دليل الأمان الرقمي

دليل وورشات عمل
حول الأمان الرقمي

حملة
المركز العربي
لتطوير الإعلام
الاجتماعي

دليل الأمان الرقمي

إصدار: "حملة" - المركز العربي لتطوير الإعلام الاجتماعي
كتابة: مسعود قبها
إعداد: روزالين حصري، مسعود قبها
اعداد الورشات: روزالين حصري
مساعدة إعداد: منى نجّار - أكاديمية "دويتشه فيله" الألمانية
تصميم جرافيك: أمجد بدران

كانون أول ٢٠١٧

تواصلوا معنا:
info@7amleh.org | www.7amleh.org
هاتف: +972 (0)774020670
تابعونا على وسائل التواصل الاجتماعي: 7amleh

بدعم من:

german cooperation
DEUTSCHE ZUSAMMENARBEIT

وبالتعاون مع:

DW Akademie
Made for minds.

الفهرس

عن المركز

حملة - المركز العربي لتطوير الإعلام الاجتماعي

مؤسسة أهلية غير ربحية تهدف إلى تمكين المجتمع المدني الفلسطيني والعربي من المناصرة الرقمية، من خلال بناء القدرات المهنية والدفاع عن الحقوق الرقمية وبناء الحملات الإعلامية المؤثرة.
لذا، يركّز مركز «حملة» مشاريعه ومبادراته في ثلاثة مجالات أساسية:

التدريب:

تدريب مؤسسات أهلية وحراكات شبابية وشعبية وناشطين في جميع أنحاء فلسطين، حول مهارات الإعلام الجديد، وبناء الحملات، وتحسين الحضور الرقمي.

المرافعة:

منتديات وإصدارات وائتلافات من أجل حماية الحقوق الرقمية كحقوق إنسان، وبالأساس الحق في منالية الإنترنت، الأمان الرقمي، وحرية التعبير والتنظيم في الشبكات الرقمية.

الحملات:

تخطيط وإدارة حملات مناصرة وتوعية لمؤسسات وأطر أهلية حول قضايا مختلفة.

الحق في التعبير والخصوصية

الإعلان العالمي لحقوق الإنسان هو وثيقة تاريخية هامة في تاريخ حقوق الإنسان صاغه ممثلون من مختلف الخلفيات القانونية والثقافية من جميع أنحاء العالم. واعتمدت الجمعية العامة الإعلان العالمي لحقوق الإنسان في باريس في ١٠ كانون الأول ١٩٤٨ بموجب القرار ٢١٧ ألِف بوصفه المعيار المشترك الذي ينبغي أن تستهدفه كافة الشعوب والأمم. وهو يحدد، وللمرة الأولى، حقوق الإنسان الأساسية التي تتعين حمايتها عالمياً.

المادة ١٩ من الإعلان العالمي لحقوق الانسان

لكلِّ شخص حقُّ التمتُّع بحرِّية الرأي والتعبير، ويشمل هذا الحقُّ حرِّيته في اعتناق الآراء دون مضايقة، وفي التماس الأنباء والأفكار وتلقِّيها ونقلها إلى الآخرين، بأيَّة وسيلة ودونما اعتبار للحدود.

المادة ١٢ من الإعلان العالمي لحقوق الانسان

لا يجوز تعريضُ أحد لتدخُّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات.

لماذا أصدرنا هذا الدليل؟

في الوقت الذي سهّلت فيه شبكة الإنترنت ومواقع التواصل الاجتماعي بالذات اختراق خصوصيات الناس وحوّلت معلوماتهم الشخصية إلى معلومات أمنية أو سلعة تجارية تُحقّقُ من خلالها الأرباح للشركات المالكة لهذه المواقع. خُلِقت تحديات أمنية جديدة أمام المستخدمين، إذ أصبحت هذه الشبكات تُشكّلُ منظومةَ مراقبةٍ وتعقّبٍ مزعجةً لدى الكثيرين.

وتبدو منظومة المراقبة والتعقّب هذه واضحة للعيان في فلسطين في ظلّ واقع الاحتلال وواقع سياسات الردع والتضييق على حرية التعبير عن الرأي. وقد رصدت عدة مؤسسات حقوقية في العامين الأخيرين حالات مرتفعة للاعتقال على خلفية ما يسمى «التحريض على الفيسبوك». وفي حال لم يكن الحديث عن اعتقال وحكم بالسجن، فإن عدداً متزايداً أيضاً من الناشطين على شبكات التواصل الاجتماعي يتعرضون للمراقبة والملاحقة والتحقيق، أو في حالات أخرى يُجبَرون – في ظلّ هذا الوضع – على ممارسة الرقابة الذاتية المفرطة على أنفسهم.

قبل إصدار هذا الدليل قام مركز «حملة» بإجراء بحثٍ ومسحٍ ميدانيٍّ في أوساط الشباب الفلسطينيين ذكوراً وإناثاً، وذلك بهدف الوقوف على مدى وعي المستخدمين حول موضوع الأمان الرقمي في الإنترنت، ورصد أهداف وطرق الاستخدام التي يتبعونها، ورصد ظواهر التعقّب واختراقات الخصوصية في صفوفهم. حاول هذا البحث تقديم معلومات حول كيفية التعامل مع موضوع الأمان الرقمي بين الفلسطينيين في مختلف أماكن تواجدهم داخل فلسطين التاريخية، وذلك في ظل تصاعد أهمية هذا الموضوع، وارتفاع في حالات التهديد والمخاطر المرتبطة باستخدام الإنترنت.

اعتمد هذا البحث منهجيتي البحث النوعي (أو الكيفي) والكمي عن طريق تعبئة الاستبانات وعقد المجموعات البؤرية مع الشباب الفلسطينيين في كافة أماكن تواجدهم. وقد شملت عينة البحث النوعي ١٣٢ شاباً وشابةً، من مختلف المناطق، من الفئة العمرية بين ١٥-٢٥ عاماً، واعتمد البحث النوعي أداة المجموعات البؤرية. أما عينة البحث الكمي فقد شملت ١٢٨٥ شاباً وشابةً من الفئة العمرية ١٥-٢٥ عاماً كذلك، واعتمد البحث الكمي أداة الاستبانات (تعبئة الاستمارات). أُجري البحث في شهر تشرين الثاني من العام ٢٠١٦.

وقد برزت في البحث نتائج متفاوتة بين المجموعات البؤرية، أهمّها الفوارق الجندرية الواضحة، خصوصاً لدى المجتمعات المحافظة، والتي تحدّ من استعمال شبكات التواصل الاجتماعي لدى النساء بسبب الحساسيات الاجتماعية المقترنة بذلك. فقد عبّرت غالبية النسوة في المجموعتين المحافظتين عن عدم استعمالهن للفيسبوك وذلك بطلب من الأهل، لتفادي مشاكل الاختراقات للحسابات، أو سرقة الصور والاستحواذ على مضامين شخصية يمكنها أن تكون شرارة لمشاكل اجتماعية وعائلية كبيرة. ولكن، من جهة أخرى، هذا الأمر لا يسري على الذكور، حيث إن معظم الشباب في تلك المجتمعات لديهم حساب فيسبوك واحد على الأقل.

ولذلك وبناءً على وجود غياب مؤسساتي واضح الداخل والضفة والقطاع وبسبب ما برز من نتائج في الاستطلاع الذي اجريناه والذي يشير الى عدم وجود وعي كافي لكيفية الوقاية والتعامل مع مخاطر الشبكة والانترنت وجدنا من مسؤوليتنا كمركز أن نقوم ببناء دليل يتلاءم مع فئة الهدف هذه بحيث يكون مرجعية لكل من يعمل مع فئة الشبيبة حتى وان لم يكن لديه الخبرة في هذا المجال

مقدمة

يعتبر المركز هذا الدليل الذي بين أيديكم أحد أهم الأهداف التي وضعت لمشروع الأمان الرقمي والذي نعمل عليه بالتعاون مع أكاديمية «دويتشه فيله»، حيث يرى المركز من واجباته رفع الوعي في كل ما يتعلق بموضوع الأمان الرقمي والحقوق الرقمية، ولذلك يولي المركز أهميةً قصوى لموضوع تدريب فئة الشبيبة، نظراً لما رأيناه من نتائج مقلقة في الاستطلاع الميداني «الأمان الرقمي والشباب الفلسطيني».

بنينا مخططاً لورشاتِ عملٍ، وقمنا بتأهيل عشرة مدربين لتمرير تلك الورشات كنواة بداية لهذا المشروع، ولنحرص على اختبارٍ ما نقوم به من عمل ونعيد تقييمه قبل إصدار الدليل، وذلك خلال شهري تشرين الأول وتشرين الثاني ٢٠١٧. وقد أُخِذت بعين الاعتبار التقييمات التي تم توجيهها لنا من قبل المدربين والمشاركين في هذه الورشات. وهكذا، كانت تجربة مركز «حملة» مع ورش العمل في مدارس الضفة والداخل نواة بداية هذا المشروع، حيث تم تمرير ٤٤ ورشة في المدارس والجامعات.

هدف الدليل

يهدف الدليل التدريبي إلى تمكين المدرّب من تمرير وإعداد أنشطة تتعلق بموضوع الأمان الرقمي، وتقديمها للطلبة المستهدفين، وذلك لرفع الوعي والمعرفة بأمنهم الرقمي وخصوصيتهم أثناء استخدام الإنترنت.

محتوى الدليل

يشمل الدليل ٦ محاور رئيسية، يشمل كل محور عدة وحدات تدريبية، ومدة تطبيق كل وحدة ٤٥ دقيقة، تتألف من ورش عمل للطلبة، مادة للمدرب، وأوراق عمل، وبعض المواد الإثرائية للمدرب. تُعرض الوحدات التعليمية على شكل جداول تشمل:

- المحتوى الذي سيتم شرحه أو تطبيقه.
- الوقت المقدر لتنفيذ كل محتوى على حدة.
- هدف التعلم المرجو من كل محتوى تدريبي.
- الأدوات اللازمة للشرح والتطبيق.
- ملاحظات إضافية مساعدة.

تم بناء هذا الدليل ليكون تفاعلياً وتشاركياً بعيداً عن الإملاء والتلقين، ليُحفّز الطلبة على استنتاج المعلومات بناءً على التجربة والدليل، وقد حرصنا على التركيز على الجانب العملي. لذلك في بعض الأحيان لجأنا لاستخدام بطلين من أعمار الطلبة المستهدفين هما رامي وسارة، وذلك لتسهيل الشرح

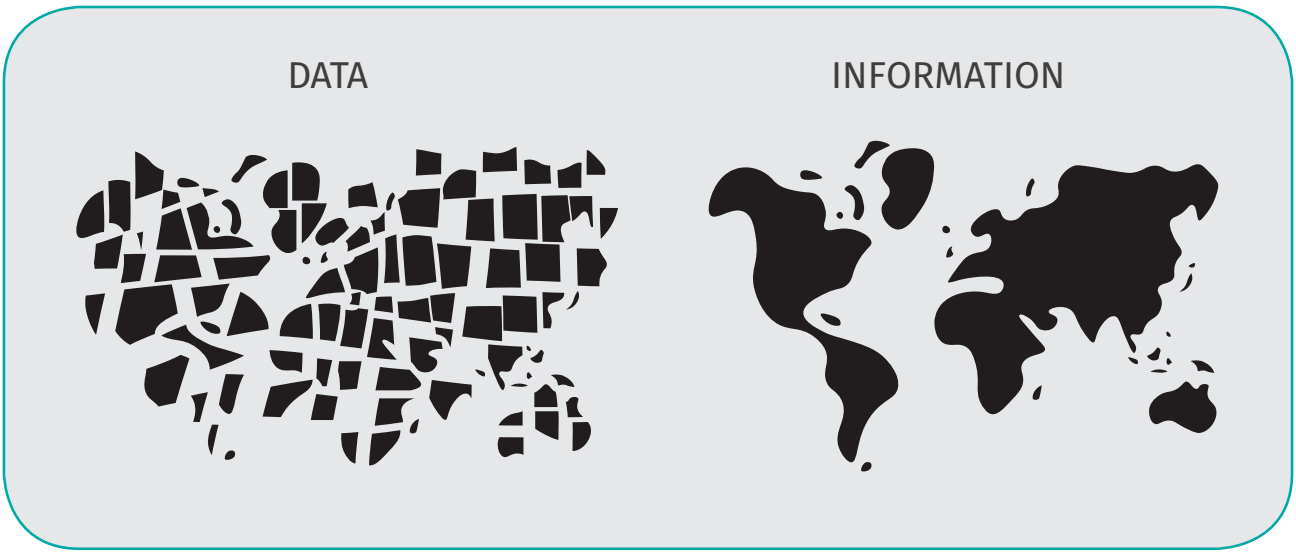
وإيصال المغزى من الوحدة بطريقة أسهل وملائمة لجيل الهدف.
كما سعينا لاستخدام أسلوب «التعلم باللعب» فشمل الدليل ألعاباً تحفيزيةً وتعليميةً، بالإضافة لاستخدام أسلوب النقاش الجماعي بين الطلبة لإثراء المعرفة. كما حرصنا على بناء بعض التدريبات من خلال تنفيذها في مجموعات عمل، وذلك لتعزيز روح التعاون والعمل المشترك بين الطلبة. إضافة إلى ذلك، حرصنا أن يتلاءم الدليل مع السياق الفلسطيني ومع المخاطر التي رصدناها في الاستطلاع الذي بحث مفاهيم الأمان الرقمي لدى الشباب الفلسطيني.
ومن المهم الإشارة إلى أن هذا الدليل مرن ويستطيع المدرب استخدامه من حيث المحتوى التدريبي أو التقدير الزمني بحرية مطلقة، ومن الممكن إجراء التغييرات بما يتلاءم مع عدد الطلبة والمكان والزمان المتاحين. كما أن هناك هامشاً للإبداع والابتكار خارج حدود الدليل يستطيع من خلالها المدرب إجراء أي تعديل يراه مناسباً، على أن يخدم تحقيق أهداف الوحدات التعليمية.

من يستخدم هذا الدليل

تم تصميم هذا الدليل بحيث يتمكن معلمو المدارس والمربون بالإضافة لأي شخص يعمل مع فئة الشبيبة من استخدامه حتى وإن لم يكن لديهم خلفية في موضوع الأمان الرقمي.

البيانات وأنا

يبدأ أي نظام للمعلومات بالبيانات (DATA) وينتهي بالمعلومات (INFORMATION). المعلومات هي البيانات التي تُقدّم بشكل مفهوم ومقروء وذي معنى. أما ما يعالج ويخزن ويرسل عبر المكوّنات الأخرى لأنظمة المعلومات فهي البيانات في شكلها الثنائي الرقمي (Digital) (أصفار وآحاد). قد تكون البيانات هيكليةً ضمن حقول مخزنة في قواعد البيانات، وقد تكون غيرَ هيكليةٍ مخزنةً في ملفات.



أما المعلومات فتعتبر نتاج معالجة البيانات، فالمعلومات عبارة عن البيانات التي تمّت معالجتها بتصنيفها وتنظيمها وتحليلها، وأصبح لها معنى لتحقق هدفاً معيناً وتُستعمل لغرضٍ معيّنٍ، كبيانات الموظفين المتمثلة في الأسماء، والأرقام الوظيفية، والمسميات الوظيفية، والصور، وتاريخ التعيين، والراتب.

وكمثال للتفريق بين البيانات وبين المعلومات بعد المعالجة، تُعتبر علامات المواد الدراسية بيانات، بينما نتيجة العملية لحساب المعدل المتمثلة في جمع علامات المواد وقسمة الناتج على عدد المواد هي معلومة.

وقد دخلت استخدامات شبكة الإنترنت إلى حياتنا في مختلف نواحيها الاجتماعية والمهنية والعائلية، فما أن ندخل عالم الإنترنت حتى نشارك أوجه حياتنا المختلفة، فنبحث على شبكة الإنترنت عن ما يُلبي احتياجاتنا ورغباتنا وآراءنا، وبالتالي نترك وراءنا قريناً رقمياً وبصمةً رقميةً خاصةً. فقريننا الرقمي يضمّ الكثير من البيانات الخاصة بنا، وهنا تقوم الشركات والخدمات المتواجدة على شبكة الإنترنت باستغلال

هـذا القريـن لتطويـر عملهـا واسـتمراريتها، فبـدون هـذا الكـم الهائـل مـن القرائـن الرقميـة لـن تسـتمر شركات عملاقـة مثـل «فيسـبوك» و»جوجـل».

تعمـل المواقـع الإلكترونيـة مـن خـلال ملفـات برمجيـة صغـيرة تدعـى (ملفـات الارتبـاط) (Cookies)، والتـي تُـزرع في المتصفّـح، عـلى حفـظ بيانـات المسـتخدم وتفضيلاتـه، وذلـك لخدمـة محـركات البحـث المختلفـة. يقـوم الخـادم (server) بإنشـاء ملفـات الارتبـاط هـذه وتخزينهـا في متصفّـح المسـتخدم، فملفـات الارتبـاط قـد تشـمل تسـجيل الدخـول مـن اسـم المسـتخدم وكلمـة المـرور وبيانـات التسـجيل وزمـن دخـول المسـتخدم ورقـم التسـجيل ومعلومـات أخـرى.

إن مثـل هـذه المعلومـات التـي تخـزن في ملفـات الارتبـاط مفيـدة جـداً بالنسـبة للأسـواق الإلكترونيـة (e-commerce)، فـإن المسـتخدم حينـما يختـار سـلعة معروضـة في موقـع مـا، يقـوم الموقـع بتخزيـن ملـف ارتبـاط يشـمل سـعر السـلعة واسـمها ورقمهـا، وحينـما يختـار المسـتخدم سـلعة ثانيـة يقـوم موقـع السـوق الإلكـتروني بتكـرار العمليـة إلى أن يطلـب المسـتخدم فاتـورة الـشراء، حينهـا يسـترجع الموقـع آخـر ملـف ارتبـاط خزنهـا ليتـم حسـاب السـعر الـكلي.

كـما تسـتخدم ملفـات الارتبـاط لاسـتهداف المسـتخدم في الإعلانـات المناسـبة لـه، فعنـد بحثنـا في محـرك البحـث «جوجـل» مثـلاً عـن موضـوع معـين سـيتم تخزيـن الموضـوع في ملفـات الارتبـاط واسـتخدام هـذه المعلومـات كأداة لمعرفـة الإعلانـات المناسـبة لنـا بنـاء عـلى ذلـك البحـث.

تُسـتخدم ملفـات الارتبـاط لـكي تسـاعدنا في تصفـح الإنترنـت والوصـول إلى هدفنـا بشـكل يسـير، لكـن إن وقعـت ملفـات ملفـات الارتبـاط في يـد مـن لا يجـب أن تقـع بيـده فسـيتم اسـتخدام هـذه المعلومـات بشـكل يخـترق خصوصيتنـا.

لمنـع المواقـع مـن تخزيـن ملفـات الارتبـاط عـلى الجهـاز يجـب تفعيـل خاصيـة (Do Not Track) وكذلـك مسـح بيانـات التصفـح (clear browsing data)، كـما يمكـن اسـتخدام محـرك بحـث آمـن لا يحتفـظ ببيانـات المسـتخدمين أو بيانـات البحـث، كمحـرك (Duck Duck Go).

الإنترنت

كيف يعمل الإنترنت؟

لنتخيل معاً أننا دخلنا مبنى كبيراً، ونوّد الذهاب لمكتب ما داخل هذا المبنى ونحن لا نعرف موقع المكتب. سيخطر في بالنا التوجه إلى الاستعلامات وسؤالهم عن مكان المكتب، ثم سننظر إلى الخريطة الإرشادية لمعرفة أقصر طريق مؤدية إلى المكتب، فتدلّنا الخريطة أن نتوجه عبر الممر الذي أمامنا مثلاً، ثم تدلّنا إلى صعود الدرج والمشي لليمين قليلاً وإذا نحن أمام باب المكتب الذي نبحث عنه؛ هذه هي تقريباً طريقة عمل الإنترنت. يُمثلُ المبنى هنا الإنترنت الذي يحتوي الكثير من الغرف والمكاتب والمحلات، وكل غرفة ومكتب ومحل مرقم برقم حسب الطابق الذي يوجد فيه.

يُمثل الموقع المحدد في الطابق في عالم الإنترنت العنوان المنطقي ip address، ولأنها زيارتنا الأولى من نوعها للمبنى فنحن لا نهتم برقم الغرفة والمكتب والمحل التجاري، وإنما نهتم باسم المكتب، بينما نجدُ أنّ موظف الاستعلامات يحفظ أرقام المكاتب. هنا يُمثل موظفُ الاستعلامات خادمَ نطاق الأسماء DNS server، فهو يقوم بترجمة العنوان لأرقام معينة لا تتشابه مع بعضها البعض، تُمثل الممرات والمفترقات والدرج أثناء توجهنا للمكتب المراد الوصول إليه، وهذه التوجيهات أو الموجهات (راوترات) routers. تقوم بإرشادنا للطريق التي يجب أن نسلكها للوصول إلى المكتب الذي نريد زيارته.

البنية التحتية للإنترنت Internet Infrastructure

تتكون شبكة الإنترنت من عدد من الحواسيب المزودة ببطاقات الشبكة Network Interface Card، والخوادم Servers، والموجّهات Routers، والمقسمات Switchs، ووسط ناقل، لتصل كل هذه الأجهزة معاً. كما تحتوي هذه المعدات الصلبة على برمجيات للتواصل وبروتوكولات لتنظيم عملية الاتصال وتشغيل شبكة الإنترنت، كبروتوكول الإنترنت TCP/IP وبروتوكول أسماء النطاقات DNS، وبروتوكول تصفح الإنترنت HTTP، وبروتوكول نقل الملفات FTP.

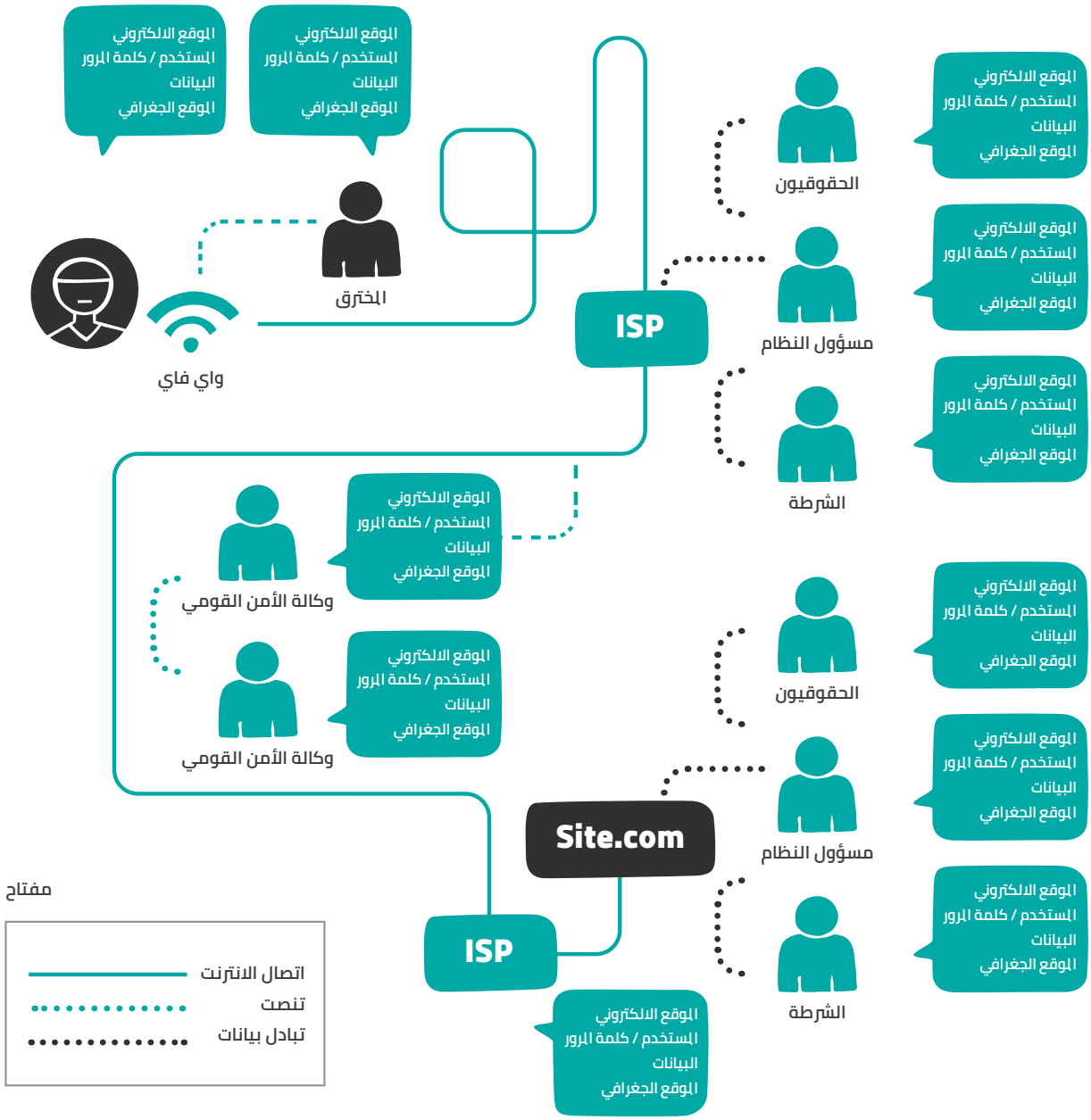
تتكون الشبكة مكونةً من عدد من أجهزة تسمى أجهزة الزبون، كما يوجد جهاز الخادم (السيرفر) Server وهو الجهاز الرئيسي والأساسي لعمل الشبكة، حيث تتصل به كل الأجهزة الأخرى، ويتصف جهاز الخادم بالكفاءة العالية من حيث مساحة الذاكرة الكبيرة، وكذلك المساحة التخزينية، حيث تُخزَن عليه قاعدة البيانات الأساسية ومعلومات الاتصال بالشبكة ومعلومات أخرى تحتاج لهذه الكفاءة. ومن أهم المهام التي يقوم بها الخادم التحكم في العمليات التي تتم عبر الشبكة، ومنح الصلاحيات المختلفة للأجهزة الأخرى وذلك باستخدام أنظمة وبرامج متخصصة.

كما تتضمن الشبكة بطاقة شبكة خاصة بأجهزة الحاسوب (NCI) وهي اختصار لـ (Network interface Card) وبطاقة الشبكة هي حلقة الوصل بين جهاز الحاسوب والوسط الناقل للشبكة، ومن مهامه الأساسية: العمل كوسيط من وإلى الشبكة، حيث تقوم بطاقة الشبكة بتحضير وتجهيز البيانات من الجهاز لبثها عبر الشبكة، ومن ثمّ تقوم بإرسالها عبر الشبكة.

كـما تتضمـن الشـبكة وسـطاً ناقـلاً للاتصـال (السـلكي أو اللاسـلكي)، فهنـاك طريقـة النقـل المعتمـدة عـلى الوسـط اللاسـلكي المتمثـل في الهـواء، وهنـاك طريقـة النقـل السـلكية والتـي تنـدرج تحتهـا العديـد مـن أنـواع الأسـلاك أهمّهـا: الأسـلاك النحاسـية والمجدولـة والمحوريـة، و الألياـف البصريـة.

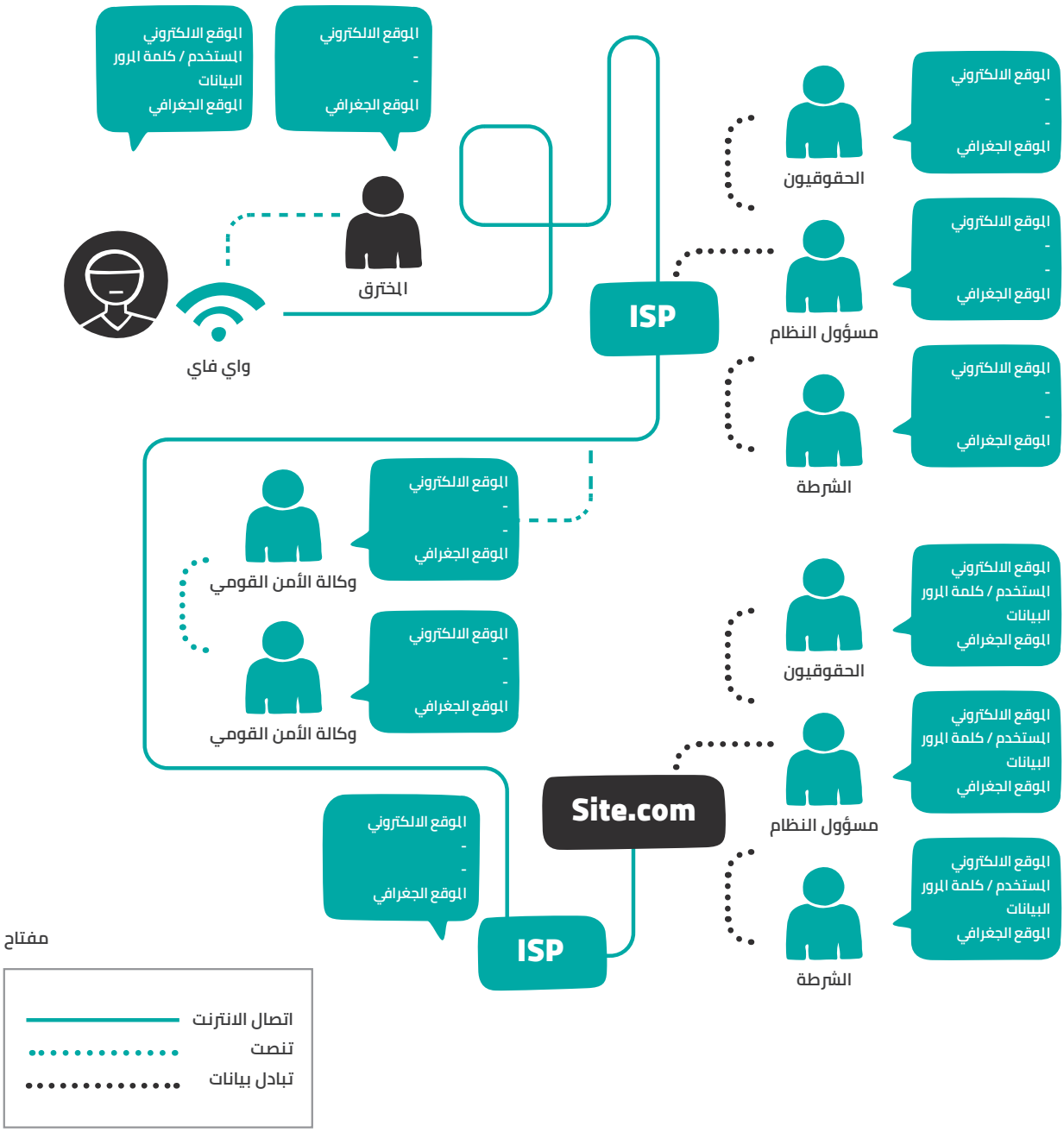
الاتصالات الآمنة

في حالـة اسـتخدام بروتوكـول http، فـإن اسـم المسـتخدم وكلمـة المـرور الخاصتـين بموقـع معـين زاره المسـتخدمُ سـوف تمـرُّ في الشـبكة مـن دون تشـفير، وسـيكون بمقـدور الأطـراف المتعـددة كالشركـة المـزود للإنترنـت ISP والمخترقـين (الهاكـر) معرفـة كلمـة المـرور واسـم المسـتخدم، وسـيكون بمقدورهـا كذلـك معرفـة طبيعـة البيانـات التـي تمـرّ في الشـبكة.



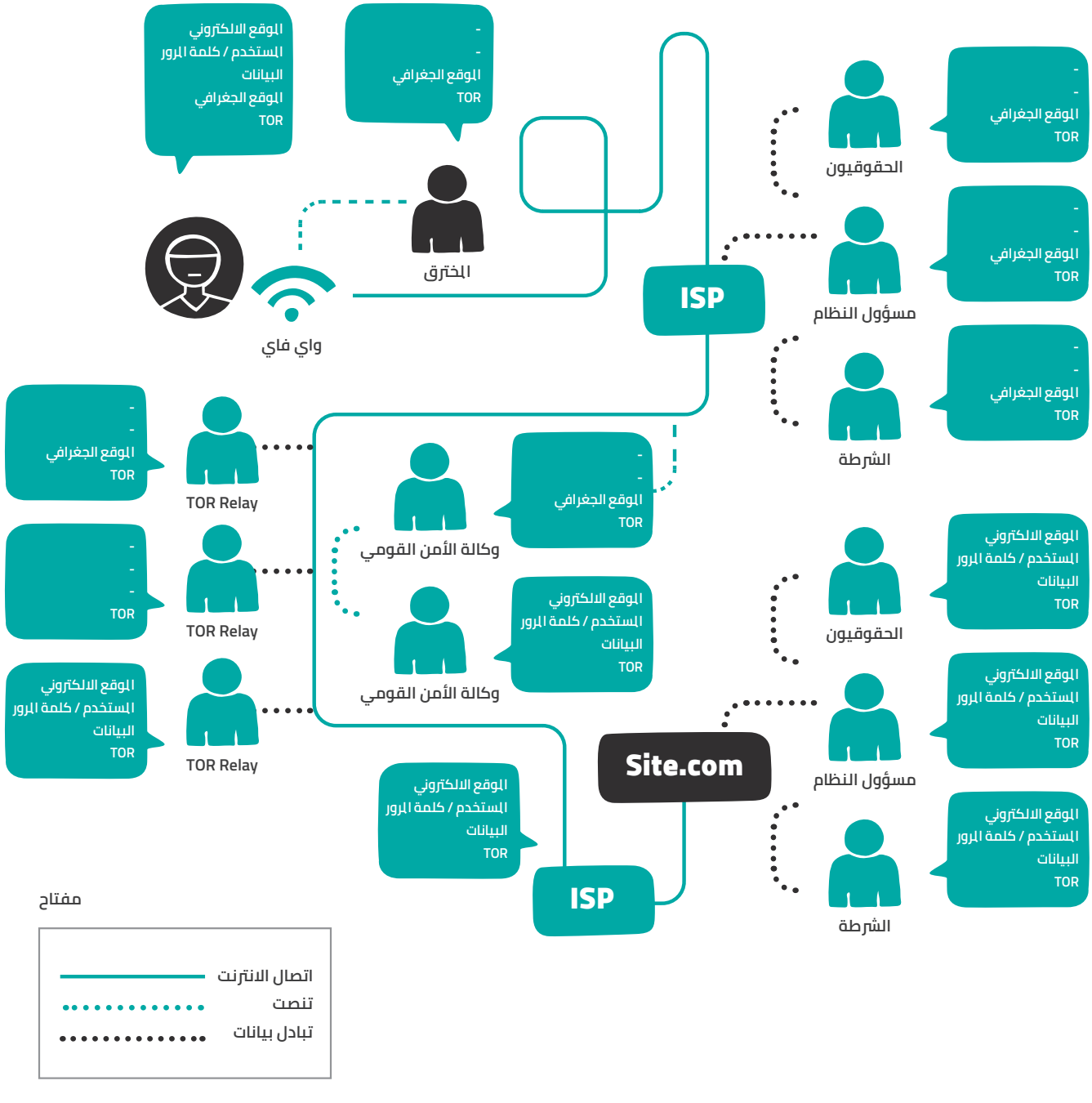
بروتوكول HTTPS

في حالة استخدام بروتوكول https فان اسم المستخدم وكلمة المرور الخاصتين بموقع معين زاره المستخدم وكذلك البيانات المُرسة سوف تُشفّر أثناء مرورها في الشبكة، ولن يكون بمقدور الأطراف المتعددة، كالشركة المزودة للإنترنت ISP، والمخترقين (الهاكر) الواقعين في طريق البيانات بين المستخدم وسيرفر الموقع المقصود، لن يكون بمقدورهم معرفة كلمة المرور واسم المستخدم أو طبيعة البيانات التي تمرّ في الشبكة. علينا التأكد دائما أننا نستخدم بروتوكول https عند زيارتنا للمواقع الإلكترونية، وللتمكن من استخدام بروتوكول https يمكننا استخدام إضافة خاصية في المتصفح تسمى https everywhere.



التوجيه البصلي TOR

TOR هـي اختصـار للمصطلـح (The Onion Router) أو مـا يعـرف بالتوجيـه البصـلي، وبـدأت كشـبكة مـن مجموعـة خـوادم حـول العـالم، وهـي الآن عبـارة عـن منظمـة غـير ربحيـة تعمـل في مجـال أبحـاث وتطويـر أدوات حمايـة الخصوصيـة عـلى الإنترنـت. تقـوم هـذه الشـبكة بإخفـاء هويتنـا عنـد تبـادل البيانـات باسـتخدام الخـوادم الخاصـة بالشـبكة، لا الخـوادم المعتـادة الخاصـة بالإنترنـت. وتقـوم الشـبكة أيضـاً بتشـفير تلـك البيانـات حتـى لا يقـوم أحـد بتتبعهـا أو اسـتخدامها، فـإذا حـاول أحـد تتبـع بياناتنـا فسـتظهر لـه عـلى أنهـا بيانـات عشـوائية تنتقـل بـين أطـراف شـبكة «تـور».



لاستخدام هذه التقنية كل ما علينا فعله هو تحميل متصفح «تور» والبدء بتصفحنا المعتاد، عندها فإن كل المعلومات التي ترسلها أو تستقبلها تنتقل عن طريق شبكة «تور» ولا تحتاج لأي ضبط مسبق

عند استخدامنا للمتصفح «تور» ستتم تعمية الموقع الذي نزوره واسم المستخدم وكلمة المرور والبيانات التي ننقلها، وتحصل عملية التعمية هذه في طريق البيانات من جهاز المستخدم لسيرفر الموقع المرادة زيارته.

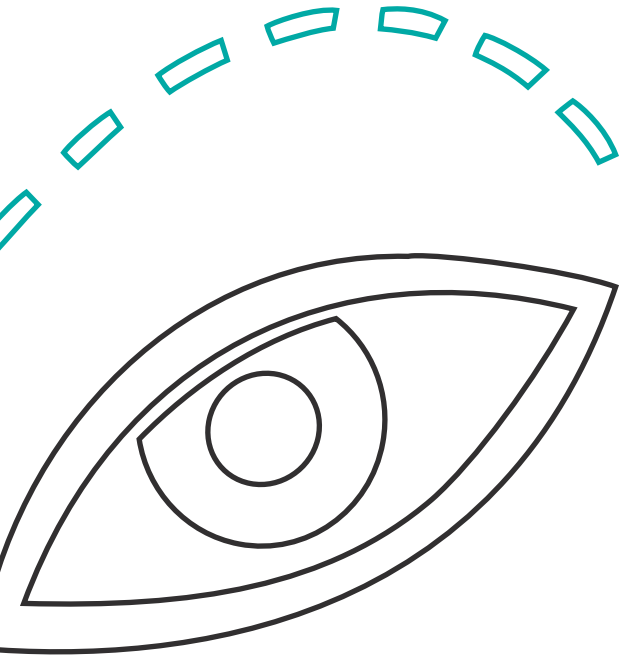
الشبكة الافتراضية الخاصة VPN

VPN هي اختصار لـ «Virtual Private Network»، وتعني الشبكة الافتراضية الخاصة، وكما هو واضح من اسمها فهي توفر لك اتصالاً آمناً بشبكات خاصة يوفرها لك التطبيق؛ مما يمنع أو يقلل من إمكانية تتبع نشاطك عبر الإنترنت، وبالتالي ستتيح لك تطبيقات الـ VPN حرية التجول بأمان دون خوف من المراقبة أو التعقب، واستخدام برامج الاتصال عبر الإنترنت بحرية تامة. صُمِمَت الشبكة الافتراضية الخاصة VPN لتُعطي خصوصيةً أكبر وسريةً أكثر في نقل البيانات والمعلومات، ويمكن إيجاز تعريفها في أنها عبارة عن توصيل شبكتين أو جهازين عن طريق الإنترنت، مع ضمان تشفير البيانات لحمايتها وكذلك إخفاء هوية المستخدم.

عند الاتصال التقليدي بالإنترنت، تنتقل البيانات من جهازك إلى مزوّد خدمة الإنترنت في بلدك ومن ثم إلى الإنترنت، وفي كل خطوة في هذا النوع من الاتصال تكون بياناتكم مكشوفة وبإمكان مزوّد الخدمة اعتراضها وكشف محتواها والتحكم بها. أما عند الاتصال بالإنترنت عبر شبكة خاصة افتراضية، تكون بياناتكم مشفرة عندما تنطلق من جهازكم وتمرّ عبر مزود خدمة الإنترنت إلى مخدّم الـ VPN، ومن ثم إلى الإنترنت. ولكون بياناتكم مشفرة، لا يستطيع مزود خدمة الإنترنت رصد حركتها. بعد وصول البيانات إلى مخدّم الـ VPN يتم فك تشفيرها هناك ومن ثم تمريرها إلى الموقع الذي تريدون دخوله.

تجدر الإشارة إلى أنه عند الاتصال عبر VPN، إن لم تستخدموا بروتوكول تشفير مثل https، فذلك يعني أن بياناتكم معرضة للكشف على مخدّم الـVPN الذي تتصلون به. لذلك عند تبادل معلومات حساسة ككلمات سرّ أو تعاملات بنكية، من الضروري التأكد من أن الموقع يعمل عبر بروتوكول https لضمان أمن بياناتكم من كافة الجهات.

يمكننا استخدام برنامج CyberGhost الذي يقدّم خدمة VPN، مع تقييم مرتفع من المستخدمين على متجر Google Play، وأكثر من ٣,٥ مليون نسخة منزلة على الأجهزة، وإشادة من المستخدمين بمقاييس الأمن والحماية المتبعة، والتحديث المستمر للتطبيق، والدعم الفني المتوفر في أي وقت، مع وجود بعض السلبيات ككثرة الإعلانات، ووضع حدود للسرعة في بعض الأحيان. وهو متوفر لأجهزة ويندوز وأندرويد وآي أو أس.




الحاسوب
قناة
مشفرة
المخترق لا يستطيع
الوصول الى بياناتكم
اتصال VPN
المواقع لا تعرف
هويتكم الحقيقية

الإنترنت

العنوان - الإنترنت
الهدف - أن يتفكر الطالب في أهمية الإنترنت في حياتنا

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يبدأ المدرب الورشة بتمرين إحماء. يُقسّم المدرب الطلبة لمجموعتين متساويتين من حيث العدد. تجلس المجموعة (أ) على كراسي ويقف خلف كل طالب في مجموعة (أ) طالب من المجموعة (ب). يحمل كل طالب في مجموعة (أ) قلماً وورقة ويكتب حرفاً، ويمرر الورقة للشخص الذي بجانبه، على الطلبة في مجموعة (أ) تكوين جمل مفيدة على كل ورقة من ترتيب الأحرف، ويكون على الطلبة في مجموعة (ب) أن يُخمنوا أكبر عدد ممكن من تلك الكلمات.	تنشيط للطلبة	تمرين	أوراق وأقلام	
٢٥ د.	يُقسّم المدرب المجموعة لمجموعتين. يطلب من مجموعة (أ) أن تُمثّل دور عائلة قبل زمن الإنترنت، وتمثل حياتهم اليومية. ويطلب من مجموعة (ب) أن تُمثل دور عائلة في زمن الإنترنت. يعطي المدرب ١٥ دقيقة لكل مجموعة حتى تبني القصة وتفكر بالمسرحية التي ستعرضها وتقسم الأدوار ، ثم يعطي ١٠ دقائق لكل مجموعة لكي تمثل المسرحية.	يتفكر الطلبة بمدى أهمية الإنترنت في حياتهم اليومية	لعب أدوار		مفضل أن يقوم المدرب بجولة بين المجموعتين ليتأكد من فهمهم للتمرين. إذا كان عدد أفراد المجموعة كبيراً، من الممكن أن يمثل البعض دور الضيوف، أو من الممكن تقسيم المجموعة إلى ٤ مجموعات وعرض ٤ مسرحيات.
١٥ د.	يقوم المدرب بتلخيص المسرحيات ليستذكر مع الطلبة ما تم عرضه، ثم يطلب منهم أن يشيروا إلى ما استنتجوه من هذه الفعالية. يمكن للمدرب أن يشير إلى تفاصيل مهمة حدثت في المسرحيات المختلفة ويشير إلى الفرق بينها.	يفهم الطلبة مدى أهمية الإنترنت في حياتنا	نقاش + شرح		

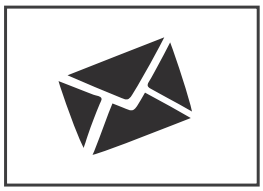
العنوان - الإنترنت
الهدف - يفهم الطلبة كيف يعمل الإنترنت
يفهم الطلبة ما هي مكونات الشبكة من أجهزة وبرامج

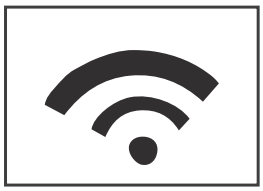
الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يطلب المدرب من الطلبة الوقوف بشكلٍ دائري ثم يبدأ أحد الطلبة بالعدّ من ١، ثم يليه الطالب الثاني بالرقم ٢، حتى الوصول إلى الرقم ١٠٠. شرط اللعبة هو أنه على المشتركين الذي يقع عليهم الرقم ٥ ومضاعفاته أن يقولوا كلمة «بوم»، ومن ينسى يخرج خارج اللعبة ويبدأ العد مرة أخرى من رقم ١.	تحفيز الطلبة	لعبة		
٣٠ د.	يسأل المدرب الطلبة هل فكروا مرة كيف يعمل الإنترنت؟ ثم يقسم المدرب الطلبة لـ٣ مجموعات ويوزع عليهم البطاقات المرفقة في ورقة العمل، ويطلب منهم أن يبنوا شبكة الإنترنت من هذه البطاقات. بحيث يقوم رامي من فلسطين بإرسال رسالة عبر البريد الالكتروني لسارة في أمريكا. تتسابق المجموعات من يبني الشبكة أولاً، ثم تعرض كل مجموعة الشبكة التي قامت ببنائها، وتشرح لماذا قامت ببناء الشبكة بهذه الطريقة. يعطي المدرب ١٥ دقيقة للمجموعات لكي تبني الشبكة، و٥ دقائق لكل مجموعة للعرض والنقاش.	يعرف الطلبة كيف يعمل الإنترنت وكيف تبنى الشبكة.	مسابقة	أوراق عمل	- يحرص المدرب على طباعة ورقة العمل وفقاً لعدد المجموعات. - على المدرب أن يصحح الأخطاء عند العرض على الفور (مرفق رسم توضيحي للمدرب حول بناء الشبكة).
٥ د.	يتفكر الطلبة بالتمرين وكيفية عمل الإنترنت	يفهم الطلبة مدى أهمية الإنترنت في حياتنا	تلخيص		

الإنترنت

مزود خدمة

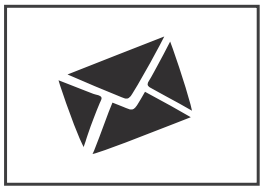
مزود خدمة

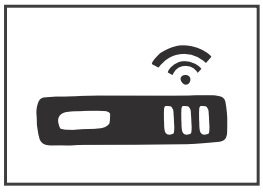

واجهة جيميل


واي فاي

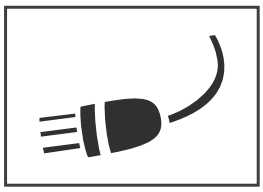

واي فاي


واي فاي

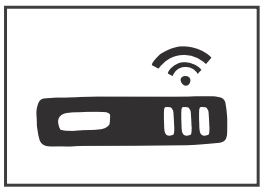

واجهة جيميل

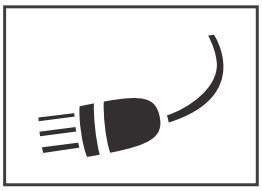

راوتر

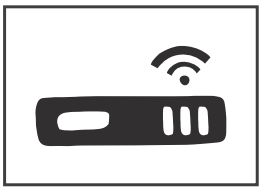

بوابة انترنت دولية


كوابل بحرية

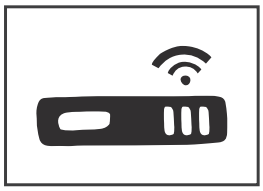

خادم سيرفر


راوتر

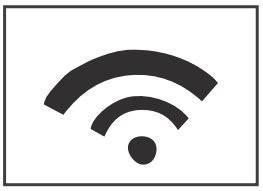

كوابل بحرية


راوتر

نظام نطاق الاسماء

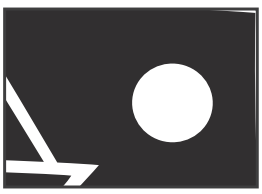

راوتر

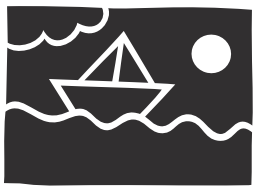

بوابة انترنت دولية

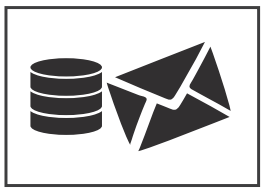

واي فاي


رامي

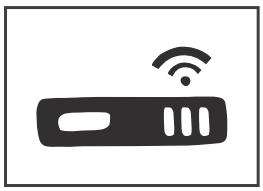

سارة

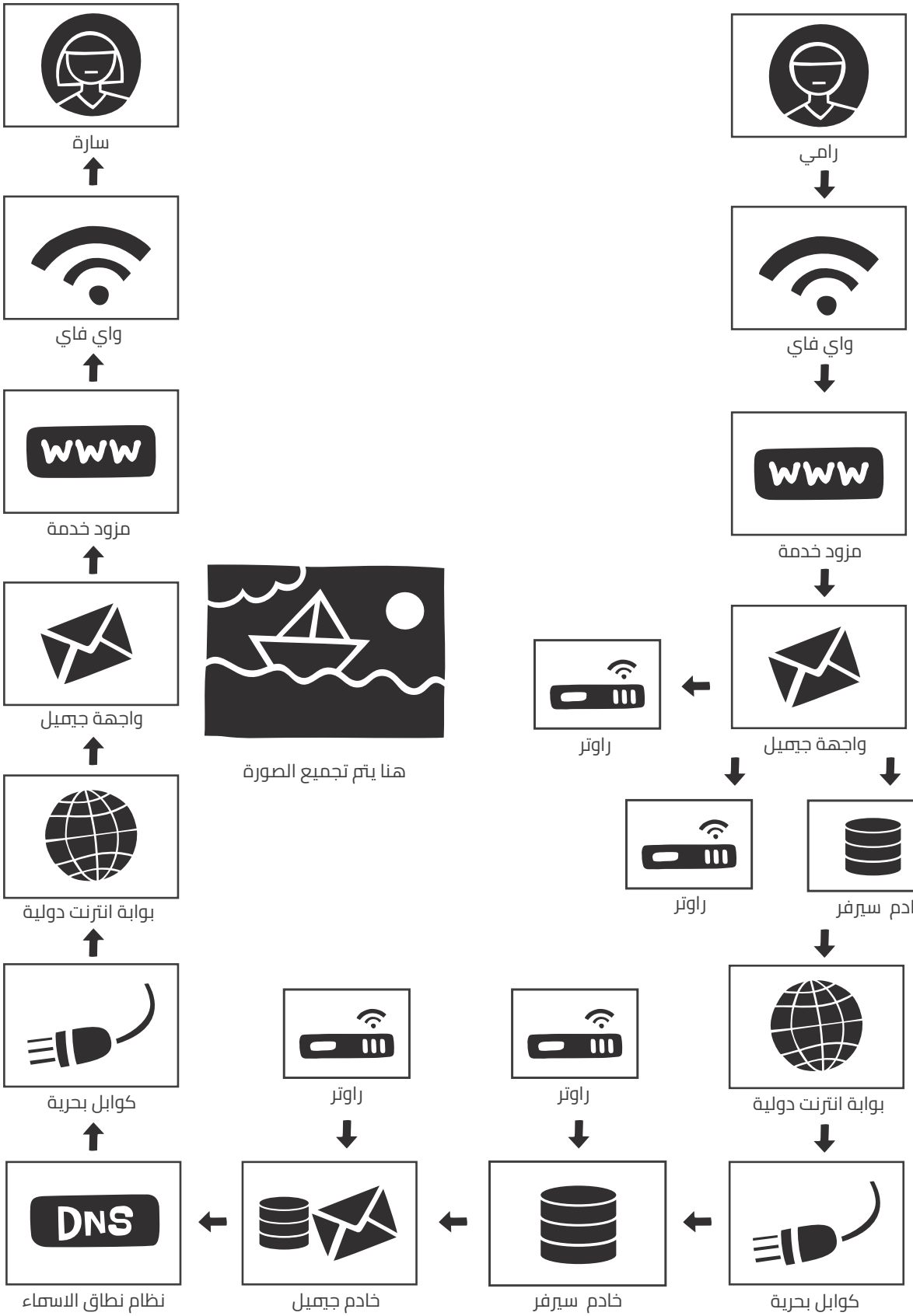



صورة


خادم جيميل


واي فاي


راوتر


رامي
واي فاي
مزود خدمة
واجهة جيميل
راوتر
راوتر
خادم سيرفر
بوابة انترنت دولية
كوابل بحرية
خادم سيرفر
خادم جيميل
نظام نطاق الاسماء
DNS
كوابل بحرية
بوابة انترنت دولية
واجهة جيميل
مزود خدمة
واي فاي
سارة
هنا يتم تجميع الصورة
راوتر
راوتر

تطبيقات الهاتف الذكي وصلاحياتها

أصبح الهاتف الذكي جزءاً مهماً في المجتمع، وهو عبارة عن هاتفٍ بميزاتٍ محوسبةٍ؛ بمعنى أنه يحتوي على مكوناتٍ صلبةٍ (Hardware) وبرمجياتٍ (Software). ولتعمل المكونات الصلبة كالشاشة، والسماعات، والكاميرا، والميكروفون وغيرها، لا بدّ من وجود نظامِ تشغيلٍ خاصٍ بالهواتف الذكية لإدارة هذه الأدوات الصلبة واستغلالها بشكل يضمن الانتفاع منها. فنظام تشغيل الهواتف الذكية يسهّل عملية استخدام الهاتف الذكي ويضمن تنفيذ عدة عمليات في وقت واحد. وأنظمة التشغيل مختلفة وأشهرها نظام «android» و «iOS» و«Windows Phone».

في دراسةٍ واستطلاع رأيٍ أجراه «حملة» - المركز العربي لتطوير الإعلام الاجتماعي، أكدّ ٩٤,٧٪ من الشباب الذين شملهم الاستطلاع أنهم يمتلكون هاتفاً ذكياً ويتمكنون من استخدامه، كما أكدّ ٩٢٪ منهم أنهم يستخدمون الإنترنت من خلال هواتفهم الذكية. توضّح هذه النتائج مدى انتشار الهواتف الذكية بين الشباب واستخدامها في الوصول لشبكة الإنترنت. يعود هذا الانتشار الكبير إلى سهولة استخدام الهاتف الذكي وسهولة التنقل به، وكذلك القدرة على إنجاز الأعمال من خلاله بسرعة أكبر. ومن إحدى الأسباب المهمة في انتشار الهواتف الذكية ازدياد تطبيقات الحوسبة السحابية (استخدام المصادر الحوسبية (العتاد والبرمجيات) عن طريق الإنترنت).

ولعل أبرز ما يميّز الهاتف الذكي إمكانية توفر الاتصال الدائم مع شبكة الإنترنت، ووجود تطبيقات تشمل كل شيء، فهو يوفر الملايين من التطبيقات المختلفة التي تستهدف اهتمامات الشباب من مختلف الأعمار وتنتشر عبر المتاجر الخاصة بكل نظام تشغيل على حدة. ولكي تعمل تطبيقات الهاتف الذكي، لا بدّ من استغلال مكونات الهاتف الصلبة والبرمجية، إلا أن التطبيقات بحاجة إلى إذنٍ مسبقٍ من المستخدم للولوج لبعض المكونات الصلبة للهاتف الذكي وبرمجياته. تكون هذه الصلاحيات غالباً ضرورية لسير عمل التطبيق وتشغيله، وفي حالة رفض هذه الصلاحيات فلن يتمكن المستخدم من استخدام هذا التطبيق على أكمل وجه. وتسمح الصلاحيات للتطبيق بأن يقوم بالاطلاع وقراءة بيانات الهاتف وربما التعديل عليها إن لزم ذلك.

وهناك اختلاف بين التطبيقات في هذا الأمر، بعضها يطلب صلاحية إرسال الرسائل النصية، أو إجراء المكالمات، أو استخدام «GPS» لتحديد المكان الجغرافي، أو التعديل والحذف في بطاقة التخزين،أو قراءة جهات الاتصال الخاصة بك، أو قراءة تاريخ تصفحك للمواقع، أو إدارة حساباتك الإلكترونية، أو استخدام «الكاميرا» لالتقاط الصور، أو الوصول إلى المقاطع المصوّرة، أو غير ذلك.

مكوّنات الهاتف الذكيّ

يُعبِّر مصطلح الهاتف الذكيّ (Smartphone) عن فئة من الهواتف المحمولة الحديثة التي تستخدم نظام تشغيل متطوّر، وشاشة لمس كواجهة للمستخدم في معظم الأحيان. لا تختلف الهواتف الذكيّة عن الحواسيب الشخصيّة كثيراً، وتتكون كل الأجهِزة الذكيّة من جُزأين مكملين لبعضهما البعض، وهما الجزء الفيزيائي (Hardware) المُمكن لمسُه، والجزء البرمجي المُشغِّل (Software) الذي يقود الجزء الأول (Hardware)، وأنت بدورك تقوده.

الجانب البرمجيّ (نظام التشغيل)

يجب أن يكون هناك مُنظِّم، مُحرِّك لكلّ شيء، في حالتنا هذه نظام التشغيل هو المُحرِك، الذي يُنظِم طاقات الأجزاء الفيزيائية. وتشمل أنظمة التشغيل الأنواع التالية: «ويندوز فون»، و«أندرويد»، و«بلاك بيري» و«آي أو أس».

الجانب الفيزيائي (مكونات الجهاز)

يتكوّن الجهاز الذكيّ من نفس المكوّنات الخاصة بالحاسب الشخصي لكن بقياسات وأحجام أصغر، وتعتمد كفاءة الجهاز بدرجة كبيرة على كفاءة هذه القطع، وأبرزها:

الذاكرة العشوائية (RAM)

وهي الذاكرة المؤقّتة المستخدمة لتخزين البيانات في الهواتف الذكية وتعتمد عليها البرامج أثناء تشغيلها. يستخدم نظام التشغيل وبرامج التطبيقات هذه الذاكرة في وقتٍ واحدٍ، لذلك فإن ذاكرة وصول عشوائية أكبر يمكنها تشغيل تطبيقات أكثر تعقيداً وفي نفس الوقت.

تطبيقات الهاتف الذكي وصلاحياتها

المُعالِج (Processor)

يقوم المعالِج بتنظيم ملايين العمليات الحسابية في كل ثانية. ومن بين العمليات التي يقوم بها المعالج في الهواتف الذكيّة: التصوير، وتشغيل الأفلام والأغاني والألعاب والتصفح على الإنترنت. لذلك فهو يُعدُّ عقل الهاتف الذكيّ.

البطاريّة (Battery)

تُقاس بالـ «ملي أمبير»، وكلما زادت سِعتها تحسّنت جودة المعالجة في الجهاز، لكن يجب الأخذ في الاعتبار قياس الشاشة وقوة المعالج لأنهما يزيدان من كمية الطاقة المسحوبة. يُنصح بعدم إجهاد الهاتف بتطبيقات عديدة في نفس الوقت (Multi-task) وعدم رفع إضاءَة الشاشة أكثر من الحاجة.

المساحَة الداخليّة (Internal Storage)

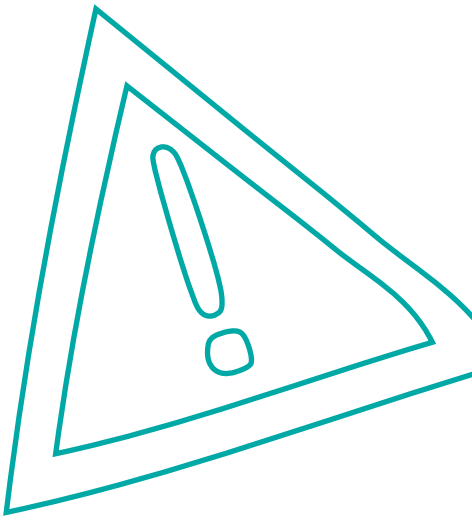
مساحة التخزين التي يُوفّرها الهاتف بعيداً عن (Memory Cards) تأتي ناقصة بسبب المساحة التي يشغِّلها نظام التشغّيل نفسه، كما أن التطبيقات تُنصّب أيضاً على هذه المساحة (يمكن نقل التطبيقات لبطاقة الذاكرة في بعض الهواتف)، كما تُخَزَن عليها بعض الملفات بشكل تلقائي. لا يُنصح عادة بشراء هاتِفٍ ذي مساحة داخليّة أقل من (١٦ GB).

هنا قائمة ببعض الصلاحيات الخطرة التي تتطلبها بعض التطبيقات وتستهدف خدماتٍ معينةً:

الخدمة	ما تحتويه الخدمة	الصلاحيات الخطرة	طبيعة الخطورة
التقويم (Calendar)	فعاليات ومناسبات قد تهتم بها الشركات لما تحتويه من تفاصيل نشاطات المستخدم.	- قراءة الفعاليات المُخَزَّنة في التقويم (reminder). - تعديل الفعاليات القديمة وإنشاء أخرى جديدة.	يمكن للتطبيق الذي يملك حق الوصول للتقويم من مشاركة الفعاليات وتمريرها لأطراف أخرى أو استخدامها في مناحي مختلفة (تجارية/ استخباراتية)، وربما يتمكن من حذف فعالياتك!
الكاميرا (camera)	استخدام الكاميرا ومشاركة الصور والفيديوهات المُلتَقَطة.	التقاط الصور والفيديوهات.	يمكن للتطبيق الذي يملك حق استخدام الكاميرا من التقاط صورٍ وفيديوهاتٍ في أي وقتٍ، ومشاركة هذه الصور والفيديوهات مع جهات قد تكون تجارية أو استخباراتية.
أرقام الاتصال (Contact)	أسماء أشخاصٍ، وأرقام هواتفهم	- قراءة أرقام الاتصال (READ_CONTACTS) - تعديل أرقام الاتصال وإنشاء أخرى (WRITE_CONTACT) - السماح بالدخول الى لائحة الحسابات في خدمة الحسابات. (GET_ACCOUNTS)	الاطلاع على معلومات الأشخاص المسجلين على الهاتف ومشاركتها، كأرقام هواتفهم ومعلوماتهم الخاصة، وكذلك التعديل عليها وإنشاء أرقام هواتف أخرى وربما حذفها. كما تتيح هذه الصلاحية الوصول إلى الحسابات المختلفة الموجودة على التطبيقات الأخرى كحسابات المستخدم على «فيسبوك» و»جوجل» مثلاً.

تطبيقات الهاتف الذكي وصلاحياتها

الخدمة	ما تحتويه الخدمة	الصلاحيات الخطرة	طبيعة الخطورة
الموقع (Location)	معرفة وتحديد الموقع الجغرافي للمستخدم	- الوصول لموقع المستخدم الدقيق. (ACCESS_FINE_LOCATION) - الوصول لموقع المستخدم التقريبي. (ACCESS_COARSE_LOCATION)	معرفة موقعك يساعد في استهدافك بمواد دعائية خاصة، وربما تكون معلومات مهمة للأجهزة الأمنية أو اللصوص الذين يودّون سرقة منزلك وأنت خارجه!
الميكروفون (Microphone)	تسجيل الصوت	- تسجيل مقاطع صوتية باستخدام «المايكروفون». (RECORD_AUDIO)	يمكن للتطبيق الذي يستخدم هذه الصلاحية تسجيل كل ما يدور حول الهاتف من أحاديث وأصوات، وفي أي وقت!
الهاتف (PHONE)	شبكة الهاتف ومُشغلها، ورقم الهاتف، بالإضافة لإمكانية إجراء مكالمات	- التعرف على رقم الهاتف واسم شبكة الاتصالات وحالة المكالمات التي تجري. (READ_PHONE_STATE) - إجراءُ مكالماتٍ من دون استخدام واجهة المستخدم الخاصة بإجراء المكالمات. بمعنى آخر، إجراء المكالمات من دون الحاجة لتأكيد المستخدم وبالتالي من دون الحاجة للمستخدم نفسه. (CALL_PHONE) - قراءة وتعديل قائمة المكالمات الواردة والصادرة وغير المجابة. (WRITE_CALL_LOG & READ_CALL_LOG) - إضافة بريد صوتي. (ADD_VOICEMAIL) - استقبال وإنشاء اتصالات عبر الإنترنت. (USE_SIP) - قراءة ومعرفة الرقم الذي تقوم بالاتصال به مع أمكانية إعادة توجيه الاتصال لرقم آخر أو إحباط المكالمة تماماً. (PROCESS_OUTGOING_CALLS)	يقوم التطبيق الذي يملك هذه الصلاحيات بإحباط عمليات الاتصال، أو إجراء مكالمات دون علمك، بالإضافة لإمكانية العبث بقائمة المكالمات وتغيير محتوياتها ومشاركة هذه المعلومات مع أطراف لن ترضى عنها(تجارية\استخباراتية).



الخدمة	ما تحتويه الخدمة	الصلاحيات الخطرة	طبيعة الخطورة
التخزين (STORAGE)	تخزين ملفات، وقراءة الملفات المخزنة	- قراءة محتويات بطاقة الذاكرة الرقمية وأماكن التخزين الأخرى. (READ_EXTERNAL_STORAGE) - حفظ الملفات في الذاكرة أو بطاقة الذاكرة الرقمية (WRITE_EXTERNAL_STORAGE)	يقرأ التطبيق أو يُغير أو يحذف أياً من الملفات المخزنة على الهاتف الخاص بالمستخدم.
الحساسات (SENSORS)	معلومات بيولوجية حول المستخدم وصحته	يتمكن التطبيق من الوصول لمعلومات من خلال الحساسات التي يستخدمها مالك الجهاز لقياس ما يحدث داخل جسم المستخدم، كمعدل ضربات القلب وبصمة الاصبع. (BODY_SENSORS)	مقدرة التطبيق على استقبال بيانات حول ما يحدث داخل جسمك، واستخدام هذه المعلومات ومشاركتها لأهداف تجارية.
أرقام الاتصال (Contact)	أسماء أشخاصٍ، وأرقام هواتفهم	- قراءة أرقام الاتصال (READ_CONTACTS) - تعديل أرقام الاتصال وإنشاء أخرى (WRITE_CONTACT) - السماح بالدخول الى لائحة الحسابات في خدمة الحسابات. (GET_ACCOUNTS)	الاطلاع على معلومات الأشخاص المسجلين على الهاتف ومشاركتها، كأرقام هواتفهم ومعلوماتهم الخاصة، وكذلك التعديل عليها وإنشاء أرقام هواتف أخرى وربما حذفها. كما تتيح هذه الصلاحية الوصول إلى الحسابات المختلفة الموجودة على التطبيقات الأخرى كحسابات المستخدم على «فيسبوك» و»جوجل» مثلاً.

لمراجعة الصلاحيات التي تم إعطائها بشكل تلقائي عند تحميل تطبيق ما في «الأندرويد»، يمكن الدخول إلى الإعدادات (Settings) والضغط على التطبيقات (Applications) ثم الضغط على التطبيق الذي تريد عرض صلاحياته وإعادة التحكم بها (يمكن أن تكون لهذه البنود والبنود التالية في القائمة أسماءً مختلفة قليلاً في إصدار الأندرويد الخاص بك).

تطبيقات الهاتف الذكي وصلاحياتها

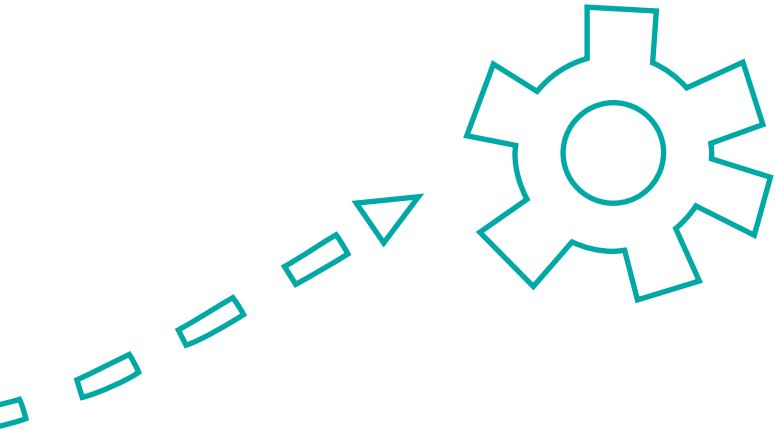
كيفية إعداد صلاحيات التطبيق

علينا أن ننظر بعنايةٍ لكل صلاحيةٍ قبل الاستجابة لها. فعلى سبيل المثال، إذا طلب تطبيقٌ لتعديل الصور الوصول إلى صلاحية تحديد موقعنا الحالي فهذا أمرٌ غريبٌ وغير ضروري. وفي الوقت ذاته، تحتاج تطبيقات الخرائط إلى الوصول لبيانات نظام تحديد المواقع، ولكنها لا تحتاج إلى الوصول إلى قائمة جهات الاتصال أو الرسائل النصية القصيرة.

في نسخة «أندرويد ٦» (مارشميلو) وما بعدها من تحديثات على نظام «أندرويد»، تطلب التطبيقات من المستخدمين الموافقة عندما تحتاج إلى «إذن خطر» كقراءة محتويات الذاكرة وجهات الاتصال، إذا لم نكن نريد الاستجابة يمكننا رفض الطلب دائماً. وبالطبع إذا كان التطبيق يحتاج إلى هذه الصلاحيات ولم نُلبيها فلن يعمل التطبيق بالشكل الصحيح.

ورغم ذلك، تحتاج بعض التطبيقات حقاً إلى الكثير من الصلاحيات. على سبيل المثال، تحتاج برامج الحماية من الفيروسات إلى الكثير من الصلاحيات لفحص النظام وحمايته من التهديدات بشكلٍ مسبق. والنتيجة هنا بسيطة: دعونا نفكر قليلاً قبل منح أي صلاحية معينة، فيما إذا كان التطبيق يحتاج حقاً لتلك الصلاحية أم لا.

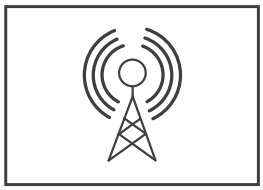
وأخيراً وليس آخراً: فإن أكثر المستخدمين حذراً لا يُعَدُّ في مأمنٍ من استغلال البرامج الخبيثة المستغِلة للثغرات الأمنية في النظام. ويعد هذا هو السبب الرئيسي خلف أهمية إدارة الصلاحيات الخاصة بك على النحو الصحيح، مما يساعد في حماية خصوصيتك من تطبيقات التجسس. إن تثبيت تطبيقٍ أمنيٍ موثوقٍ به من شأنه حماية جهازك ضد أكثر الفيروسات خطورة مثل فيروس «حصان طروادة» وغيره من الفيروسات الأخرى.

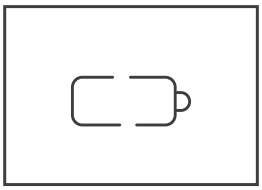


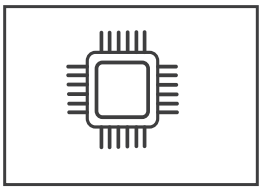
العنوان – الهاتف الذكي
الهدف: يفهم الطالب كيف يعمل الهاتف الذكي

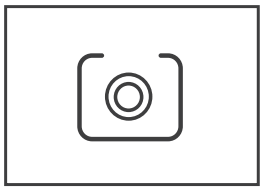
الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يقسم المدرب المجموعة الى قسمين، ويخرج من كل مجموعة طالب، يعطي المدرب الطالبين نفس الكلمة، على كل طالب أن يُمثل أو يشرح هذه الكلمة لمجموعته بدون كلام.	تنشيط الطلبة وكسر الجليد	لعبة		
١٥ د.	يقسم المدرب الطلبة لمجموعات ويطلب منهم ان يرسموا الهاتف الذكي مع مكوناته وان يشيروا مما يتكون الهاتف الذكي ثم يعرض الطلبة ما توصلوا له في المجموعات تختار كل مجموعة طالب ليعرض مما يتكون الهاتف الذكي امام الجميع	يتفكر الطلبة كيف يعمل الهاتف الذكي	مجموعات عمل	اوراق واقلام	
٢٠ د.	يقوم المدرب بتوزيع بطاقات العمل على الطلبة ويطلب منهم ان يضعوا البطاقات التي يحتاجها الهاتف الذكي لكي يعمل ويشرحوا لماذا	يفهم الطالب كيف يعمل الهاتف الذكي	مجموعات عمل	بطاقات عمل	التأكد من طباعة البطاقات قبل الورشة

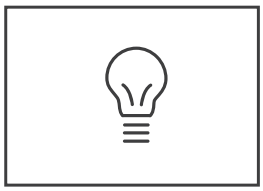
تطبيقات الهاتف الذكي وصلاحياتها

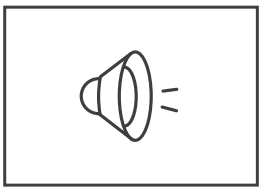

نطاق الترددات الأساسية

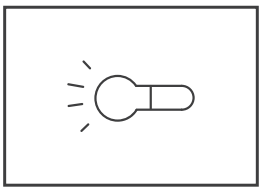

البطارية

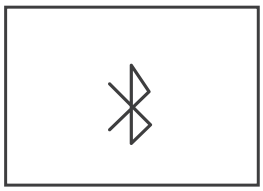

وحدة المعالجة المركزية


كاميرا

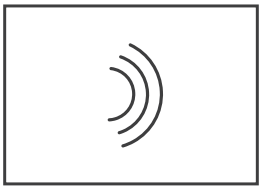

مستشعر الضوء

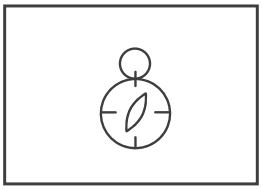

مذياع / سبيكر

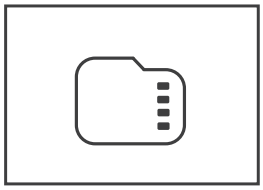

مستشعر البيئة


بلوتوث

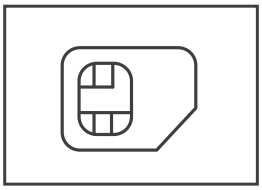

نظام تحديد المواقع


اتصالات قريبة المدى

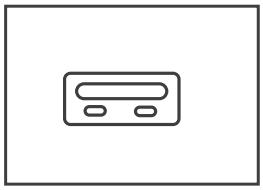

مجسات الموقع


بطاقة SD

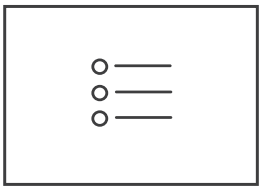

واي فاي


شريحة هاتف محمول


ميكروفون

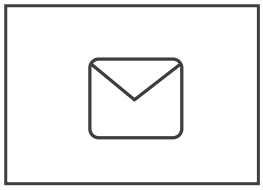

منفذ USB

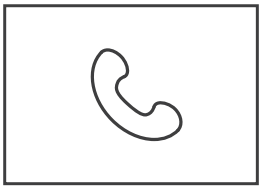

الصور


الأجندة / جدول الأعمال

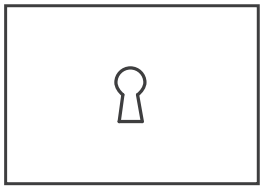

الرسائل

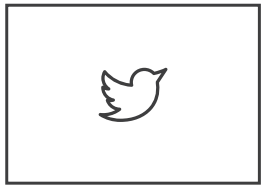

الخرائط

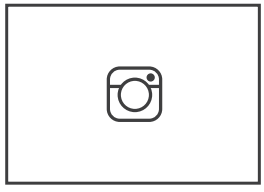

البريد


الهاتف


فايرفوكس


سيجنال


تويتر


انستاغرام


فايسبوك


واتساب

عنوان الدرس: صلاحيات تطبيقات الهواتف الذكية
الهدف: يتعرّف الطلبة على الصلاحيات الممنوحة للتطبيقات التي يستخدمونها.
يفهم الطلبة سبب وجود هذه الصلاحيات.
يكوّن الطلبة مهارة التعامل مع التطبيقات والصلاحيات التي تطلبها.

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يقوم الطلبة بالوقوف بشكل خط مستقيم. تتم الإشارة إلى أن يمين الخط يعني أن المشارك موافق على المقولة التي ستطرح، أما من يقف على يسار الخطّ فهذا يعني أنه غير موافق عليها. يطرح المدرب ٤ أسئلة للتعرف على الأشخاص، ويتم التعرف على أسماء الطلبة من خلال سؤالهم عن اسمهم أثناء تفسيرهم لماذا وقفوا في هذه الجهة دون الأخرى. ١. استخدم الهاتف الذكي أكثر من الحاسوب. ٢. التطبيقات في الهاتف الذكي تساعدنا في تسهيل حياتنا؟ ٣. تحتاج التطبيقات في هاتفي لاستخدام بياناتي من أجل أن تعمل؟ ٤. استخدم التطبيقات بشكل يجعلني أكثر أمناً؟	تنشيط الطلبة وتحضيرهم للورشة	لعبة		يمكن للمدرب اختيار أسئلة أخرى لها علاقة بموضوع التطبيقات.
١٥ د.	- يُشكّل المدرب مجموعات عمل، كل مجموعة من طالبين، ويوزع عليهم ورقة عمل حول الهاتف الذكي. (صورة هاتف ذكي فارغ من الداخل) - يتناقش الطالبان مع بعضهما حول تطبيقاتهما المفضلة، ثم يختارون ٤ تطبيقات لا يستطيعان التخلي عنها ويرسمانها داخل صورة الهاتف الذكي. - تعرض كل مجموعة الخيارات التي اعتمدتها، ثم يدخل المدرب في نقاش معهم حول سبب اعتماد هذه الخيارات. -يشرح المدرب طريقة عمل تطبيقات الهاتف الذكي وصلاحياتها.	- يتفكر الطلبة في كيفية استخدامهم لتطبيقاتهم المفضلة. - يفهم الطلبة الخلفية التقنية البسيطة للتطبيقات. - يفهم الطلبة القواعد التقنية لطريقة عمل تطبيقات الهاتف الذكي والصلاحيات اللازمة لتؤدي عملها.	مجموعات عمل، ومناقشة، وشرح	لوح وأقلام نسخ ورقة عمل، هاتف ذكي.	يحتاج المدرب لشرح كيفية معرفة الصلاحيات الممنوحة لكل تطبيق وآلية الوصول إليها في نظام «الاندرويد». يمكن الوصول إلى إعدادات الهاتف ثم التوجه إلى التطبيقات ثم اختيار التطبيق والنظر إلى الترخيص ومن هناك الدخول إلى كل الأذونات الممنوحة.

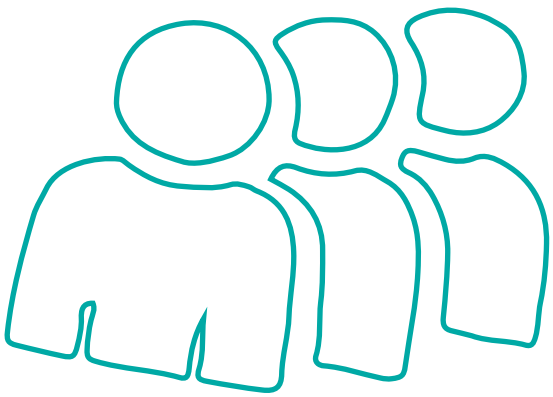
تطبيقات الهاتف الذكي وصلاحياتها

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
٢٠ د.	- يُقسّم المدرب الطلبة لمجموعات. تُعطى كل مجموعة تطبيقاً معيناً، ويُطلب منهم فحص صلاحيات هذا التطبيق وتسجيلها على ورقة، ثم فحص ما إذا كانت هذه الصلاحيات ضرورية لعمل هذا التطبيق أم لا. - يدخل المدرب في نقاش مع الطلبة. يطرح المدرب السؤال «هل هذه التطبيقات بحاجة لهذه الصلاحيات لكي تعمل، لماذا؟» ويبدأ بشرح كل التفاصيل المتعلقة بذلك.	- يكتشف الطلبة بأنفسهم الصلاحيات الممنوحة للتطبيقات التي يستخدمونها. - يفهم الطلبة أسباب وجود هذه الصلاحيات.	مجموعات عمل، ونقاش، وشرح	هواتف ذكية وأوراق وأقلام. نسخ ورقة العمل.	يجب التأكد من توفر هواتف ذكية مع المجموعة.

واجب بيتي

يقوم المدرب/ة بتلخيص ما تمت مناقشته مع الطلبة حول التطبيقات.

يطلب المدرب/ة من الطلبة التفكير بتوصيات يوجهونها إلى الشباب لحماية أنفسهم من الصلاحيات التي تطلبها التطبيقات، ويقترحون تطبيقات آمنة بعد أن يقوموا بفحص الأذونات الممنوحة للتطبيقات.



عنوان الدرس: صلاحيات تطبيقات الهواتف الذكية.
الهدف: يعرف الطلبة الصلاحيات الممنوحة للتطبيقات التي يستخدمونها.
يفهم الطلبة سبب وجود هذه الصلاحيات.
يكوّن الطلبة مهارة التعامل مع التطبيقات والصلاحيات التي تطلبها.

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يقف الطلبة على شكل دائرة، يُقسّم المدرب الطلبة لأربع مجموعات. يسمي كل مجموعة باسم تطبيق (سنابتشات، انستجرام، فيسبوك، واتساب) ويطلب من كل مجموعة تَذكُرَ مميزاتها.	التفكير في المحتويات التي يشاركها الطلبة في كل تطبيق.	تمرين تحفيزي		من المفضل أن يقوم الطلبة بالوقوف من أجل كسر الحواجز والتفاعل بشكل أكبر.
٢٠ د.	- يُقسّم المدرب الطلبة لعدة مجموعات ويوزع عليهم القصص المختلفة المرفقة للجدول (يوزع المدرب قصة لكل مجموعة). - يطلب المدرب من الطلبة أن يقوموا بتوضيح ما إذا كان تصرف الشخصية آمناً أم لا، مع توضيح الأسباب. - يناقش الطلبة هذه المواضيع داخل المجموعات، ثم يعرضون القصص التي معهم ويناقشونها مع المدرب والمجموعات الأخرى بشكل جماعي.	تفكير الطلبة في طبيعة المحتوى الذي يشاركونه عبر التطبيقات المختلفة.	مجموعات عمل ونقاش	أوراق عمل	يتأكد المدرب من طباعة أوراق العمل
١٥ د.	يفتح المدرب النقاش من أجل أن يسمع قصص الطلبة الشخصية، ويطلب منهم التفكر بالتصرفات السليمة وغير السليمة لاستخدام هذه التطبيقات ثم يشرح المدرب معنى الخصوصية وأهميتها.	يخرج الطلبة بتوصيات حول موضوع الخصوصية في استخدام التطبيقات.	مجموعات عمل	أوراق اقلام	

وظيفة بيتية

يطلب المدرب من الطلبة العمل بمجموعات لكتابة توصيات من شأنها مساعدة الطلبة للحفاظ على خصوصيتهم أثناء استخدام تطبيقات الهاتف الذكي، وذلك وفق قائمة «أفعل ولا أفعل»، حسب كل تطبيق على حدة. يمكن للطلاب الاستعانة بهذه الأسئلة لكتابة التوصيات: ما اسم التطبيق؟ ما هي المهام التي يقوم بها التطبيق؟ هل هو مجاني؟ ما هي الصلاحيات التي يطلبها؟ أي من هذه الصلاحيات ضرورية من أجل عمل التطبيق؟ ولماذا؟ ما الصلاحيات الأخرى التي يطلبها التطبيق والتي حسب رأيك ليست ضرورية لعمل التطبيق؟ ولماذا؟

تطبيقات الهاتف الذكي وصلاحياتها

ورقة عمل

قصة ١

سافرت سلمى مع أهلها في رحلة إلى أوروبا، قامت سلمى بتوثيق الرحلة من خلال تطبيق «سنابشات»، وتفاعلت مع أقربائها وأصدقائها المقربين من خلال تصوير فيديوهات للعائلة وهم يقتنون المجوهرات ويسهرون في الفندق.

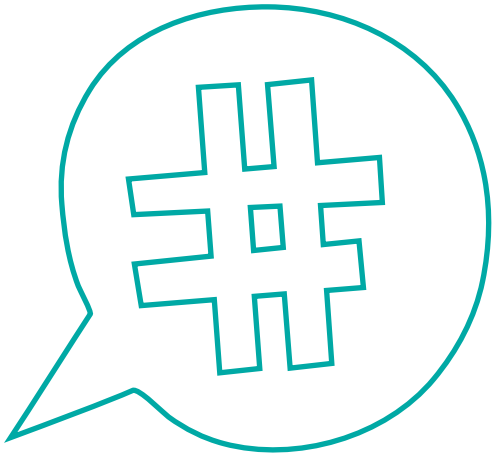
يقوم أقاربها وأصحابها بالتفاعل مع هذه الفيديوهات بشكل كثيفٍ ودائمٍ ويسألون عن تفاصيل الفيديوهات القصيرة، أين تم تصويرها؟ وماذا يفعلون تحديداً؟.
تملك سلمى حسابات أخرى على «فيسبوك»، «انستجرام»، «واتساب» إلا أنها لم تشارك صور الرحلة هناك إلا بعد عودتها من السفر.

ما رأيكم في تصرف سلمى؟

قصة ٢

يملك أحمد حساباً على «فيسبوك»، يقوم من خلاله بإبداء آرائه السياسية في كل ما يتعلق بأخبار الساعة، ويعتبر أن هذا حق له، لذلك يقوم أحمد بجعل كل المنشورات التي يكتبها عامة.
ما رأيكم في ذلك؟

هل هذا تصرف آمن؟
هل على أحمد أن يتوقف عن نشر آرائه عبر حسابه على «الفيسبوك»؟



قصة ٣

يهتم سليمٌ بمعرفة من قام بزيارة حسابه على «الفيسبوك»، فقام بتحميل تطبيق (من قام بزيارة حسابك)، وقد قام التطبيق بترشيح أحد أصدقائه المقربين كأحد الأشخاص الذين قاموا بزيارة حسابه مؤخرا.

كيف يعمل هذا التطبيق حسب رأيكم؟
هل نجح سليم بمعرفة من زار حسابه على «الفيسبوك» حقا؟

قصة ٤

تعمل لارا في مجال المبيعات، فتتلقى اتصالات من عملائها وزبائنَ محتملين جددٍ بشكل مستمر، لذلك قامت بتحميل تطبيق «تروكولر» لكشف أسماء المتصلين، تفاجأت لارا عندما اتصلت لها صديقتها سارة أن التطبيق قام بتسمية سارة بـ»سوسو الأمورة» رغم أن الرقم محفوظٌ في جهازها باسم سارة.

كيف حصل ذلك حسب رأيكم؟

قصة ٥

هيا ودنيا صديقتان مذ كانتا في السابعة من العمر، تتشارك هيا ودنيا كل أسرارهما سويةً، حتى كلمات السر في مواقع التواصل المختلفة.
هيا ودنيا في المرحلة الثانوية الآن وقد نشب بينهما خلاف، فقامت دنيا بكتابة منشور من حساب هيا تقول فيه « أنا أكره أهلي وسوف أقوم بقتلهم يوماً ما »

ما رأيك بتصرف هيا ودنيا، وكيف يجب أن تتصرف هيا إزاء ما حصل؟

المتصفّحات

تعـدّ متصفّحـات الإنترنـت البوابـة التـي يَعـبرُ مـن خلالهـا المسـتخدم إلى الشـبكة العنكبوتيـة، ليتصفّـح كل مـا قـد تـمّ تحميلـه عـلى هـذه الشـبكة الواسـعة. فالغـرض الأسـاسي مـن متصفّـح الإنترنـت هـو جلـب مـوارد المعلومـات وتقديمهـا للمسـتخدم بشـكلٍ سـهلٍ ومبـاشرٍ.

ومـن أبـرز المتصفّحـات وأقدمهـا متصفّـح «مايكروسـوفت إيـدج» (Microsoft Edge) الـذي يُنصَّـب بشـكلٍ تلقـائي مـع نظـام التشـغيل «ويندوز»، وكذلـك متصفّحـا «جوجـل كـروم» (Google Chrome) و«موزيـلا فايرفوكـس» (Mozilla Firefox) واسـعا الانتشـار، بالإضافـة لمتصفّـح «أوبـرا» (Opera) وسـفاري (Safari) وهـما الأقـل رواجـاً.

عنـد تصفّـح الإنترنـت، فإننـا بشـكل مـن الأشـكال مرَاقَبـون. فـلأن كثـيراً مـن المواقـع الإلكترونيـة ترغـب في الحصـول عـلى أكـبر قـدرٍ ممكـنٍ مـن المعلومـات عنـا وحولنـا، فإنهـا – أي المواقـع – تُثبـتُ برمجيـات بأحجـام صغـيرة جـداً تدعـى ملفـات تعريـف الارتبـاط أو (Cookies) في المتصفّـح الخـاص بنـا، تسـاعدها في معرفـة مـا هـي أكـثر المواقـع التـي نرتادهـا ونتنقـل بـين صفحاتهـا.

كـما أن هنـاك طريقـةً أخـرى شـائعةً للتعقـب تعتمـد عـلى تثبيـت برنامـج في المتصفّـح يدعـى (Adware)، وهـو نـوع مـن البرامـج يراجـع المواقـع الإلكترونيـة التـي نزورهـا بشـكلٍ دوريٍّ، ليقـوم بعـد ذلـك تلقائيـاً بإظهـار الإعلانـات أمامنـا بمـا يتناسـب مـع محتـوى تلـك المواقـع. كـما أن هنـاك مواقـع إلكترونيـة قـادرة عـلى تحديـد موقعنـا الجغـرافي مـن خـلال عنـوان «بروتوكـول الإنترنـت» (IP).

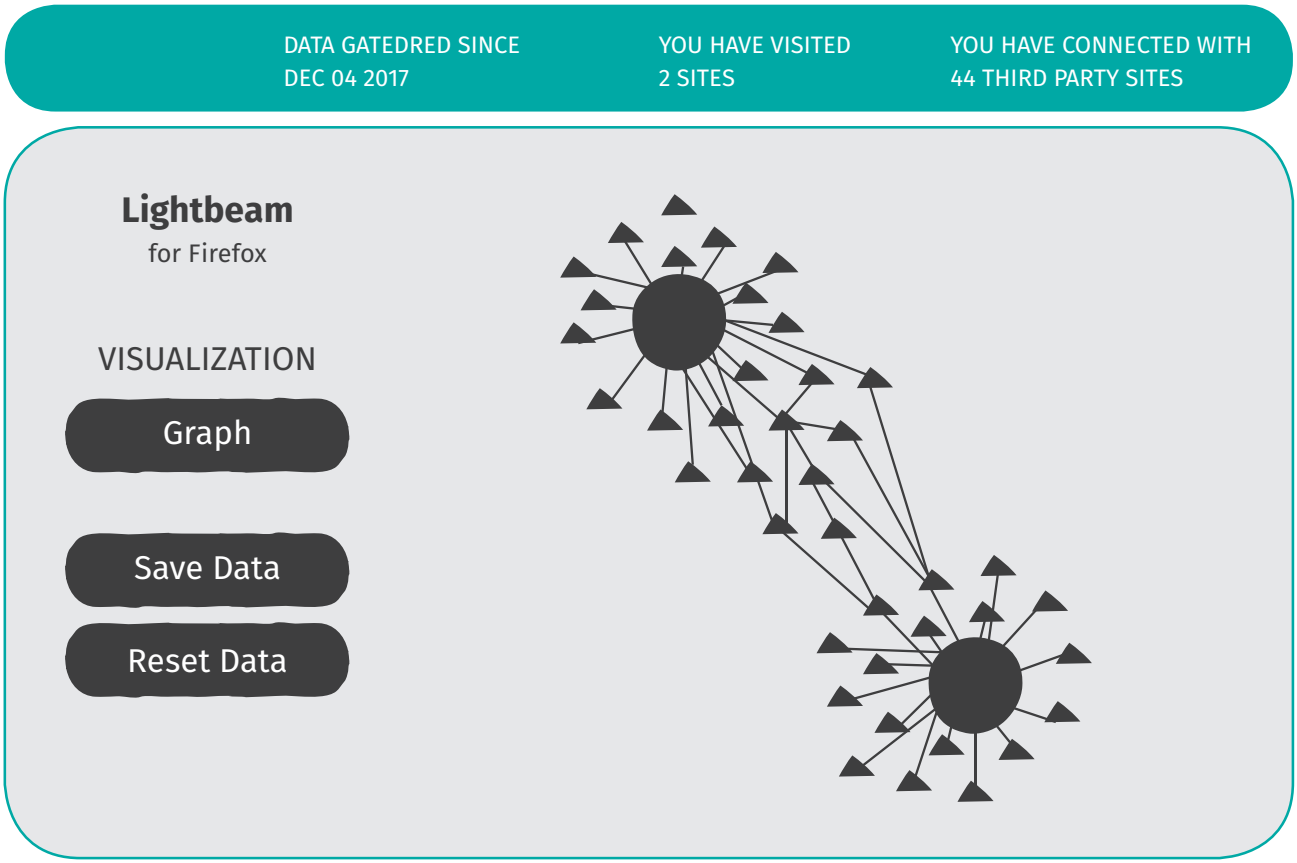
يُمكـن لأيّ موقـع إلكـتروني تعقـب نشـاط المسـتخدم عـلى الإنترنـت وانتهـاك خصوصيتـه، وذلـك عنـد اسـتخدام المتصفّحـات العاديـة مثـل «مايكروسـوفت إيـدج» و«فايرفوكـس» و«جوجـل كـروم» و«سـفاري»، في المقابـل، يُمكـن للمسـتخدمين تجربـة بعـض المتصفّحـات التـي توّفـر حمايـةً للخصوصيـة وتشـفيراً لبيانـات المسـتخدم، وتمنـع كذلـك خاصيـة التعقـب.

تُعـرّف المتتبِعـات (Trackers)، وتُدعـى كذلـك «تقنيـات الطـرف الثالـث»، بأنهـا ملفـات تتعقـب متصفّـح الإنترنـت، لتقـوم بجمـع المعلومـات حـول المواقـع التي نزورهـا وبيانـات أجهزة المسـتخدمين. وتشـمل المتتبعات ملفـات «الكوكيـز» (ملفـات تعريـف الارتبـاط) ومنـارات الشـبكة و«كـوكي فـلاش» وعلامـة «البيكسـر» وعنـوان «بروتوكـول الإنترنـت» (IP) الخـاص بنـا. تجمـع هـذه المتتبِعـات معلومـات حـول تاريـخ التصفـح، وحجـم الشاشـة، والمنطقـة الزمنيـة، والمكونـات الإضافيـة، ونظـام التشـغيل، كل هـذه الأشـياء تُمثـلُ بصمـةً فريـدةً لـكل واحـد منـا، وبالتـالي تتمكـن المتصفّحـات بسـهولة مـن التعـرّف علينـا بوسـاطة هـذه البصمـة.
قـد تتواجـد المتتبِعـات في المواقـع الإلكترونيـة عـلى شـكل متعقـبٍ واحـدٍ فقـط أو قـد تصـل لسـتين (٦٠) متعقبـاً للموقـع الواحـد، وقـد لا يكـون هنـاك أي متعقّـبٍ في الموقـع الإلكـتروني. بعـض هـذه المتتبِعـات (Trackers) ضروريـة تقنيـاً لعمـل الموقـع الإلكـتروني بالشـكلِ الصحيـح، كالمتعقِبـات الخاصـة بإعطـاء صاحـب الموقـع فكـرة حـول حركـة المـرور (أي نشـاط المسـتخدمين عـلى موقعـه، والوقـت الـذي يقضونـه فيـه، وغـير ذلـك)، إلا أن هنـاك معلومـات حـول العمـر ومـكان السـكن والأشـياء التـي تهمّنـا والمواضيـع التـي نقـرأ، كل هـذه المعلومـات يتـم تصديرهـا لـشركات الإعلانـات أو الحكومـات.

عنـد قبـول هـذه المتَتَبِعـات (تقنيـات الطـرف الثالـث) نكـون قـد سـمحنا لجميـع المتعقِبَـات الموجـودة بالوصـول إلى معلوماتنـا. ومـن بينهـا بعـض المتعقِبَـات المرئيـة كـزر الإعجـاب عـلى «فيسـبوك» وطائـر «تويـتر» الصغـير وزر «جوجـل+» (+G).

يمكننـا فحـص درجـة الأمـان في المتصفّـح الخـاصّ بنـا مـن خـلال خدمـة (panopticlick) التـي تُبـيّن إذا مـا كان متصفّحنـا متصفحـاً آمنـاً مـن متتبعـات الإعلانـات والمتتبعـين غـير المرئيـين وبصـمات التصفـح. كـما يمكننـا مشـاهدة المتعقبـات عـلى متصفّـح «فايرفوكـس» مـن خـلال أداة (Lightbeam) وملاحظـة كيـف تـؤدي المتعقِبَـات دورَهـا في التواصـل والترابـط فيـما بينهـا.

في الصورة أدناه، قمنا بتصفّح موقعين إلكترونيين، فتبين أن هذين الموقعين تقبّلوا ٤٤ متتبعاً!



المتصفّحات

محاولة للحدّ من تلك السلبيات، يمكننا استخدام أداة (Privacy Badger) التي تقوم بتحديد الإعلانات التي تتجسس علينا عبر الإنترنت وحجبها تلقائياً، كما تقوم بحجب كافة أنواع المتتبعات. تعدّ هذه الأداة مُركّباً إضافياً للمتصفّح، تحلّلُ المواقع الإلكترونية للكشف عن المحتوى الذي يتتبّع نشاطاتنا وتحجبه. فحينما نزور موقعاً ما، فإن هذه الأداة ترصد كذلك المحتوى الذي تم تضمينه من مواقع أخرى، أو ما يُعرَف بمواقع «الطرف الثالث» كالصور والبرمجيات الصغيرة والإعلانات. وفي حال كانت إحدى تلك المواقع من النوع الذي يتتبع، فإن هذه الأداة ستمنع ظهور أي محتوى يتضمن أوامر برمجية للتتبع.

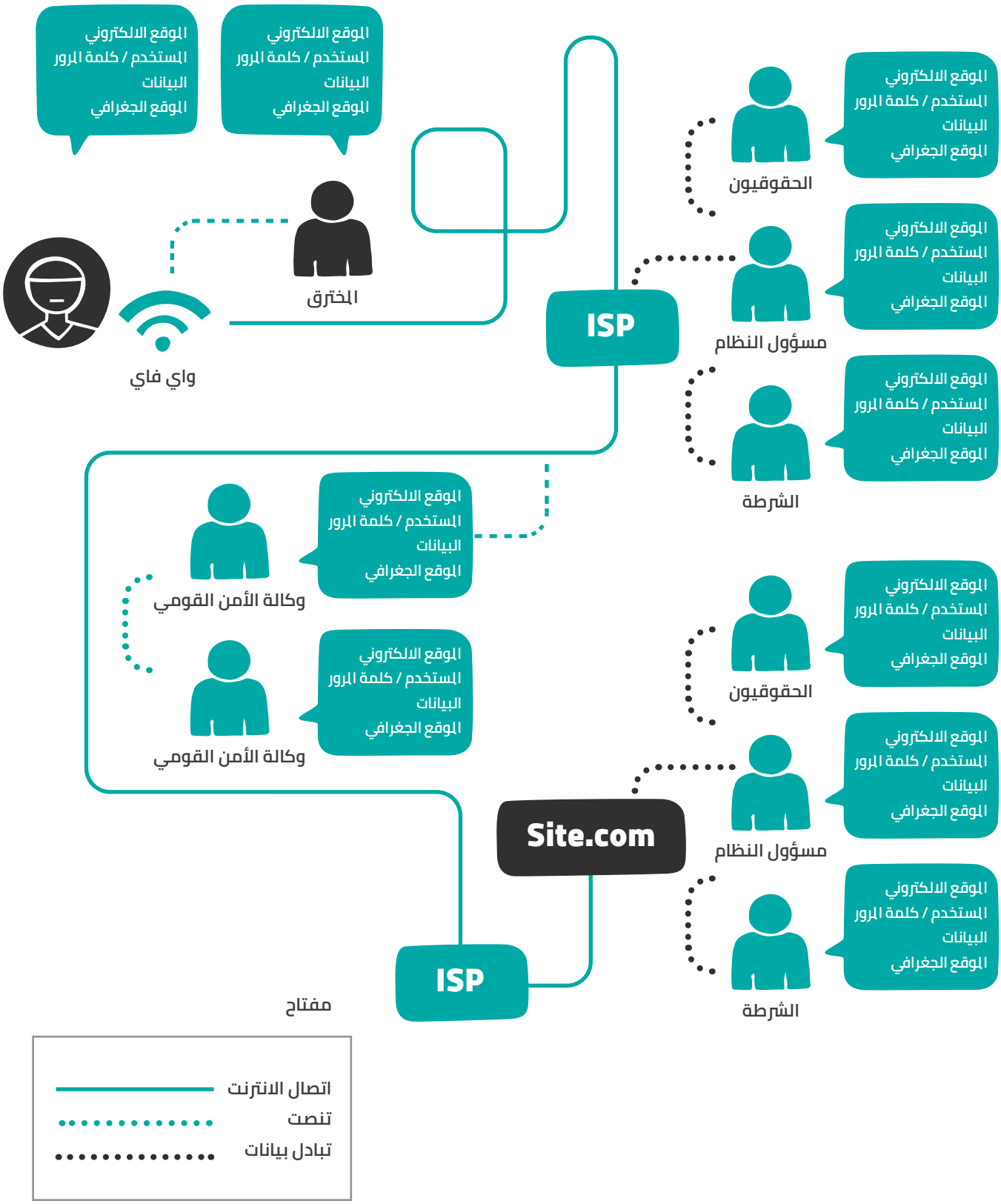
كما تمكن الاستفادة من أداة (Ghostery) التي تمنع المواقع والشركات من تعقب خصوصية الزائر، وذلك عبر منع وصولها إلى بيانات الشخص المستخدم، وتتيح الأداة لمستخدميها درجة تحكم كبيرة تمكنهم من تحديد المواقع التي تتعقب خصوصيتهم وتستهدف بياناتهم، وهي متوفرة لجميع أنواع المتصفّحات.

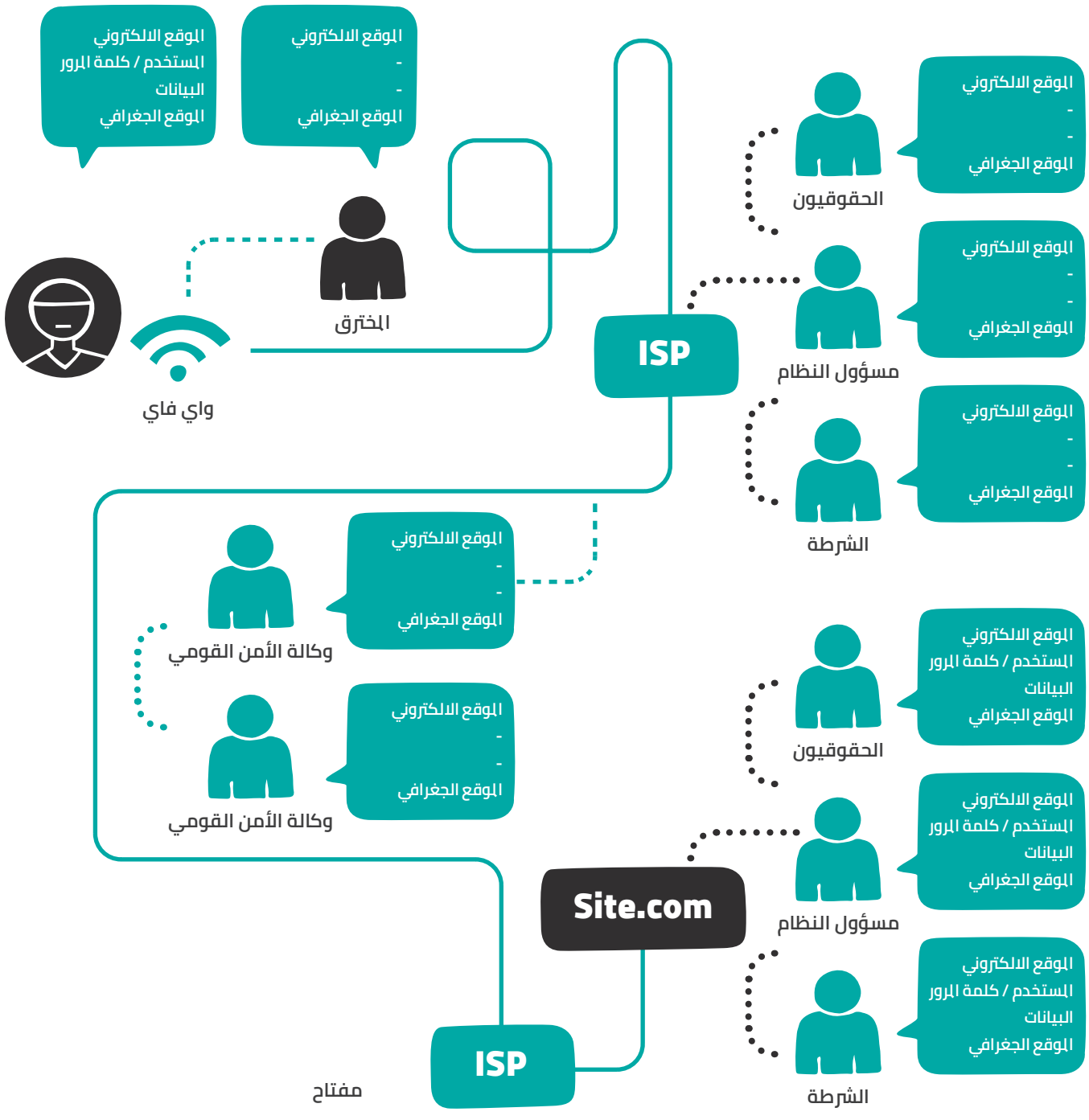
ويعتبر متصفّح (Tor Browser) المتصفّح الأفضل من ناحية الحفاظ على خصوصية المستخدم وتعطيل عمل المتتبِعات. المتصفّح من منتجات شركة (Tor) المتخصصة في مجال برامج تشفير اتصال المستخدم، والمُصنّفة من قبل وكالة الأمن القومي (NSA) على أنها إحدى أفضل شركات تشفير البيانات في العالم. المتصفّح مبنيٌّ على نسخةٍ من «فايرفوكس» ويتوفر لأنظمة «ويندوز» و«ماك» و«لينكس».
كما تمكن الاستعانة بمتصفّح (Epic Privacy Browser)، الذي يقوم بحجب جميع «السكربتات» (النصوص؟) البرمجية التي تتّبع نشاطاتنا. يحتوي هذا المتصفّح على إضافات حماية مثل المتصفّحات الأخرى تُمَكِّن من حجب الإعلانات غير المرغوب بها. ما يميّز هذا المتصفّح أنه حتى مطوِّروه فعلياً لا يجمعون المعلومات عنا.

العنوان: المتصفحات
الهدف: يفهم الطالب الفرق بين المتصفحات المختلفة
يفهم الطالب كيف تتعقب المتصفحات تحركاته.
يقوم الطلبة بحماية متصفحاتهم من المتتبعات.

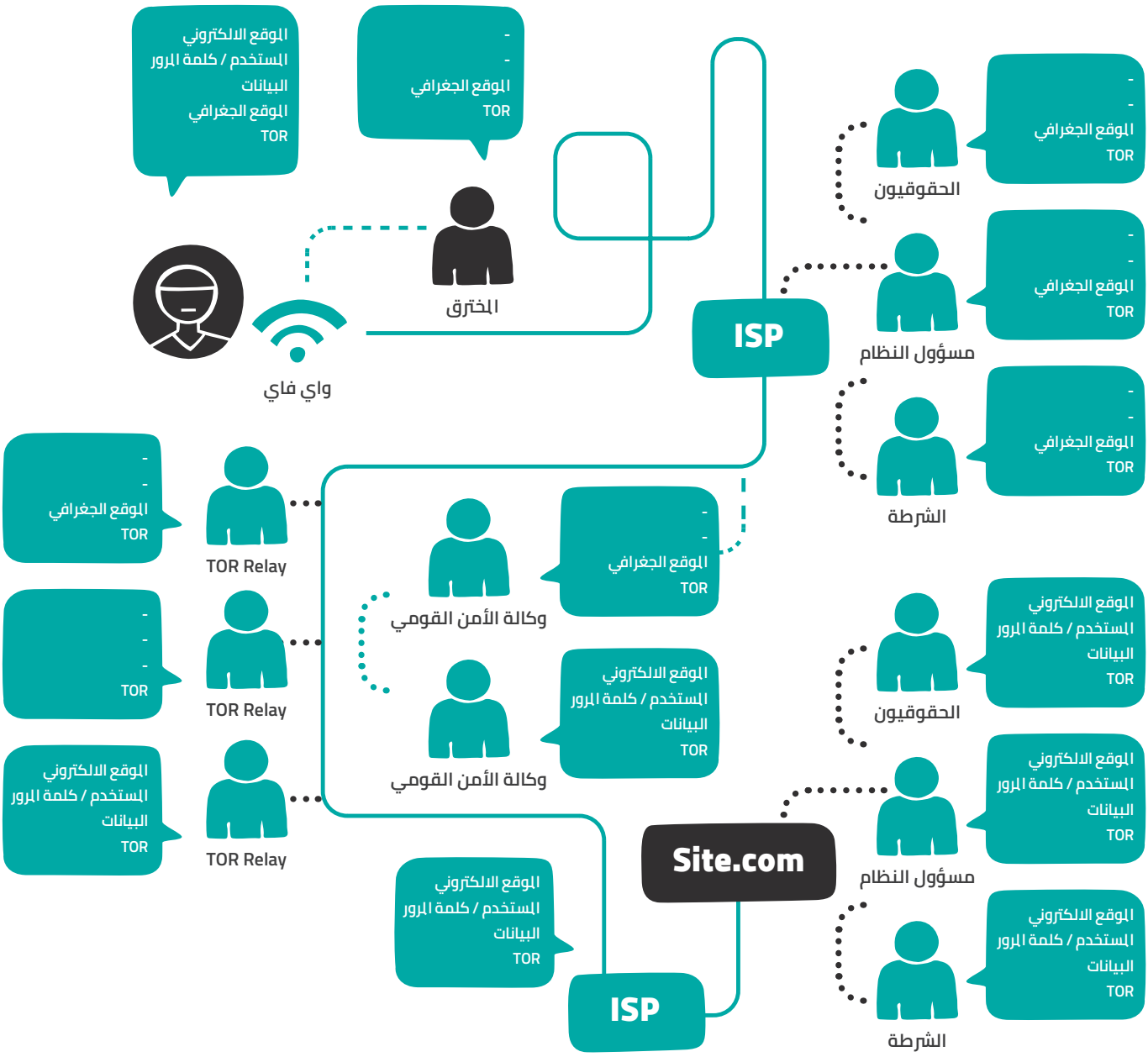
الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يسأل المدرب الطلبة ما هي أنواع المتصفحات التي يستخدمونها ثم يقوم بتسجيلها على اللوح. يسألهم المدرب إن كانوا يستطيعون تصنيف هذه المتصفحات، بدءاً بالأفضل نحو الأسوأ، وأن يشرحوا السبب . يؤكد المدرب أن لكل متصفح حسنات وسلبيات أهمها موضوع اختلاف السرعة. (يراجع المدرب المواد في فصل المتصفحات قبل الورشة).	يتفكر الطلبة بأنواع المتصفحات المختلفة	نقاش		يمكن للمدرب أن يذكر أن متصفح «كروم» مثلاً هو متصفح تابع لشركة جوجل، بالتالي البيانات التي يستخدمها الشخص في هذا المتصفح أو المواد التي يبحث عنها تُحفظ في خوادم (سيرفرات) جوجل.
١٠ د.	يقوم المدرب بفتح lightbeam على المتصفح ويقوم بالدخول على مواقع مختلفة من نفس المتصفح ويراقب المدرب والطلبة عدد المتتبعات على المتصفح يشير المدرب للمتتبعات المترابطة التي ترتبط بعدة مواقع مختلفة	يرى الطلبة كيف تتعقب المتصفحات تحركاتهم	عرض	حاسوب متنقل + اتصال بشبكة الإنترنت + آلة عرض ضوئي.	يتأكد المدرب من وجود انترنت و بروجيكتور قبل الورشة + هواتف نقالة مع الطلبة.
١٠ د.	يعرض المدرب على الطلبة موقع panopticlick ثم يطلب منهم أن يفتحوا موقع panopticlick على المتصفحات التي يستخدمونها من الهواتف النقالة، يقوم هذا الموقع بفحص إن كان هذا المتصفح آمناً من الإعلانات والمتتبعين غير المرئيين وبصمات المتصفح	يفحص الطلبة إن كانت المتصفحات التي يستخدمونها آمنة من المتتبعات	تمرين	هواتف نقالة	يتأكد المدرب من وجود انترنت و بروجيكتور قبل الورشة + هواتف نقالة مع الطللبة.
١٥ د.	يُحمّل المدرب أداة Privacy Badger وأداة Ghostery ويعرضها على آلة العرض الضوئي (بروجكتر) أمام الطلبة، ليقوموا بتحميلها على متصفحاتهم. يحرص المدرب على أن يتأكد أن كل الطلبة استطاعوا تحميل تلك الأدوات على متصفحاتهم.	يقوم الطلبة بحماية متصفحاتهم من المتتبعات.	تمرين +عرض		يتأكد المدرب من وجود اتصال مع شبكة الإنترنت، وآلة عرض ضوئي (بروجكتر)، وهواتف ذكية مع الطلبة.

المتصفّحات


الموقع الالكتروني
المستخدم / كلمة المرور
البيانات
الموقع الجغرافي
الحقوقيون
مسؤول النظام
الشرطة
ISP
المخترق
واي فاي
وكالة الأمن القومي
Site.com
مفتاح
اتصال الانترنت
تنصت
تبادل بيانات


الموقع الالكتروني
المستخدم / كلمة المرور
البيانات
الموقع الجغرافي
الموقع الالكتروني
-
-
الموقع الجغرافي
المخترق
واي فاي
ISP
الحقوقيون
مسؤول النظام
الشرطة
وكالة الأمن القومي
Site.com
ISP
مفتاح
اتصال الانترنت
تنصت
تبادل بيانات

المتصفّحات



مفتاح

اتصال الانترنت

تنصت

تبادل بيانات

العنوان :- المتصفحات
الهدف :- يفهم الطلبة أنواع البروتوكولات المختلفة
يفهم الطالب كيف يعمل متصفح TOR

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يطلب المدرب من الطالب أن يتطوع للخروج خارج الغرفة. تجلس المجموعة بشكل دائري وتقوم باختيار «ملك الحركات»، بحيث تكون مهمته القيام بحركات معينة من فترة لأخرى، وعلى باقي الطلبة تقليده. على المتطوع خارج الغرفة كشف من هو ملك الحركات.	تحفيز الطلبة	لعبة		
١٥ د.	يسأل المدرب الطلبة عن الـ HTTP, HTTPS ومن ثم يسألهم عن متصفح «تور». يشرح المدرب خصائص متصفح «تور»، وبروتوكولات الـ HTTP, HTTPS	يفهم الطلبة الفرق بين البروتوكولات المختلفة وكيفية عمل TOR	نقاش + محاضرة من المدرب		على المدرب مراجعة المادة في فصل الإنترنت حول البرتوكولات ومتصفح TOR
٢٠ د.	يُقسّم المدرب الطلبة إلى ٣ مجموعات، يوّزع على المجموعات أوراق العمل، ثم يطلب منهم ذكر أي من الرسومات الموجودة في أوراق العمل تعبر عن TOR , http, https ، ثم يقومون بعرض النتائج مع الشرح.	يفهم الطلبة الفرق بين البروتوكولات المختلفة وكيفية عمل متصفح «تور».	تمرين + مجموعات عمل	أوراق عمل	يطبع المدرب أوراق العمل قبل بدء الفعالية.

شبكات التواصل الاجتماعي

تمتاز شبكات التواصل الاجتماعي في أن المستخدم نفسه هو من يصنع المحتوى الخاص به، والذي يتألف مما يضيفه ويشاركه مع الآخرين؛ فمالكو الموقع أو مطوّروه لا يمكنهم إضافة محتوى إلا بصفتهم مستخدمين. وقد تكون مشاركة المستخدم في صنع المحتوى عبارة عن مشاركة نصيّة كما في العديد من شبكات التواصل الاجتماعي، أو صوتية كـ«الساوند كلاود»، أو فيديو كـ«اليوتيوب»، أو صور كـ«فليكر»، أو مزيج بينها كـ «الفيسبوك».

كما تمتاز وسائل التواصل الاجتماعي بتوفر صفحات تمثل الفرد أو المؤسسة داخل الشبكة الاجتماعية، فكل مستخدم يجب أن يكون له صفحة شخصية تمثله، يعتمد عليها عند بناء العلاقات داخل الشبكة ويملؤها بالمحتوى الخاص به.

تعتمد العلاقات في وسائل التواصل الاجتماعي على الصفحات وليست علاقات شخصية، فالصفحة تعبر عن الشخصية الحقيقية بمحتواها واهتماماتها وقد تكون بعيدة كل البعد عن ذلك؛ فالعلاقات في وسائل التواصل الاجتماعي قد تكون من طرف واحد، بمعنى أن تتاح محتويات صفحة ما كمنشورات الطرف الأول في صفحة الطرف الثاني كخاصية المتابعة على «تويتر» أو «فيسبوك»، وقد تكون العلاقة تبادلية بمعنى أن تتاح محتويات الصفحات لكلا المستخدمين، كخاصية الصداقة على «الفيسبوك».

تتميّز وسائل التواصل الاجتماعي بالحيوية، ففيما تظهر لك منشورات معينة كونها من طرف أصدقاء، ستظهر منشورات أخرى كونها من أصدقاء مختلفين لصديقك، هذه المرونة تعتمد في الغالب على العلاقات بين المستخدمين لأن المحتوى يتشكل من خلال منشورات الأصدقاء والصفحات التي يتابعها المستخدم.

خصائص شبكات التواصل الاجتماعي:

- المستخدمون هم من يملكون حرية صناعة المحتوى.
- الصفحات شخصية (Profiles).
- العلاقات مباشرة بين المستخدمين.
- المحتوى متغير حسب المستخدم.

ما هو دور شبكات التواصل الاجتماعي في حياتك؟

اجتمعت عائلة أحمد وخرجت لقضاء وقت ممتع في البحر الميت، صوّر أحمد العائلة وقام بنشر الصورة على شبكة «الفيسبوك» وكتب على الصورة أن كل العائلة تقضي وقتاً ممتعاً معاً، وضَبَطَ الإعدادات كمنشورٍ عامٍ، أي يراه الجميع. ما خطورة هذا المنشور على عائلة أحمد؟

تطبيقات الفيسبوك

تطبيقات «فيسبوك» هي تلك التطبيقات التي يرتبط تشغيلها بتطبيق الفيسبوك، وتعمل فقط في بيئة حسابنا على الـ«فيسبوك»، كالألعاب أو التطبيقات التي تقدّم خدمات معينة كتلك التي تخبرك من قام بزيارة حسابك مثلاً.

أصبحت تطبيقات «فيسبوك» في الفترة الأخيرة من أخطر طرق الاختراق، فمنها ما يكون مثيراً للفضول فتقوم بالسماح والإذن له فيتحكم بدوره في حسابك، كأن ينشر على صفحتك أو يرسل رسائل لأصدقائك أو ينشر منشورات على المجموعات التي تشترك فيها بإذنك وغالباً من دون إذنك.

تمتاز بعض هذه التطبيقات بالذكاء نوعاً ما، فمن الممكن أن يكون هذا التطبيق من أجل هدفٍ سامٍ ونبيلٍ، كأن يتولى التطبيق نشر أحاديث نبوية أو مقولات ثقافية، ولكن مظهرها العام لا يبطل محتواها غير الخلّاق؛ حيث تقوم بالتجسس عليك دون أن تدري ودون أن تزعجك. ولا حاجة لي عزيزي القارئ أن أذكرك بما يحتويه حسابك على «الفيسبوك» من معلومات كتاريخ ميلادك أو صورك أو المنشورات على صفحتك أو رسائلك مع أقاربك وأصدقائك...إلخ.

لكي تُفرق بين التطبيقات الخبيثة والأخرى الجيدة، يكفي أن تقوم بالدخول لهذه الأداة وتحميلها والسماح لها بالشروع في العمل (http://mypermissions.com)، ستظهر لك هذه الأداة جميع التطبيقات والأذونات الخاصة في كل تطبيق وما المعلومات التي يستطيع كل تطبيق الولوج إليها.

بإمكانك عزيزي القارئ التحكم في هذه التطبيقات وتعديلها وترويضها كي تعمل حسب ما تريد، فيكفي أن تضغط على كلمة تعديل في اللون الأزرق المقابل للتطبيق الذي تريد ليظهر بوضوح التطبيق والمعلومات التي سَمحتَ له بالوصول إليها.

شبكات التواصل الاجتماعي

الإعلانات

تعتبر مواقع التواصل الاجتماعي من أكثر الطرق نجاعة في بث الأخبار ونشر المعلومات، وقد أصبحتْ الاختيار الأفضل والأنجع للشركات التجارية والمؤسسات الاجتماعية والكثير من الأفراد ورجال الأعمال لتحسين وترقية عملها بغض النظر عن مجاله. ويعود سبب هذا النجاح بشكل رئيس إلى الانتشار الواسع لمواقع التواصل الاجتماعي، فخلال دقيقة واحدة من الزمن أصبح بإمكانها نشر إعلان يحتوى على أية معلومات، وبالتالي أصبحت عملية الإعلان سريعة وفعالة وناجحة جداً لتسويق المنتجات أو المعلومات.

بالمقابل تزيد نسبة استخدام مواقع التواصل الاجتماعي وجذب واستقطاب المستخدمين الجدد، مما يعني زيادة أعداد من يندرجون ضمن جمهور الهدف لتلك الإعلانات. في هذه العملية يستفيد المستخدم (المُعلن) وتستفيد الشركة المالكة للموقع، وبذلك أصبحت هذه الإعلانات البناء الأساسي الذي تعتمد عليه جميع مواقع التواصل الاجتماعي لتبقى فعالةً وناجحةً ومنتشرةً بطرق ترضي المستخدم وتزيد من رغبة استخدامها وتترك مردوداً مالياً لمواقع التواصل الاجتماعي من الشركات التي تقوم بعرض إعلاناتها.

فمثلاً، موقع الفيسبوك يتيح للمستخدمين خدمة الترويج والإعلان عن منتج معين مقابل مبلغ مالي معين، فيستفيد المستخدم بتسويق منتجه أمام فئة واسعة من الناس، وعلى مسافات بعيدة، فيصل جمهوراً ربما لم يكن ليصله بدون الفيسبوك.

الحيادية

مواقع التواصل الاجتماعي هي من أكثر المواقع استخداماً خلال الفترة الأخيرة، حيث ارتبطت ارتباطاً كلياً بجميع مناحي الحياة، فأصبحت الطريقة الأولى للتعبير ونشر الأفكار والتواصل الاجتماعي وربط العلاقات بين الأفراد بغض النظر عن المسافة أو المكان، ونجحت في جذب كميات هائلة جداً من المعلومات، وتحديداً بين أفراد المجتمعات غير المستقرة سياسياً، حيث تمكنت هذه المواقع من الحصول على كامل الصلاحيات لفعل ما يتناسب مع قوانينها أو قوانين من يديرها، فتتحكم بجميع الصفحات والحسابات لمستخدميها وتشدد الرقابة عليهم، وتقتحم حياتهم الخاصة.

ولطالما كانت مراقبة الفلسطينيين جزءاً لا يتجزأ من مشروع إسرائيل الاستعماري، وعلاوة على ذلك، أعلنت وزيرة العدل الإسرائيلية ووزير الأمن العام جلعاد إردان في ٢٠١٦ إبرام اتفاق بين إسرائيل وفيسبوك ينص على تشكيل فرقٍ لرصد المحتوى «التحريضي» وإزالته. وإزالة أي صفحة أو موقع أو حساب فلسطيني ينظر إلى القضيةِ الفلسطينية بطريقة صحيحة أو ينبض باسم الحرية والشعب الفلسطيني، فأصبح الاحتلال يتجاوز كل القوانين العالمية والدولية. أصبح الصراع الفلسطيني الإسرائيلي أكثر تطوراً ليصل إلى أفكار الفلسطيني ويحاربه إلكترونياً بكل الطرق.

العنوان - مواقع التواصل الاجتماعي - فيسبوك نموذجاً.
الهدف - أن يتفكر الطالب ما هي البيانات التي يشاركها في فيسبوك.
أن يتفكر الطالب في الجانب التجاري في وسائل التواصل الاجتماعي.

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يبدأ المدرب الورشة بتمرين إحماء. يُقسّم المدرب الطلبة لمجموعتين متساويتين من حيث العدد. تجلس المجموعة (أ) على كراسي ويقف خلف كل طالب في مجموعة (أ) طالب من المجموعة (ب). يحمل كل طالب في مجموعة (أ) قلماً وورقة ويكتب حرفاً، ويمرر الورقة للشخص الذي بجانبه، على الطلبة في مجموعة (أ) تكوين جمل مفيدة على كل ورقة من ترتيب الأحرف، ويكون على الطلبة في مجموعة (ب) أن يُخمنوا أكبر عدد ممكن من تلك الكلمات.	تنشيط للطلبة	تمرين	أوراق وأقلام	
٢٠ د.	يقسم المدرب المجموعة لمجموعات صغيرة: بحيث يكون طالبان أو ثلاثة في كل مجموعة. يطلب المدرب منهم كتابة نوعية المعلومات التي يشاركونها على موقع فيسبوك (صور شخصية، آراء سياسية، أماكن تواجدهم، بياناتهم،..) على ورقة، ثم يقومون بعرض النتائج أمام الجميع ومناقشتها مع المجموعة. على المدرب إدخال المستوى التحليلي للنقاش فيسال الطلبة: ماذا تعني هذه المعلومات؟ إلامَ تؤدي؟ ما هي التبعات لمشاركتنا مثل هذه التفاصيل (التطرق للجانب الإيجابي والسلبي).	يتفكر الطلبة بماهية المعلومات التي يشاركونها في فيسبوك	مجموعات عمل،نقاش، محاضرة (شرح)	أوراق وأقلام	
١٠ د.	يعرض المدرب فيديو «تعلقش بالشبكة»، https://www.youtube.com/watch?v=yfnaLh_iOJs يسأل المدرب الطلبة عن فهمهم للفيديو ويفتح باب النقاش حول محتواه والعبرة منه. ومن ثم يشرح للطلبة كيف تستغل شركة فيسبوك ما نشاركه عبر موقعها من معلومات وبيانات.	التواصل واستغلالها لبياناتهم		متنقل + آلة عرض ضوئي (بروجكتر).	التأكد من نوعية الإنترنت أو عدم توفره أثناء الحصة.

شبكات التواصل الاجتماعي

العنوان - أخلاقيات استخدام فيسبوك
الهدف :- يتفكر الطلبة بطبيعة مشاركاتهم في موقع فيسبوك
يفهم الطلبة أهمية وجود قواعد يلتزمون بها في تعاملهم مع فيسبوك
ينتج الطلبة دستورا أو قائمة السلوك في فيسبوك.

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	- يجلس الطلبة بشكل دائري، يطرح المدرب أسئلة لها علاقة بـ«الفيسبوك» قد تنطبق أو لا تنطبق على الطلبة. مثلاً: هل سبق لك أن نشرت صورةً مضحكةً لنفسك على «الفيسبوك»؟ هل سبق لك أن قبلت طلب صداقة من شخص لا تعرفه؟ هل تشارك منشوراتك مع كل أصدقائك في «الفيسبوك»؟ الشخص الذي تنطبق عليه الإجابة بنعم يقفز في الهواء أو يصفق، ثم يختار المدرب أحدهم للوقوف في الوسط وطرح سؤال جديد. - يناقش الطلبة طبيعة استخدامهم للفيسبوك ولأي غرض (تعارف، أخبار، مشاركة حياتهم اليومية) - يُسجّل المدرب كل ذلك.	- تنشيط الطلبة وتحفيزهم للمشاركة في الحصة. - يتفكر الطلبة في كيفية استخدامهم لتطبيق «الفيسبوك».	لعبة	لوح وقلم	
١٠ د.	-يُقسّم المدرب الطلبة إلى فريقين (أو حسب العدد إلى ثلاث فرق). الهدف: اختبار المعلومات الموجودة لدى الطلبة عن «الفيسبوك»، كيفية استخدام «الفيسبوك» بشكل آمن. الهدف من النشاط تقديم معلومات جديدة وتحفيز المناقشة. بعض الأفكار لأسئلة محتملة على طريقة «صحيح أم خاطئ»: -الإنترنت، بما في ذلك «الفيسبوك»، فضاءٌ مفتوحٌ لا يتبع قوانين معينة. كل شيءٍ مسموحٌ. -ليست هناك مشكلة من إطلاق بعض الشتائم في «فيسبوك»، فهناك تقريباً ٢ مليار مستخدمٍ حول العالم. كلماتي لن تؤثر على أحد. -من الممكن أن أربط حسابات أصدقائي بمنشوراتي (tag making) دون موافقتهم. - ممنوع أن أنشر صوراً محرجةً لأصدقائي فقط، أما الصور الجميلة فمسموح أن أنشرها على صفحتي في «فيسبوك» دون أخذ موافقتهم. يلخص المدرب للطلبة معنى المبادئ الأخلاقية والخطوط الحمراء التي يجب اتباعها أثناء استخدامهم «للفيسبوك»، وذلك خلال نقاش مفتوح.	يستوعب الطلبة في مخاطر «فيسبوك» ويدركون أخلاقيات استخدامه.	مسابقة نقاش		من الممكن إضافة أسئلة أخرى

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
٢٥ د.	- يُلخص المدرب ما توصل إليه الطلبة من مبادئ وجمعها كلها على ورقة واحدة. - تتم مناقشة كل مبدأ على حدة والتأكد من أن جميع الطلبة يوافقون عليه. (من الممكن أن يقوم الطلبة بالإمضاء على هذه الورقة على أنها وثيقة مبادئ متفق عليها - حسب الفئة العمرية) اقتراح: إنتاج «بوستر» يتضمن بنود «الدستور»، بتصميم جذاب، تعليقه في مكان مناسب داخل المدرسة و/أو نشره عبر الانترنت. من الممكن أن يتضمن «البوستر» على شقين: افعل ولا تفعل	بناء «دستور أخلاقي» لاستخدام الطلبة للفيسبوك	نقاش وتمرين عملي	ورقة كبيرة وأقلام	

العنوان - الأمان في مواقع التواصل الاجتماعي - فيسبوك نموذجاً
الهدف - أن يفهم الطلبة أهمية إعدادات الأمان
أن يعرف الطلبة ما هي الخطوات التي تجعلهم أكثر اتباعاً لمعايير الأمن الرقمي.
أن يكتسب الطلبة مهارة تطبيق إعدادت الأمان في حساباتهم في فيسبوك

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
٥ د.	- يبدأ المدرب الورشة بتمرين الظل يسأل الطلبة: - أضعُ صورتي الشخصية على «فيسبوك» لأنني أحب أن يعرفني الناس. - أشارك كل تفاصيلي الشخصية الحقيقية على «الفيسبوك». - مشاركة أفكاري وآرائي على «الفيسبوك» أمر مهم بالنسبة لي. - يُقسّم المدرب الطلبة لمجموعات صغيرة (٢-٣ طلبة لكل مجموعة) - يطلب المدرب من الطلبة القيام بكتابة المعلومات التي يشاركونها على مواقع التواصل الاجتماعي (صور شخصية، آراء سياسية، أماكن تواجدهم، بياناتهم..) على ورقة العمل المرفقة. - يقوم الطلبة بعرض النتائج أمام الجميع ومناقشتها بشكل جماعي. - على المدرب إدخال المستوى التحليلي للنقاش فيسأل الطلبة: ماذا تعني هذه المعلومات؟ إلى ماذا تؤدي؟ ما هي التبعات هل هي إيجابية أم سلبية؟ - يشرح المدرب البيانات التي نشاركها وكيف يتم استغلالها.	تنشيط الطلبة، وتفكرهم بالمعلومات التي يقومون بمشاركتها على مواقع التواصل	تمرين حركة		

شبكات التواصل الاجتماعي

الوقت	المحتوى	هدف التعلم	الطريقة	الأدوات اللازمة	الملاحظات
١٠ د.	يعرض المدرب على الطلبة هذا الفيديو https://www.youtube.com/watch?v=tavKNwLKqOI بعنوان - شركات بيع البيانات الشخصية (مدته ٢:١٦) ثم يفتح النقاش مع الطلبة: ما هو أكثر ما أدهشهم في الفيديو من معلومات؟ ماذا نفهم من هذا الفيديو ؟ يشرح المدرب الغرض من جمع هذه البيانات وبيعها .	يعرف الطلبة حجم استغلال بياناتهم من قبل الشركات	فيديو ونقاش محاضرة/ شرح	اتصال بشبكة الإنترنت + حاسوب متنقل + آلة عرض ضوئي (بروجكتر)	التأكد من توفر متطلبات العرض قبل الورشة وفحص الصوت مسبقاً. من الممكن تحميل الفيديو قبل الورشة في حال عدم وجود إنترنت.
٥ د.	يسأل المدرب الطلبة هل هناك أهداف أخرى يتم لسببها جمع بياناتنا (غير الأسباب التجارية)، ثم يفتح المدرب النقاش حول قصص لأشخاص تم توقيفهم أو اعتقالهم بسبب منشورات.	يفهم الطلبة ما هي أهمية البيانات والتفاصيل التي يشاركونها	شرح نقاش		
٢٥ د.	يسأل المدرب: ما هي الخطوات التي يتبعونها لكي يكونوا أكثر أمناً أثناء استخدامهم للفيسبوك؟ ثم يقوم بكتابة ما ذكر على اللوح ويقوم بشرح هذه الإعدادات بشكل تقني. يحرص المدرب على أن يتبع الطلبة الخطوات التي يتبعها هو بواسطة عرض إعدادات الأمان على الفيسبوك في آلة العرض الضوئي (البروجكتر)، ويطبقونها في نفس الوقت على هواتفهم الذكية. *هذه الإعدادات متشابهة لكثير من وسائل التواصل الاجتماعي مثل واتساب انستجرام فيسبوك. يمكن للطلبة أيضا أن يقوموا بنفس الإعدادات في حساباتهم الأخرى على هذه التطبيقات *يستطيع المدرب سؤال الطالب الذي يقترح إحدى هذه الإعدادات أولاً عن كيفية عملها، من ثم يقوم هو بتوضيح الأمر بواسطة عرضه من خلال الفيسبوك على الشاشة (بشكل عملي).	أن يعرف الطلبة ما هي الخطوات التي تجعلهم أكثر أمناً، أن يكتسب الطلبة مهارة تطبيق إعدادات الأمان	عرض على الشاشة.	حاسوب متنقل + آلة عرض ضوئي (بروجكتر) + حساب فيسبوك فعّال.	- يتأكد المدرب أنه قام بتغطية كل الإعدادات المرفقة في المادة الإثرائية المرفقة حتى وإن لم تذكر من قبل الطلبة. - يمكن الاستغناء عن البروجيكتر وتوزيع ورقة العمل

وظيفة بيتية – اختبر نفسك

وسائل التواصل الاجتماعي – الفيسبوك نموذجاً

لكي يختبر الطلبة الجانب التجاري لوسائل التواصل الاجتماعي يُطلب منهم أن يتحدثوا بشكل مكثف عن موضوع لا يشغلهم عموماً مثل (البرازيل، القطط، الاسمنت ...) لمدة يومين، وذلك من دون الحاجة لكتابة منشور عبر وسائل التواصل عن ذلك، فقط عليهم التحدث عن هذا الموضوع من خلال المراسلات والحديث عبر الهاتف أو عندما تكون هواتفهم إلى جانبهم.

مادة اثرائية للمدرب
إعدادات الأمان وإجراء خطوات لإعدادات أكثر أمناً.

الهدف - توضيح طريقة إعدادات الأمان على مواقع التواصل الاجتماعي (فيسبوك نموذجا).
على المدرب التوجه الى تطبيق «الفيسبوك»

١. الدخول على «إعدادات الحساب من القائمة».
٢. اختيار «الأمان وتسجيل الدخول».

يقوم هنا المدرب بالمرور على كل القائمة واحداً تلو الآخر وإظهار كيفية الدخول لكل إعداد وتطبيق الإجراءات الأكثر أمناً.

اسم الإعداد	ماذا يحتوي هذا الإعداد؟	الخيار الأكثر أمناً
المكان الذي سجلت دخولك منه	الأجهزة التي سجل المستخدم من خلالها الدخول على حسابه على «الفيسبوك».	تسجيل الخروج من جميع الأجهزة التي لم يعد يستخدمها صاحب الحساب.
إعدادات طبقة أمان إضافية - تلقي تنبيهات بشأن تسجيلات دخول غير معروفة	يخبرك الإعداد إذا قام أي شخص بتسجيل الدخول من جهازٍ أو متصفحٍ لا تستخدمه أنت عادةً.	تشغيل الخاصية
إعدادات طبقة أمان إضافية - استخدام مصادقة ثنائية	يقوم الإعداد بإرسال رسالة نصية تحتوي رمزاً إلى رقم هاتفك في كل مرة تسجل الدخول إلى حسابك من جهاز أو متصفحٍ جديدٍ، وبذلك لا تتمكن من تسجيل الدخول من جهازٍ/متصفحٍ جديدٍ بدون إدخال هذا الرمز.	تشغيل الخاصية (يجب تفعيل رقم الهاتف وربطه بالحساب)
إعدادات طبقة أمان إضافية - اختيار أصدقاء للاتصال بهم إذا تم قفل حسابك.		

مفاهيم وتعريفات

الإنترنت: مثل عالم البحار والمحيطات.. يتكون من آلاف الجزر (شبكات) الموزعة حول العالم تربطها العديد من الكابلات والأجهزة تحدد المسارات وتيسر مرور البضائع وتقديم الخدمات من نقطة أ إلى نقطة ب، ويتكون الإنترنت مثل الحال في عالم البحار من طبقات عديدة (لغات برمجية وبروتوكولات) منها طبقات على السطح ويليها طبقات أعمق وصولا إلى القاع تقوم بأدوار مختلفة ومتجانسة لعمل الإنترنت. ويتواصل سكان الجزر عبر مراكب صغيرة وكبيرة (مثل الحواسيب و المتصفحات والهواتف) للوصول من نقطة أ إلى نقطة ب لتبادل المعلومات والنفاذ للمحتوى والدردشة وإلى آخره من أنشطة مختلفة تحدث على الإنترنت. وبطبيعة الحال تختلف موازين القوى في عالم الإنترنت من مقدم الخدمة (شركات) إلى المشرف على الخدمات (سلطات وجهات رسمية) والمواطنين. والأنشطة البحرية التي تتم منها ما هو متاح للجميع للاطلاع ومنها ما هو خاص كما يمكن تبادل البضائع على نحو علني وعلى نحو خاص.

الشبكات الاجتماعية والبريد الإلكتروني: هي عبارة مراكب ضخمة (شركات) تمتلك موارد مهولة لتقديم خدماتها للمواطنين في مقابل مبالغ مالية أو بيانات شخصية، وجميع استخدامات المواطنين لخدمات الشركات تدور في فلك موارد الشركة حيث تقوم الشركة بتحديد القواعد والقوانين ويلتزم المواطن ويمكن للشركة معرفة ما يقوم به المواطن والتحكم في بياناته ولها سيطرة مطلقة. أغلب الشركات تفرض على مواردها وآلية عمل خدماتها سرية بحيث لا يمكن للمواطنين التيقن من ادعاءات الشركات او التحقق من سلامة الخدمة، وعلى الجانب الأخر تقوم بعض الشركات بتبني فلسفة البرمجيات الحرة ومفتوحة المصدر لمشاركة كيفية عمل موارد وتمنح الاخرين حقوق للمراجعة وإعادة الاستخدام والاشتقاق والتطوير على نحو تشاركي. ولكي يقوم المواطن باستخدام إحدى تلك الخدمات يقوم بملء استمارة تحتوي على بيانات شخصية عديدة ويقوم المواطن بالتأشير على زر «أوافق» على سياسات الاستخدام والخصوصية - وفي الغالب دون قراءتها.

نظام التشغيل Operating System: هو واحد من أهمّ أنواع البرمجيّات التي لا يمكن الاستغناء عنها عند استعمال الحاسوب، إذ يعتبر وسيلة الإنسان لاستعمال قطع الحاسوب الصلبة، والاستفادة من إمكانياته إلى أقصى حدّ ممكن، ومتاح. فهو عبارة عن البيئة التي تعمل بها البرمجيات عموماً، فهي بمثابة الأرض التي تزرع بها المحاصيل .فالحاسوب عبارة عن عتاد وبرامج، ولا يوجد أي اتصال ما بين هذين الفرعين إلا من خلال نظام التشغيل. فنظام التشغيل عبارة عن مجموعة من البرامج التي تقوم بالتنسيق بين عمل وحدات الحاسوب المختلفة وادارة عمل كل منها فيما يتعلق بالبيانات والمعلومات يمكن نظام التشغيل التحكم والسيطرة بالمصادر والمهام وإدارتهما، مثل التحكم بإدارة الذاكرة الرئيسية. فهو وسيلة تفاهم وحلقة وصل بين المستخدم والجهاز بواسطة واجهة مستخدم (User interface)، والتي تمنح المستخدم من تشغيل البرامج. إدارة تدفق البيانات ومسارها من خلال التحكم بانتقالها بين وحدات الحاسوب. تنظيم الملفات في مجلدات وفهرستها. ومن الأمثلة على أنظمة التشغيل أنظمة ونـدوز Windows، لينكس Linux، ماكنتوش Macintosh، أندرويد Android آي أو أس IOS وغيرها

الهواتف الذكية: الهواتف الذكية تتشكل من مكونات عديدة من ضمنها مساحة تخزين داخلية، والتي يتم عليها وضع نظام التشغيل للهاتف والتطبيقات التي يقوم المستخدم بتنزيلها وجميع استخدامات مخزنة على تلك المساحة مثل الصور ومقاطع الفيديو والبريد الإلكتروني، وفي بعض الأحيان يمكن للمستخدم إضافة مساحة تخزين خارجية لتخزين مواده مختلفة. توجد مناحي مختلفة لتأمين الهواتف سواء تأمين المحتوى أو تأمين الاتصالات وهكذا. وفي هذا الفيديو سنتحدث فقط عن تأمين المحتوى من مخاطر مثل السرقة أو فقدان الهاتف في مكان ما. الأمر البديهي أنه في حالة فقدان الهاتف فإن الشخص الذي حصل عليه يستطيع النفاذ لكل المحتوى الشخصي على الهاتف، وهو في الغالب يكون محتوى خاص جدا سواء أسري أو حميمي من محادثات وصور وإلى أخرة مما يشكل تهديد للخصوصية ويتفح الباب للابتزاز المالي على سبيل المثال. لا ينتبه الكثير من المستخدمين لخطوات بسيطة يمكن اتخاذها لحماية المحتوى من أي مشكلات قد تحدث مثل السرقة. فنجد الكثير من المستخدمين لا يقومون بتفعيل قفل الشاشة، وهذا يعني أن أي شخص بمجرد الحصول على الهاتف يستطيع النفاذ إلى أي محتوى، أو يقوم المستخدم بتفعيل قفل شاشة ضعيف وغير آمن بالمرة مثل أن يستخدم رمز لقفل الشاشة عبارة عن أرقام متسلسلة ١٢٣٤٥ مثلا. وكثير ما يبدأ المستخدمين في التساؤل عن مدى وجود اختيار لحذف محتوى الهاتف عن بعد في حال سرقته أو فقدان. وهذه مسألة ممكن ولكنها تحتاج إلى إعداد وتحضير مسبق حتى يمكن استخدامه وقت الضرورة. بعد الهواتف تعتمد على أنظمة تشغيل توفر قدر من الحماية أفضل من أنظمة أخرى. وبشكل عام تعتبر أجهز أبل وأندرويد أفضل من هواتف ويندوز.

البروتوكول Protocol: كما في شؤون السياسة والدولة كان البروتوكول عبارة عن قواعد التي توجه الكيفية التي يجب أن يؤدى بها تصرف أو نشاط معين عندما يقوم اثنين من البشر بإجراء مُحادثة، سيحتاجان إلى إستخدام نفس اللغة، ولكنهما يفهمان بعضهما البعض بدون الحاجة إلى العودة إلى القواعد الأساسية للغة الرسمية. على الجانب الآخر، فإن الحواسيب، يجب عليها أن تمتلك كل شيء مُعرف ومبني. إذا أرادت الحواسيب أن تتواصل مع بعضها البعض، يجب عليهم أن يعرفوا بطريقة مُتقدمة كيفية تبادل المعلومات وماهية الصيغة التي ستكون عليها. لذلك يتم إستخدام طرق أساسية لتبادل ومُعالجة الأنواع المُختلفة من المعلومات وسُميت بالبروتوكولات. فالبروتوكولات قد تم تأسيسها بواسطة إتفاقيات دولية للتأكد من إمكانية تواصل كل حاسب مع الآخر. يوجد العديد من البروتوكلات لمُختلف أنواع المعلومات والوظائف.

العنوان المنطقي IP Address: هو رقم فريد غير قابل للتكرار يتم تخصيصه للحاسوب بغرض تحديد المكان الذي توجه إليه الرسائل المنقولة عبر الإنترنت. عنوان بروتوكول الإنترنت يشبه رقم المنزل الذي توجه إليه الرسائل في البريد العادي. فيتم تعريف كل جهاز ضمن شبكة الحاسوب بشكل متميز عن طريق عنوان خاص به.

مفاهيم وتعريفات

أسماء المجال Domain Name: يملك كل خادم Server مرتبط بشبكة الإنترنت اسما معينا يقابل عنوان IP الخاص به. تعرف هذه الأسماء ب «أسماء المجال» Domain names والسبب وراء استخدامها يعود في معظمه إلى صعوبة تذكر واسترجاع الأرقام المكونة لعناوين IP من قبل المستخدمين البشر. على سبيل المثال نجد أنه من الأسهل على غالبيتنا تذكر العنوان www.facebook.com بدلا من العنوان الرقمي الخاص بهذا الموقع والممثل ب ٦٥,٥٤,١٥٢,١٢٦ وهكذا يمكن التحكم بإمكانية الوصول إلى خادم معين بالإعتماد على اسم الحقل المخصص له.

أمن المعلومات Information Security: يتضمن الإجراءات المتخذة لضمان وصول المعلومات للأشخاص المصرح لهم فقط وفقاً لصلاحياتهم سواءً إطلاعاً، تعديلاً أو حذفاً أو كلاهما، وذلك يتطلب إجراءات محددة وخبرةً ومهارات، ومعرفة بطرق حماية المعلومات. والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي الأشخاص غير المخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات. وأمن المعلومات قد حددت بالسرية Confidentiality ويعني بمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالأطلاع عليها أو الكشف عنها. والتكامل Integrity بمعنى الحفاظ على البيانات من التغيير أو التعديل من الأشخاص غير المخولين بالوصول اليها والتوافر Availability ويعني أن تكون المعلومات متوفرة عند الحاجة إليها. وأن تعمل عناصر النظام بشكل صحيح و مستمر فمهددات أمن المعلومات تتمثل في البرمجيات الخبيثة كالفايروسات ومصادرها وهجوم الحرمان من الخدمة Denial of Service Attacks ومهاجمه المعلومات المرسلة وتتمثل طرق الحماية في الاتصال بشبكة آمنة وتفعيل وضبط إعدادات جدار الحماية وتثبيت واستخدام برامج مضاد الفيروسات ومكافحة التجسس و.تحديث البرامج وأنظمة التشغيل.

جهاز الخادم (Server): وهو الجهاز الرئيسي والاساسي لعمل الشبكة، حيث تتصل به كل الاجهزة الأخرى، ويتصف جهاز الخادم بالكفاءة العالية من حيث مساحة الذاكرة الكبيرة، وكذلك المساحة التخزينية، حيث يتم تخزين عليه قاعدة البيانات الأساسية ومعلومات الاتصال بالشبكة ومعلومات أخرى تحتاج لهذه الكفاءة، ومن أهم المهام التي يقوم بها الخادم هي، التحكم في العمليات التي تتم عبر الشبكة، ومنح الصلاحيات المختلفة للأجهزة الأخرى وذلك باستخدام أنظمة وبرامج متخصصة.

خادم نطاق الأسماء DNS server: يقوم بتحويل أسماء المواقع لأرقام. على سبيل المثال نجد أنه من الأسهل على غالبيتنا تذكر العنوان www.facebook.com بدلا من العنوان الرقمي الخاص بهذا الموقع والممثل ب ٦٥,٥٤,١٥٢,١٢٦. فيتولى خادم نطاق الأسماء تحويل اسماء المجالات إلى عنوانها المنطقي IP التعمية: المصطلح الدارج تشفير... هي عبارة عن عمليات رياضية من خلال يتم تحويل المحتوى من شكله الواضح المقروء الصريح إلى صيغة معماة لا يمكن قراءته إلى بردها إلى صيغتها الأصلية أو فك تعميتها باستخدام كلمة سر أو مفتاح معين. وتطورت خوارزميات التعمية وأصبحت ممكن لتعمية أي محتوى من محتوى بريد إلكتروني ودردشات وصور ومحادثات فيديو. بعض مقدمي الخدمات يتبنوا التعمية والبعض الاخر لا يقوم بذلك، وبالتالي يوجد خدمات آمنة وخاصة وخدمات غير امنة لا توفر التعمية. وتساعد التعيمة بشكل عام المواطنين الحفاظ على خصوصية بياناتهم وأنشطتهم على الإنترنت وتجنب أي مشكلات ناتجة عن التعدي على حيواتهم الخاصة.

الجدار الناري Firewall: جزء من شبكة الحاسوب تم تصميمه للإيقاف أي اتصال غير مسموح له الدخول أو الخروج من شبكة الحاسوب أو الحاسوب نفسه، فهو يعمل على حماية شبكة الحاسوب من أي تدخل غير مرغوب قد ينتج عنه خرق للنظام الأمني المعتمد لدى أجهزة هذه الشبكة كإفساد بعض المعلومات المهمة وتغيرها والعبث بمحتوياتها. فقد يأتي الحائط الناري على هيئة أداة Hardware ترتبط بحد ذاتها مع شبكة الحاسوب أو على هيئة تطبيق برمجي Software يعمل على أحد الأجهزة والحواسيب التي تعمل داخل الشبكة وكما يمكن أن يأتي الحائط الناري على هيئة أداة وتطبيق في نفس الوقت وإن اختلف شكل الحائط الناري وطريقة عمله فإن وظيفته الأساسية تتمثل في كونه يشكل حداً مشتركا بين الشبكة الموثوقة والمراد حمايتها وتلك غير الموثوقة التي قد تمثل مصدرا للتهديدات. فيؤدي الحائط الناري وظيفته بالاعتماد على سياسات أمنية Security Policy خاصة تضم مجموعة مختارة من القواعد والقوانين Rules يتم وضع هذه القوانين من قبل مسؤول الشبكة المراد حمايتها حيث يتم السماح لاتصالات معينة ورفض اتصالات معينة من وإلى الشبكة الخاصة. فيمكن اتباع طريقتين عند وضع القوانين والقواعد الخاصة في اعداد وتشغيل الحوائط النارية الأمر الذي يسمح بوجود نوعين من الحوائط النارية: الحائط الناري الشامل Inclusive Firewall والحائط الناري الاستثنائي Exclusive Firewall ففي الحائط الناري الشامل يتم إيقاف جميع خطوط الاتصال القادمة أو الخارجة ومنعها من إكمال طريقها ما عدا تلك التي تتفق مع أحد عناصر مجموعة القواعد Rule Set الممثلة لسياسة الشبكة الأمنية حيث يسمح لها بالمتابعة أي أن في هذا النوع من الحوائط النارية كل شيء لم يتم السماح به تخصيصا ضمن مجموعة القوانين والقواعد يجب منعه وإيقافه. أما نوع الحائط الناري الاستثنائي فيسمح لجميع محاولات الاتصال سواء من أو الى شبكة الحاسوب الخاصة بالمرور وإكمال طريقها ويعمل على استثناء وإيقاف تلك التي تتفق مع مجموعة القوانين لديه، أي: كل شيء لم يتم منعه تخصيصا بقاعدة ضمن مجموعة القوانين سوف يسمح له بالمرور والمتابعة.

كلمات السر: تعتمد اغلب الخدمات الإلكترونية والمواقع على الإنترنت بشكل جوهري على قيام المستخدم بإنشاء حساب لتلقي الخدمة أو استخدام الموقع. وأصبحنا اليوم مجبرين على إنشاء عدد كبير من الحسابات وكل حساب مكون من اسم مستخدم وكلمة سر. وجانب كبير من المخاطر التي تهدد سلامة بياناتنا وخصوصية المعلومات تعتمد على استهداف كلمات السر اما عن طريق خداع المستخدم لكتابة كلمة السر في صفحة وهمية أو عن طريق استخدام إحدى تقنيات الاختراق للوصول إلى كلمات السر أو الطريق الأكثر شيوعا وهي عن طريق لعبة التجربة والخطأ لتخمين كلمات السر بطريق إلكترونية وهي معروفة باسم هجوم القوة العمياء أو Brute Force Attack. وللأسف نجاح تلك الطرق قائم على مجموعة ممارسات خاطئة أو مفاهيم غير دقيقة لدينا تسهل على الآخرين قدرتهم على الاختراق ومن ضمنها: استخدام نفس كلمة السر عبر كل المواقع والخدمات. فنجد أن الشخص يستخدم نفس كلمة السر لحساب الجيميل وهوتميل وياهو وفيسبوك وتويتر. وبالتالي إذا تم استهداف حساب واحد سوف يتمكن من استهداف باقي الحسابات بمنطق تأثير الدومينو. استخدام حروف أو ارقام فقط في تكوين كلمة السر. تخمين كلمات السر قائم على تجربة تنويعات كبيرة من لوحة المفاتيح وبالتالي كلما كانت كلمة السر مكونة من حروف أو أرقام فقط أصبحت ضعيفة للغاية. الاعتماد على بيانات شخصية معروفة لتكوين كلمات السر. عملية التخمين تعتمد على حاسوب يقوم بتوليد كلمات السر بالاستعانة بمجموعة عبارات أو كلمات مفتاحية تكون في الغالب ناتجة عن معلومات عامة قام المخترق بتجميعها عنك ومن ضمنها تاريخ الميلاد، رقم الهاتف، الاسم الكامل، محل الإقامة، الوظيفة،

اسم حيوانات أليف وإلى آخره من بيانات شخصية متاحة ومعروفة. الاعتماد على المتصفح لتذكر كلمات السر بالنيابة عننا.. حيث نجد أن أغلب المستخدمين يعتمدون على المتصفح لتخزين وتذكر كلمات السر وتسجيل الدخول على المواقع بالنيابة عننا. تلك كلمات السر مخزنه فعليا على الجهاز في مكان ما وعند اختراق الجهاز يتم استهداف ذلك المكان. استخدام نفس كلمات السر لمدة سنوات وسنوات. نسيان تسجيل الخروج بعد استخدام المواقع أو الخدمات.

البرمجيات الخبيثة: تتضمن البرمجيات الخبيثة أشكال عديدة تعرف باسم الفيروسات وأحصنة طروادة والسخام.. وهي مثل البرامج الإلكترونية يتم تطويرها باستخدام لغة برمجية ولكن بهدف الإضرار أو أذية مستخدمين أخرين. يوجد برامج خبيثة تقوم بأشياء عبثية مثل تحريك الفأرة وتغيير صورة سطح المكتب ومنها برمجيات أكثر ضررا تقوم بإتلاف الجهاز وسرقة محتواها ومنها برامج شديدة الخطورة تسمح مراقبة أنشطة المستخدم خال اصابته. وفي عالم الجرائم الإلكترونية يوجد هواة يقوموا بتطوير برمجيات خبيثة من باب التباهي بالمهارات ومنهم شركات وهيئات لها موارد مكلفة تقوم بتطوير برمجيات ضارة. ويتم استهداف المواطن اما من خلال البريد الإلكتروني أو رسائل مواقع التواصل الاجتماعي أو روابط مزيفة إلى آخر تنقل البرمجية الضارة وتسمح التحكم عن بعد.

شبكة افتراضية خاصة (VPN): عند قيام أي مستخدم بالاتصال بالإنترنت يقوم بتلقي خدمة الإنترنت من شركة تقدم الخدمة، وبالتالي جميع أنشطة المستخدم على الإنترنت تتم من خلال ذلك المقدم مما يعني قدرة مقدم الخدمة معرفة نشاطك والتحكم في قدرتك على النفاذ للمواقع والمحتوى. استخدام VPN ببساطة يعني قيام المستخدم باستخدام برنامج مخصوص لتعمية اتصالك بالإنترنت، وعند استخدام أحد برامج vpn يقوم جهاز اولا بالاتصال بخادم البرنامج (سيرفر) ويعمل الخادم كوسيط لتمرير واستقبال البيانات بين جهازك والإنترنت ويوفر درجة خصوصية أعلى. مفيدة في احوال عديدة، منها مثلا عند استخدام شبكة واي فاي عمومية يمكن استخدام vpn لحماية كلمات السر مثلا أو أنشطة التصفح من تطفل أي شخص على نفس الشبكة. ويساعد أحيانا في تجاوز الحجب. الشبكات الافتراضية الخاصة مثلها مثل أي خدمة منها الجيدة والأمان ومنها الضعيف. يوجد تقنية أعلى أو مختلفة عن الشبكات الافتراضية الخاصة، يعرف متصفح تور وهو عبارة عن متصفح مثل فيرفوكس وكروم ولكن يعتمد على تعمية نشاط المستخدم على محو معقد يوفر مجهولية وخصوصية جيدة للمستخدم يصعب تتبعها، في حالة الشبكة الافتراضية الخاصة تقوم أغلب الخدمات بتعمية نشاطك في طبقة واحدة (من خلال سيرفر واحد) وفي تور يتم استخدام عدة طبقات.

الهندسة الاجتماعية: عبارة عن تقنيات تواصل تهدف إلى تشجيع الناس على القيام بعمل ما أو الإفصاح عن معلومات شخصية ذات طابع سري أو طابع علني. وعادة ما تتسم أساليب الهندسة الاجتماعية بتحضير بيانات شخصية تساعد في إتمام المهمة قد تتضمن حصر العلاقات المهنية والاجتماعية، والحسابات الإلكترونية، وأرقام الهواتف، ومراقبة ما ينشره الشخص على مواقع التواصل الاجتماعي لرصد أسلوب الكتابة.. إلى آخره. وفي السياق الرقمي يتم تنفيذ الهجمة من خلال الهاتف أو البريد الإلكتروني عن طريق انتحال هوية شخص ذي سلطة أو شركة أو في منصب ما لتقليل إثارة الشبهات ويتم إرسال الأسئلة أو الصياغة التي عادة تكون محكمة وتطلب من المتلقي بيانات أو القيام بشيء ما. ومن بين أساليب الهندسة الاجتماعية ما يعرف باسم الاصطياد.

الاصطياد: الوصول إلى معلومات خاصة بمستخدمي الإنترنت مثل المعلومات الشخصية أو البنكية أو كلمات السر، أو الموقع الجغرافي للشخص، أو بيانات نظام التشغيل على الحاسوب، عن طريق البريد الإلكتروني أو استمارات أو مواقع أو روابط، اعتمادا على انتحال هوية جهة ما. وبمجرد نجاح عملية الاصطياد تبدأ فعليا عملية الاختراق للحسابات باستخدام البيانات التي تم الوصول إليها.
اصطياد كلمات المرور: اصطياد كلمات المرور تقنية بسيطة من حيث التكلفة المادية ودرجة التعقيد التقنية، بالمقارنة ببرمجيات اختراق الأجهزة. وهي الطريقة التي تم استخدامها في جميع الهجمات محل البحث في التقرير.

الاختراق: يوجد أنواع كثيرة للاختراق تختلف تكلفتها ودرجة التعقيد التقني بها بناء على المراد اختراقه سواء كان حسابًا إلكترونيًّا أو حاسوبًا أو هاتفًا. وبطبيعة الحال فإن تقنيات الاختراق أكثر كلفة من تقنيات اصطياد كلمات المرور.

برمجيات خبيثة: يقصد بها برمجيات تم تصميمها لإلحاق مستويات مختلفة من الضرر. ويستخدم مصطلح برمجيات خبيثة للإشارة إلى مختلف الأساليب الممكنة مثل: فيروسات - أحصنة طروادة.
اختراق الحسابات: قيام شخص أو جهة بالنفاذ إلى حسابات إلكترونية لشخص آخر من خلال سرقة كلمة السر، وقد يقوم المخترق باستخدام كلمات السر (التي حصل عليها من خلال الاصطياد) للنفاذ إلى الحسابات مع الإبقاء عليها دون تغيير أو مع تغييرها، وبالتالي عدم قدرة الشخص الأصلي على النفاذ وإدراك الاختراق. ويعتبر الإبقاء على كلمة السر دون تغيير في حالات الاختراق أشد خطورة حيث، فقد يقوم شخص بمطالعة البريد الإلكتروني لشخص آخر على مدار شهور بدون علم صاحب الشأن، وقد يعتبر هذا الأسلوب إحدى مصادر المعلومات للهندسة الاجتماعية لتطوير هجمة أكثر تعقيدًا.

مفاهيم وتعريفات

اختراق الجهاز: يتضمن وسائل مختلفة منها القيام بزرع برمجية خبيثة على الحاسوب أو الهاتف من أجل التحكم الكلي في الجهاز عن بعد والنفاذ في كل المحتوى بما فيها كلمات السر وفي هذه الحالة يتم زرع البرمجية من خلال إحدى أساليب الهندسة الاجتماعية لإقناع المتلقي بالضغط على رابط أو تنزيل ملف ما أو القيام بفعل مختلف، ويعتبر هذا النوع من أكثر الأنواع التقنية المعقدة والمكلفة. ومن بين الوسائل الأخرى البحث عن نقاط ضعف في إعدادات الحاسوب أو النظام أو الشبكة الداخلية لاستغلالها

التشفير المتماثل Symmetric Encryption: في التشفير المتماثِل، يستخدم كل من المرسِل والمستقبِل المفتاحَ السري ذاته في تشفير الرسالة وفك تشفيرها. ويسمى التشفير بالمفتاح المتناظر لأن المفتاح الذي يستخدم لتشفير الرسالة هو نفسه المستخدم لفك تشفيره فنستطيع استنتاج قيمة مفتاح فك التشفير من مفتاح التشفير والعكس بالعكس. في حين أن معظم خوارزميات التشفير بالمفتاح المتناظر تستخدم نفس المفتاح للعمليتين. تعد خوارزمية Data Encryption System (DES) أحد أهم الخوارزميات المتناظرة المستخدمة بشكل كبير ولا تزال تستخدم على نطاق واسع لتحقيق الاتصال الآمن على الإنترنت ضمن بروتوكول SSL ومجالات أخرى شبيهة.

التشفير الغير المتماثل Asymmetric Cryptography: وجد التشفير اللامتماثل نتيجة للعيب الموجود في التشفير المتماثل والذي يتمثل في التوزيع الغير آمن لمفاتيح التشفير المتماثل فتم حل هذه المشكلة من خلال خوارزمية رياضية تنتج مفتاحين أحدهما يدعى المفتاح العام Public Key وهو المفتاح التشفير الذي يشفر به، والمفتاح الخاص Private Key وهو المفتاح السري الذي تفك به الشيفرة، فالمفتاح الخاص والعام في النهاية لا يمكن تفريقهما لما بينهما ارتباطات انتجتها الخوارزمية الرياضية فهما في النهاية كنصفي حجر لا يمكن أن يتشابكا أو يلتحما إلا بوجود النصفين الصحيحين بالذات، يمكن للجميع الحصول على المفتاح العام ولكن لا يمكن لأحد أن يعلم ما هو المفتاح الخاص الذي يكون مستقلا استقلالا تاما عن المفتاح العام فهو غير مشابه له ولا يمكن استنتاج المفتاح الخاص من المفتاح العام ومن أشهر الخورازميات الغير متماثلة النوع RSA وهي عبارة عن خوارزمية تشفير مبنية على الأعداد الأولية تقوم بإنتاج مفتاحين أحدهما هو المفتاح العام Public Key الذي يشفر به الرسالة والآخر المفتاح الخاص Private Key وهذا أخير يتم الحصول عليه عن طريق خوارزمية Extended Euclidean algorithm أو ما تعرف بخوارزمية إقليدس

هجوم القوة الجبارة Brute force atack: يعتمد هذا الهجوم على استخدام جميع القيم والاحتمالات الممكنة للمفتاح في محاولة فك الشيفرة وتتوقف المحاولات فور الحصول على نص رسالة plaintext ذي معنى سليم، يستعمل هذا الهجوم ضد كل الأهداف المحمية بكلمات المرور مثل الملفات أو المستندات وكذلك حسابات المواقع و المنتديات و البريد الالكتروني، حيث يشبه هذا الأسلوب محاولة فتح خزنة ذات قفل رقمي وذلك بتجريب جميع التراكيب الممكنة من الأرقام إلى أن تفتح الخزنة وبالطبع كلما ازداد عدد الخانات التي يتكون المفتاح السري (المفتاح) منها كلما ازداد عدد القيم الممكنة للمفتاح وبذلك يزداد الجهز اللازم لنجاح هذا الأسلوب وبطريقة مشابهة نستطيع أن نجعل أسلوب القوة الجبارة أمرا شبه مستحيل وبذلك بأن نزيد حجم المفتاح بشكل كبير نوع من الهجوم الذي يعتمد على النص المشفر فقط، وتتم فيه محاولة تجربة كل المفاتيح المحتملة لفك النص المشفر،

المصادر

حبر - مجلة الكترونية ومؤسسة اعلامية

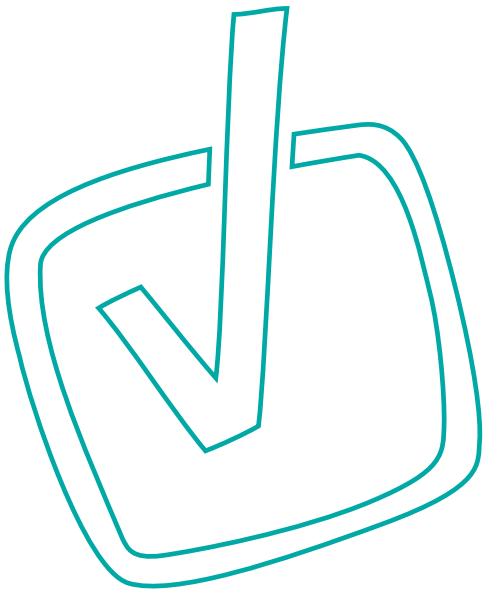
Smex - موقع تشارك

مؤسسة التعبير الرقمي العربي - أضف

موقع CyberArabs

موقع MyShadow

Tactical technology collective



حملة
المركز العربي
لتطوير الإعلام
الاجتماعي

تواصلوا معنا:
info@7amleh.org | www.7amleh.org
هاتف: +972 (0)774020670
تابعونا على وسائل التّواصل الاجتماعيّ: 7amleh