تهديدات رقمية بارزة خلال الحرب: التصيّد والهندسة الاجتماعية

1

تهديدات رقمية بارزة خلال الحرب: التصيّد والهندسة الاجتماعية

كيف يمكن استخدام الخداع للحصول على معلوماتكم الشخصية؟

2

الهندسة الاجتماعية وهجمات التصيد تعتمدان على التنكر بشكل ما، والتظاهر بأنها جهات موثوقة للحصول على معلومات حساسة مثل كلمات المرور وتفاصيل بطاقات الائتمان.

3

التهديدات الشائعة

سرقة البيانات الشخصية

سرقة الأموال

زراعة البرامج الضارة

انتحال الهوية

4

أنواع الهجمات:

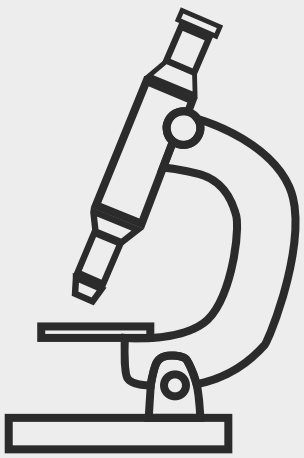
1. التصيد عبر البريد الإلكتروني
2. الرسائل النصية المضللة
3. التصيد المستهدف (رسائل مخصصة وشخصية للغاية لخداع أفراد أو مؤسسات)

5

كيفية الكشف عن الهجمات؟

التحقق من مصداقية العنوان الإلكتروني.

والحذر من الرسائل المضللة.



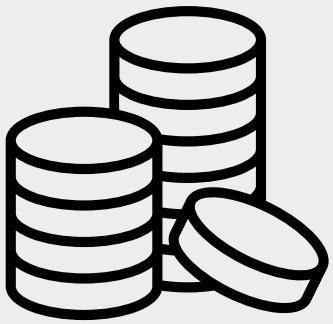
6

الإجراءات الوقائية

- تحديث النظام والبرامج
- تغيير كلمات المرور بانتظام
- تنزيل برامج مكافحة الفيروسات
- تفعيل المصادقة الثنائية
- الإبلاغ عن الرسائل المشبوهة

7

نصائح أساسية



- فكّروا جيدًا قبل مشاركة المعلومات الحساسة.

- الحرص والتأكد قبل الضغط على الروابط.

- **الحذر** هو المفتاح **للوقاية** من الهجمات الإلكترونية.

7amleh.org

حملة - المركز العربي لتطوير الاعلام الاجتماعي

تم إنشاء موارد الاستجابة لحرب غزة بالتعاون مع عدد من المنظمات
وهي متاحة للاستخدام والنشر من دون أي شرط.