجراميّة تنظيم ذا هرميّة يضلع بأنشطة إجراميّة جسيمة.

يُقصد بتعبير **بروتوكول**، المخطّط والتّدابير الدّقيقة الّتي ينبغي اتباعها استجابةً لسلسلة من الافتراضات الّتي يُحتمل تحقّقها، تستلزم هذه التّرتيبات كتابة المؤشّرات، والسّجلات، والخيارات، وجهات الاتصال التي ينبغي اللّجوء إليها لتحقيق الهدف. تُنْشَأ البروتوكولات عادةً باعتبارها جزءاً من سياسة أمنية، وقد تُشير إلى تدابير موحدة، نحو بروتوكول الاتصالات على سبيل المثال لا الحد.

يُشير مصطلح **الحدث الخَطِر** إلى حدث ينشأ عن وقوعه درجة معينة من الضّرر المادّي أو غير المادي، أو الخسارة الاقتصاديّة، أو إهانة لشرف الضّحية، علمًا الشّخص المُسبب بالشعور "بالخطر،" يُشار إليه بالمعتدي، أمّا الذي يدرك الخطر أو يعانيه، فيُشار إليه بالضّحية.

يُقصد **بتحليل المخاطر** تقييم الأدوات الّتي تمكّننا من تمييز التّهديدات والمخاطر المحتملة وعواقبها والتّخطيط لمجابهتها والتّخفيف من آثارها. يُمكن لهذه العمليّة أن تأخذ شكل وثيقة بها جُملةً من الأسئلة التّوجيهيّة. يُذكر أنّ تحليل المخاطر هو أولى الخطوات الأساسيّة الّتي لا بدّ منها لبناء خطط وبروتوكولات أمان تُساعدنا على تنفيذ عملنا بأمان، يُشار في هذا السّياق إلى ديناميّة عمليّة تحليل المخاطر وما يعنيه ذلك من تقلّب وتبدّل متغيّراتها بالاستناد إلى جُملة من العوامل.

المخاطر القانونيّة	المخاطر النّفسيّة والعاطفيّة	المخاطر الرقميّة	المخاطر الجسديّة
يُعاني الإعلاميون والإعلاميّات في بعض الأحيان جرّاء الأطر القانونيّة والتّنظيميّة (أو غيابها) حيث يخضعون لبعض القوانين الصّارمة في بعض الدّول. ينطبق هذا الأمر على النّشطاء أيضًا. من المهم أن تعرف ما هي قوانين الإعلام التي تخضع لها بناءً على موقعك.	تشمل هذه المخاطر زعزعة الاستقرار، وقد يكون مرجعها داخلياً أو مرتبطاً بالبيئة المحيطة، الأمر الّذي يجعل أثر هذا الضّرب من الخطار يتخطّى الإعلامي الفرد إلى فريقه. مثال ذلك: التّجارب المؤلمة والصّادمة والتّوتّر المهني/ الشّخصي. وتتسع دائرة هذه النوع لتشمل الكوارث الطبيعية المرتبطة بالعمل والضّغوط الأسرة النّاجم عن فقدان أحد أفراد أسرته— جميع هذه الأخطار قد تُلقي بظلالها على الحالة النّفسيّة والعاطفيّة.	يشمل هذا النّطاق من المخاطر، حجب المعلومات الرّقميّة أو الإضرار بها، بالإضافة للتخزين والحفظ، والاتصالات، والحسابات، والوصول للمعلومات. ومن الأمثلة على هذه المخاطر التحرش على وسائل التّواصل الاجتماعي، والرّقابة، وإزالة المحتوى، وفقدان المعلومات، وصولًا إلى اختراق الحسابات. في بعض الحالات، قد تُترجم المخاطر الرّقمية في مخاطر مادية؛ مثلًا عندما تؤدي التّهديدات على وسائل التّواصل الاجتماعي إلى هجوم جسدي.	يضم هذا الضّرب من المخاطر الأذية الجسديّة وصولًا إلى قتل الإعلاميين. مثال ذلك السّرقة، والسّطو، والابتزاز، والخطف.

يُذكر في هذا السّياق أنّ **الأزمات النّفسية** ما هي إلّا نتاج للافتقار للأدوات اللّازمة للتعاطي ظروف معيّنة لم نكن مستعدين لها. ويتوقّف التّغلب على الأزمات على المتاح من هذه الأدوات، يُمكن لبعض التّمارين التّنفس العميق أن تخفف وطأة بعض الحالات، لكن ثمّ حالات تُوجب اللّجوء إلى المختصين.
يُشير اصطلاح **المتسببين بالمخاطر** إلى المؤسّسات والأشخاص الّذين يلحقهم ضررًا—مباشرًا أو غير مباشر، أو يعتقدون ذلك—جرّاء عمل صحفيّ. بالتّالي فإن دائرة هؤلاء تتسع لتشمل مؤسّسات، وأشخاص، أو فئات اجتماعيّة قد تُشكّل تهديدًا، ولو محتملًا، لنزاهة العمل الإعلامي، أو تِلك الّتي تُمثّل خطراً "مستوطنًا" في المنطقة، ومن أمثلة ذلك، السّاسة الفاسدون.

تُشير **خطّة الأمان** ضمن سياق التّغطية الإعلاميّة إلى المُخطّط الّذي يُحدّد التّدابير الوقائيّة لتجنب المخاطر وتخفيفها بكافة ضروبها، الجسديّة، والمادّيّة، والرّقميّة، والنّفسيّة، والقانونيّة، وذلك في ضوء المعطيات التّأصيلية لتحليل المخاطر.

يُراد بتعبير **المُحيط** السّياق المادّي، والاجتماعي، والسّياسي الّذي يُوجد به الإعلاميّ أو محط العمل الإعلامي أو أحد خيوطه.

المحيط السّياسي	المحيط الاجتماعي	المحيط المادّي
من الطّرف أو الأطراف الّتي يدعمها النّاس؟ ومن المعارضة؟	التّصورات الاجتماعيّة والاقتصاديّة حيال تطبيع حقوق ما.	الشّارع؛ الحي؛ المدينة

يُقصد **بالتّهديد** الشّيء أو الشّخص المحتمل خلف الخطر أو الضّرر المُحيق بشخص أو شيء ما. يتجسّد غرض التّهديدات بالتّلويح بالضّرر الفعلي الّذي قد ينزل بشخص ما نتيجة فعل أو موقف ما أو الإحجام عنه.

يُشير اصطلاح إلى إجابة سؤال على أيّ جهة من المُعادلة تكمن الفرص؟ وما الفوائد الرّئيسة من للقيام بهذه المهمّة؟ ما الآثار الإيجابيّة؟

هل يستحق الأثر الّذي سيتمخض عن هذه المهمّة يستحق المخاطرة؟ هل سيحقق هذا سيثمر النتائج المرجوة؟ مجددًا، هل يستحق هذا المخاطرة وما تشمله من موقع، وكوادر إعلاميّة، وأمور تشغيليّة، ونفقات، وتنظيم، وجهود رقميّة؟

مصفوفة المخاطر													
الفائدة						الخطورة							
ما هي احتمالية الحصول على الفائدة؟ الاحتمالية	تقريبًا مؤكّدة 5	جيدة 5	جيدة جدًا 10	كبيرة 16	ممتازة 20	ممتازة 20	شديدة 25	شديدة 20	مرتفعة جدًا 15	مرتفعة 10	متوسطة 5	تقريبًا مؤكّدة 5	ما هي احتمالية حدوث الخطر؟ الاحتمالية
	محتملة 4	جيدة 4	جيدة 8	جيدة جدًا 12	كبيرة 16	ممتازة 20	شديدة 20	مرتفعة جدًا 16	مرتفعة 12	متوسطة 8	متوسطة 4	محتملة 4	
	متوسطة الاحتمال 3	محدودة 3	جيدة 6	جيدة 9	جيدة جدًا 12	كبيرة 16	مرتفعة جدًا 15	مرتفعة 12	متوسطة 9	متوسطة 6	منخفضة 3	متوسطة الاحتمال 3	
	غير محتملة 2	منخفضة جدًا 2	محدودة 4	جيدة 6	جيدة 8	جيدة جدًا 10	مرتفعة 10	متوسطة 8	متوسطة 6	منخفضة 4	منخفضة جدًا 2	غير محتملة 2	
	نادرة 1	منخفضة جدًا 1	منخفضة جدًا 2	محدودة 3	جيدة 4	جيدة 5	متوسطة 5	متوسطة 4	منخفضة 3	منخفضة جدًا 2	منخفضة جدًا 1	نادرة 1	
		ضئيلة 1	طفيفة 2	بارزة 3	كبيرة 4	شديدة 5	شديدة 5	كبيرة 4	بارزة 3	طفيفة 2	ضئيلة 1		
		أثر إيجابي					أثر سلبي						
		الأثر / الفائدة إلى أي حد يمكن أن تكون النتائج ممتازة في حالة حدوث التأثير؟					**الأثر / العاقبة** ما مدى خطورة النتائج في حال حدوث الخطر؟						