الهجمات الإلكترونية

تقدمة : أ/هيله الحارثي

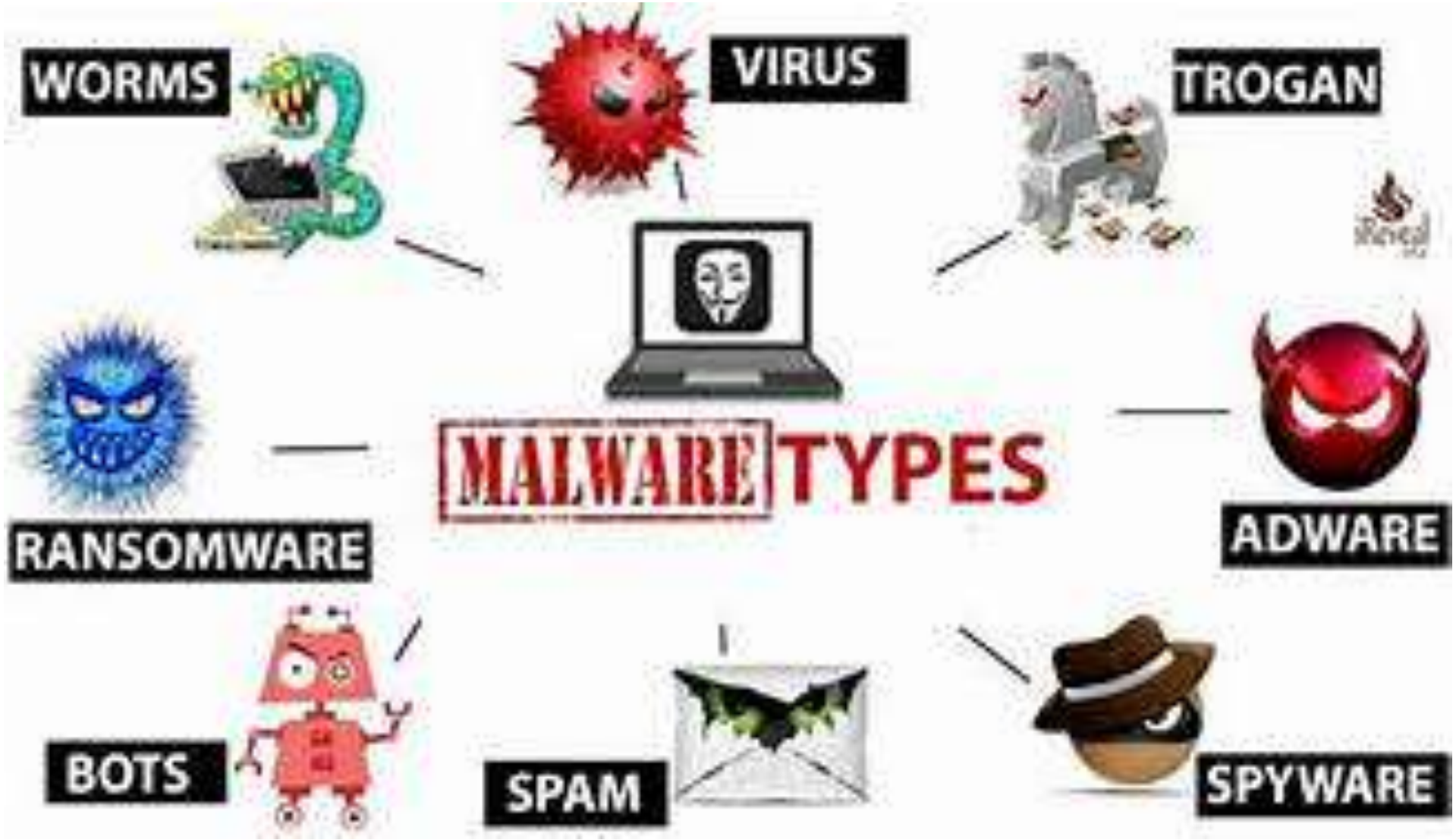
التصيد

البرامج الخبيثة -
Malicious software

- **البرامج الضارة (malware):**
- هي أي برامج يمكن استخدامها لسرقة البيانات أو تجاوز عناصر التحكم في الوصول أو إلحاق الضرر بالنظام أو تعريضه للخطر

- **برامج الحماية من البرامج الخبيثة (anti-malware) :**
- هي برامج تحمي جهازك من البرامج الخبيثة اما بتنبيهك او حذفها مباشرة بمجرد اكتشافها

Malware types



Types of Malware أنواع البرامج الخبيثة

- **الفيروس (Virus)**
  - هو عبارة عن كود تنفيذي خبيث (malicious code)
  - ملحقة بملفات قابلة للتنفيذ وغالبًا برامج مشروعة.
  - تنتشر الفيروسات بسرعة هائلة بمجرد الضغط على الملف التنفيذي (exe)

- **الديدان (Worms)**
  - الديدان هي كود خبيث مستقل
  - تقوم بتكرار نفسها من خلال استغلال الثغرات في الشبكات.
  - الديدان عادة تبطئ الشبكات.
  - تستطيع الدودة أن تنتشر بسرعة كبيرة عبر الشبكة.

- **حصان طروادة (Trojan horse)**
  - حصان طروادة هو برنامج خبيث يقوم بعمليات خبيثة تحت غطاء العملية المطلوبة.
  - يستغل هذا الرمز الخبيث صلاحيات المستخدم الذي يشغله.
  - في كثير من الأحيان ، يتم العثور على أحصنة طروادة في ملفات الصور والملفات الصوتية أو الألعاب.
  - حصان طروادة يختلف عن الفيروس لأنه يربط نفسه إلى الملفات غير القابلة للتنفيذ.

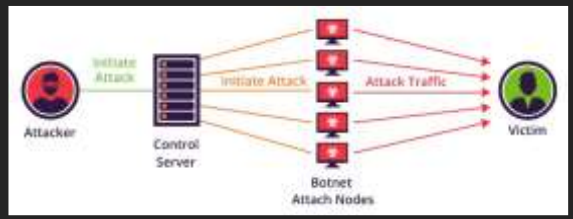
Types of أنواع البرامج الخبيثة Malware

- **برامج التجسس (Spyware)**
  - هذا البرنامج هو مصمم للتتبع والتجسس على المستخدم.
  - غالبًا تتضمن برامج التجسس: برامج تعقب النشاطات وجمع البيانات
  - **الغرض :** محاولة للتغلب على الإجراءات الأمنية بتعديل إعدادات الأمان
  - غالبًا ما توجد نفسها مع البرامج الشرعية المعدل عليها (أحصنة طروادة Trojan horses)

- **برامج الرعب (Scareware)**
  - هذا هو نوع من البرامج الضارة المصممة لإقناع المستخدم باتخاذ إجراء محدد بناء على الخوف.
  - تقوم برامج الرعب بتكوين نوافذ منبثقة تشبه نوافذ حوار نظام التشغيل.
  - تنقل هذه النوافذ رسائل مزورة تفيد بأن النظام في خطر أو يحتاج إلى تحميل برنامج أو أمر معين للعودة إلى التشغيل العادي.
  - في الواقع لم يتم تقييم أو اكتشاف أي مشكلات ، وإذا وافق المستخدم على البرنامج المذكور وتم تنفيذه ، فسيتم إصابة نظامه ببرامج ضارة.

Types of أنواع البرامج الخبيثة Malware

- **Ransomware الفدية**
  - برنامج خبيث يقيد الوصول للنظام و يطلب فديه فك التشفير
  - عادةً ما يتسلل إلى نظام به بريد إلكتروني تصيد (phishing email)أو إصابة موقع ويب ويستغل ثغرة أمنية موجودة في نقطة النهاية
  - ثم تنشئ Ransomware موطئ قدم (foothold)، وتتوسع إلى نقاط نهاية أخرى (endpoints)، وتتحرك لاكتشاف البيانات المستهدفة وجمعها وتنظيمها وتشفيرها.
  - .تشفير البيانات في الكمبيوتر باستخدام مفتاح غير معروف للمستخدم.
  - ينتشر الفدية بواسطة ملف تم تنزيله أو بعض ثغرات البرامج.
  - يطلب مقابل للحصول على مفتاح فك التشفير
- **Bots and Botnet**
  - جزء من برنامج تحت تحكم برنامج اخر برامج خبيثة تجعل من جهازك شبح (BOT)
  - يستخدمها المهاجمين عادة لهجمات تعطيل الخدمة (DOS)



ما هو الهجوم المخلوط

- **ما هي الهجمات الممزوجة (Blended attacks)**
- هي هجمات تستخدم تقنيات متعددة لخرق هدف.
- عن طريق استخدام العديد من تقنيات الهجوم المختلفة في وقت واحد ، يكون لدى المهاجمين برامج ضارة هي مزيج من :
  - الديدان ، وأحصنة طروادة ، وبرامج التجسس ، هندسة اجتماعية.
- النوع الأكثر شيوعًا في الهجمات الممزوجة يستخدم رسائل البريد الإلكتروني غير المرغوب فيها والرسائل الفورية والمواقع الشرعية لتوزيع الروابط حيث يتم تنزيل البرامج الضارة و برامج التجسس سراً إلى الكمبيوتر.

كيف اعرف ان جهازي مصاب

أعراض البرامج الضارة
Symptoms of Malware

بغض النظر عن نوع البرامج الضارة التي أصيب بها النظام ، فهناك أعراض شائعة للبرامج الضارة لمعرفة هل جهازك مصاب أم لا(:

1 - زيادة في استخدام وحدة المعالجة المركزية CPU.

2 - انخفاض في سرعة الكمبيوتر.

3 - الكمبيوتر يتجمد أو يتعطل في كثير من الأحيان.

4 - انخفاض في سرعة تصفح الإنترنت.

5 أ- مشاكل غير قابلة للتفسير)غير مفهومة(مع اتصالات الشبكة.

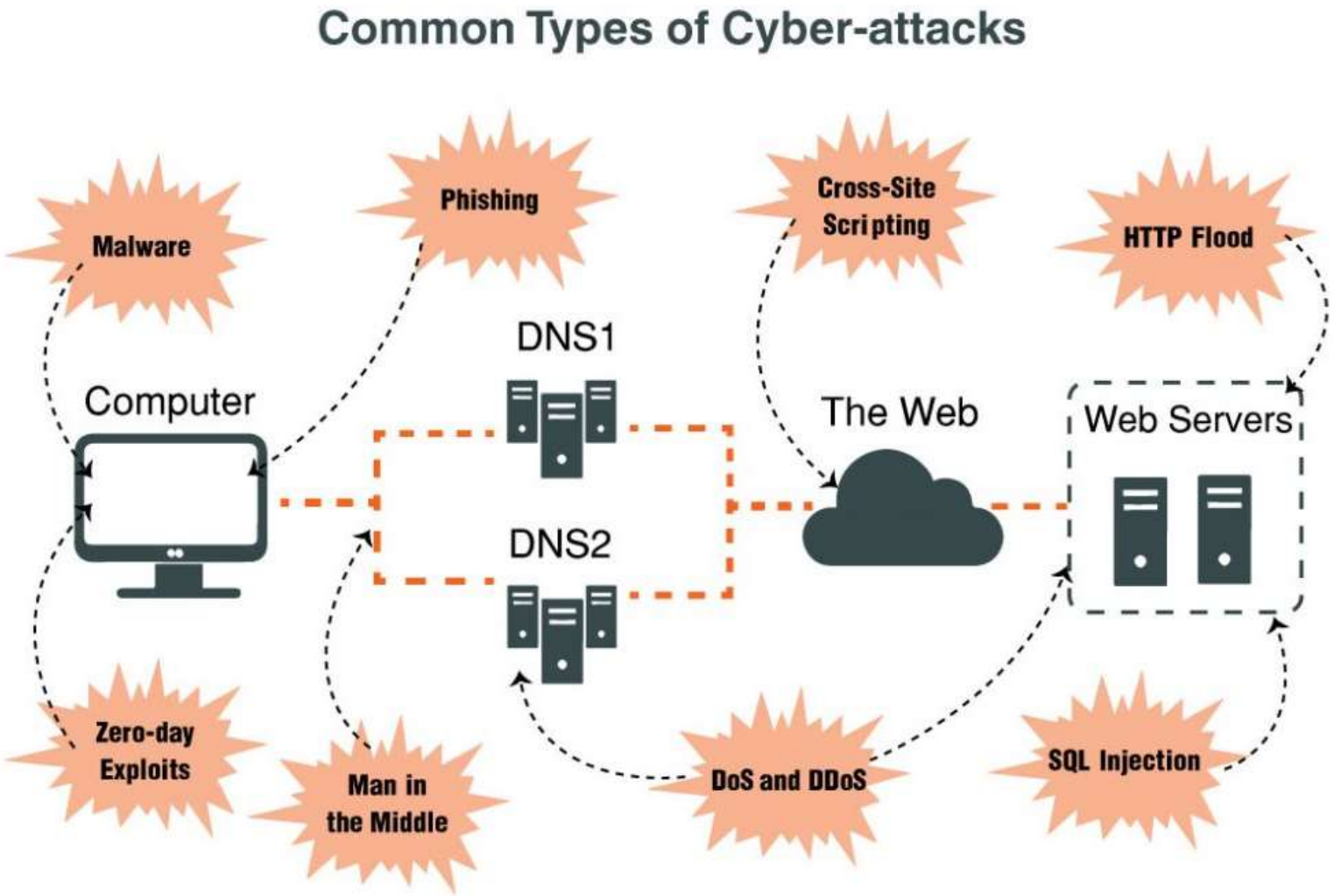
6 - تعديل الملفات الإلكتروني دون علم المستخدم و موافقته.

7 - حذف الملفات الإلكتروني دون علم المستخدم أو موافقته.

8 - وجود ملفات غير معروفة أو برامج أو رموز سطح المكتب.

9 - إيقاف البرامج أو إعادة تكوين نفسها.

10 - إرسال البريد الإلكتروني دون علم المستخدم أو موافقته.



امثلة على الهجمات السيبرانية

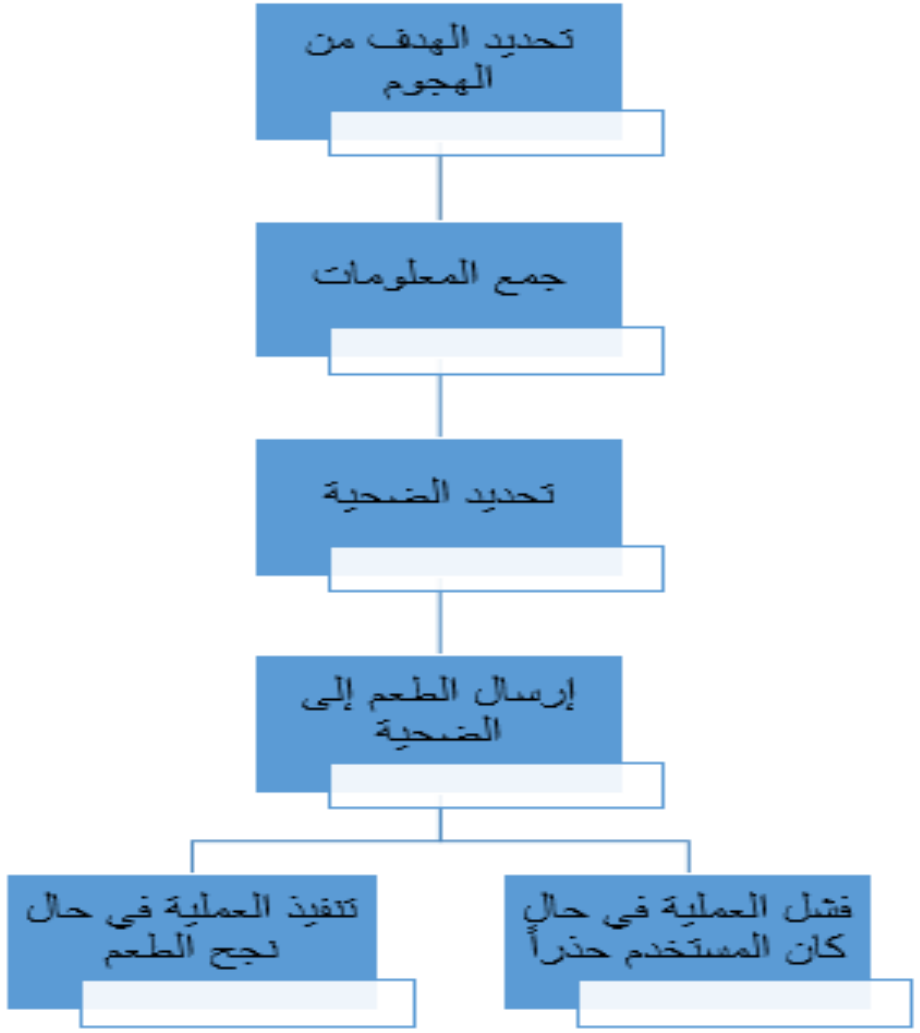
مصطلحات terminology

الهندسة الاجتماعية

- **ماهي الهندسة الاجتماعية Social Engineering؟**
- هو أسلوب من أساليب الاختراق والاحتيال التي تعتمد على العنصر البشري حيث يستخدم المهاجم مهاراته في الاتصال مع الآخرين ويستخدم أساليب الخداع والحيل النفسية ليحصل منهم على المعلومات المطلوبة ليتمكن بواسطتها من القيام بعملية الاختراق او الاحتيال

- Social engineering attacks can occur:
  - in person,
  - over the phone,
  - while surfing the Internet
  - and via email
- Many social engineers attempt to impersonate others

الهندسة الاجتماعية (life cycle)



أنواع الهندسة الاجتماعية

Shoulder Surfing
Tailgating

- التتبع لأخذ معلومات قيمه عن الهدف ممكن يضع كاميرا(قلمك - ساعتك) بدون علمك وممكن شخص يتتبعك بدون علمك

انتحال الهوية:

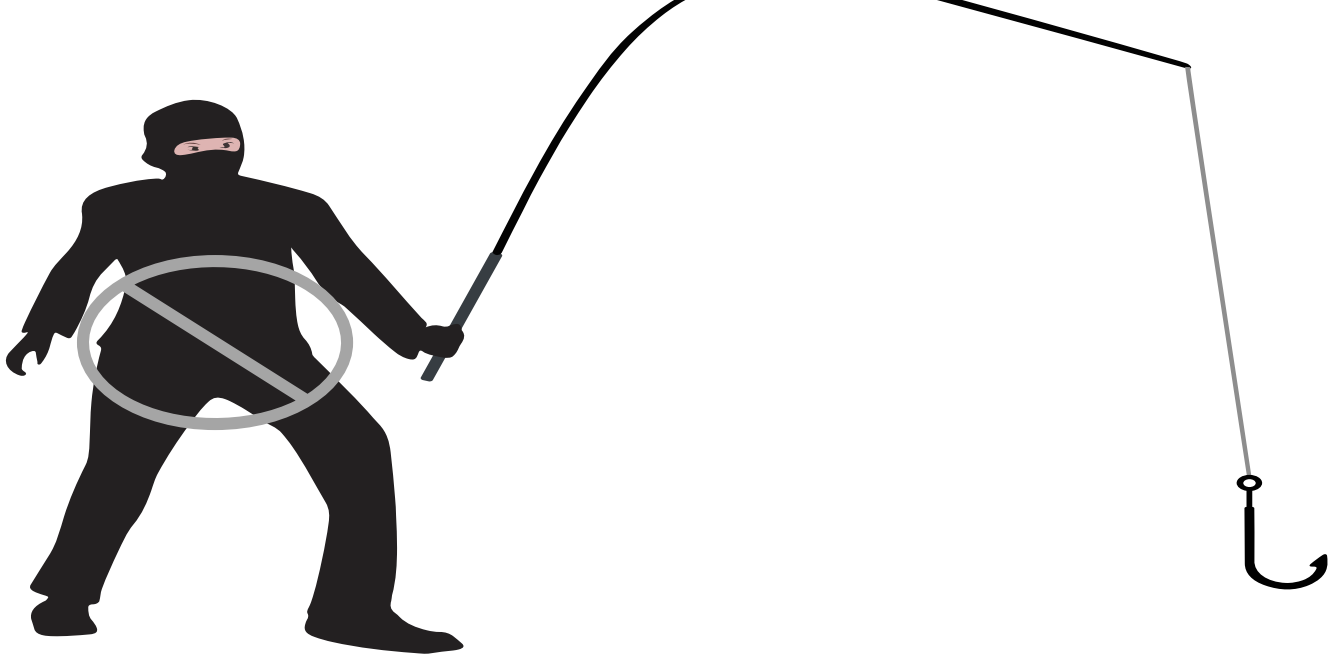
- تتطلب الهندسة الاجتماعية عادة بعض أشكال انتحال الهوية من أجل كسب ثقة الضحية.

التجسس والتنصت

- يمكن سرقة كلمة المرور ومعلومات مهمة عن طريق مراقبة الضحية حين كتابتها أو التنصت والاستماع لمحادثة هاتفية لذلك يُنصح دائما بتجنب كلمات السر والمعلومات الهامة على اوراق او أن يتم تبادلها مع اشخاص آخرين.

التصيد الإلكتروني
Phishing

- يُعد أحد أهم طرق الهندسة الاجتماعية
- وهو عبارة عن رسالة الكترونية تصل للضحية وتحتوي على لينك لصفحة وهمية تظهر مشابهة تماما للموقع الرسمي ومن الممكن ان تطلب من الضحية ادخال كلمة السر واسم المستخدم ومن ثم توجهه للصفحة الصحيحة بعد أن حصلت على البيانات السرية للضحية.



أبرز طرق عمليات التصيّد والهندسة الاجتماعية:

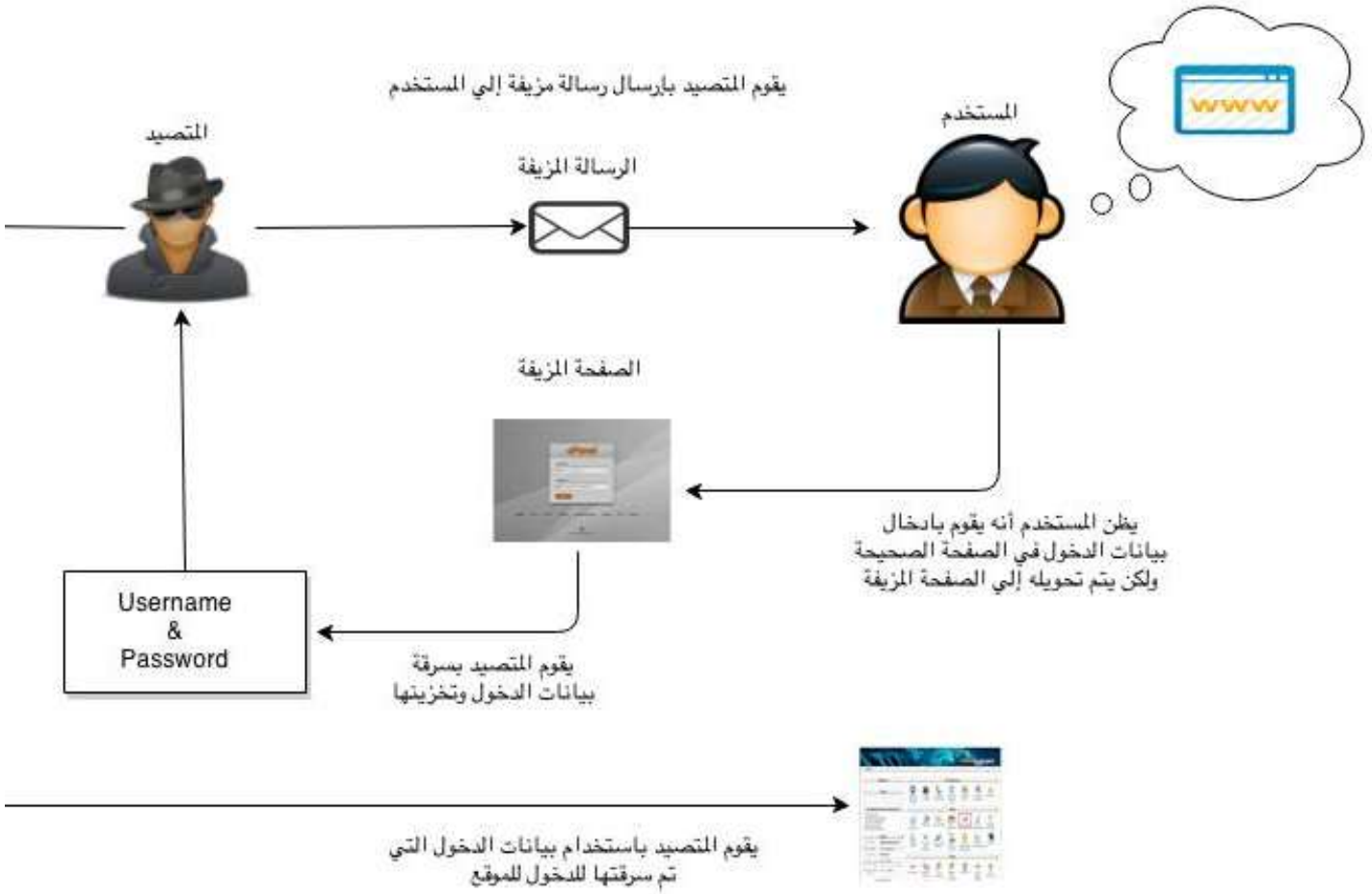
- محاولة الاتصال بك وإيهامك بتمثيل جهة رسمية أو شركة تجارية.
- اختراق حساب أحد أصدقائك أو أقربائك وإرسال رسائل منه تحتوي مرفقات خبيثة.
- إرسال روابط إنترنت أو ملفات أو برامج لمحاولة خداعك لفتحها للسيطرة على أجهزتك.

أمثلة عملية على عمليات التصيّد والهندسة الاجتماعية:

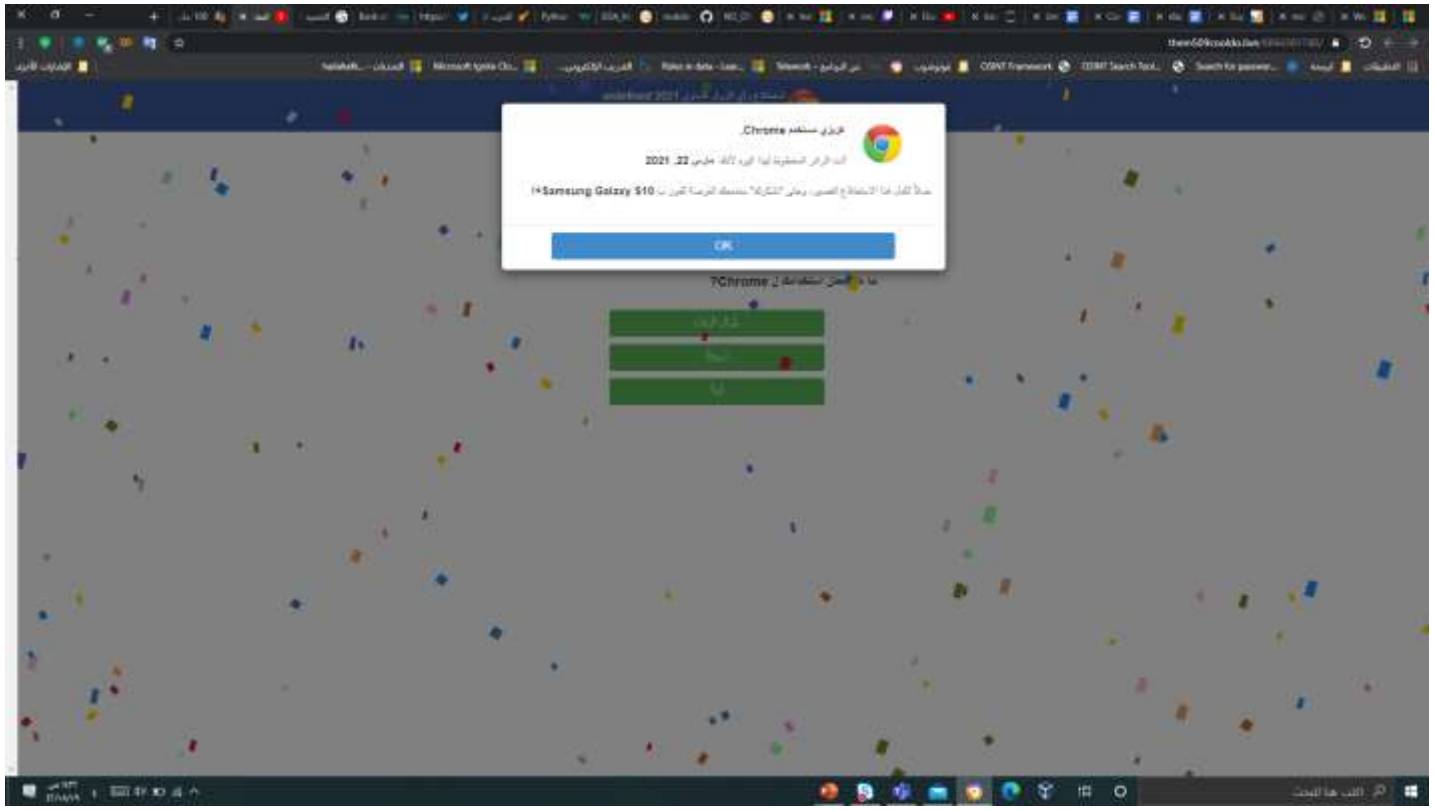
- متصل ينتحل شخصية مسؤول الدعم الفني في أحد المؤسسات، يطلب منك تزويده بمعلومات حسابك من أجل تحديث البيانات.
- اختراق حساب صديق لك ومن ثم تصلك رسائل من حسابه تطلب معلوماتك أو مساعدة مالية.
- نشر إعلانات لوظائف شاغرة مغرية وطلب تعبئة معلوماتك الشخصية لترشيحك لها.
- يصلك تنبيه عبر رسالة جوال بإيقاف حسابك المصرفي مع طلب فتح رابط لتحديث بياناتك.

https://cert.gov.sa/ar/awareness/?page=5&sort=oldest

سيناريو التصيد



امثلة على التصيد (المتصفح)



حملات تصيدية تستهدف
مايكروسوفت تيمز (Microsoft Teams)

وزارة التعليم
Ministry of Education

تجنب الضغط على الإعلانات الظاهرة في محركات البحث والتي تدعي وجود تحديث مجاني ومزيّف لمايكروسوفت تيمز

01 توخي الحذر عند النقر على الروابط ، والتحقق دائماً من صحة الرابط

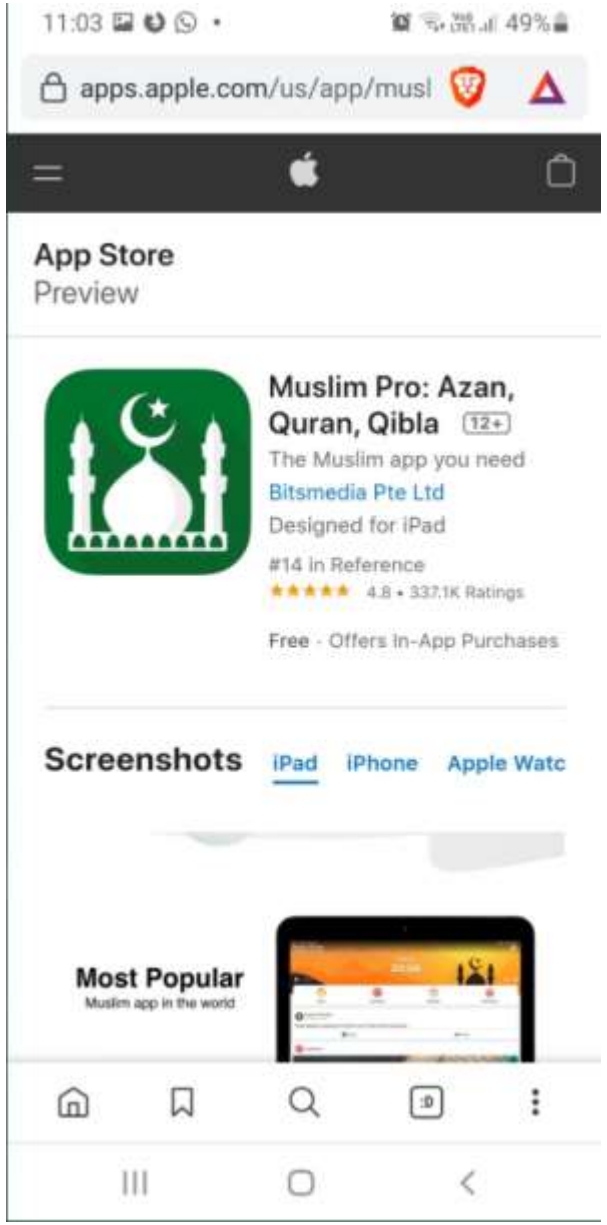
02 استخدام الروابط الرسمية التي تنشرها وزارة التعليم في موقعها الرسمي والقنوات التابعة لها

03 تحديث الانظمة والبرامج من المصادر الرسمية

www.moe.gov.sa @moe_gov_sa

امثلة على التصيد

امثلة على التصيد

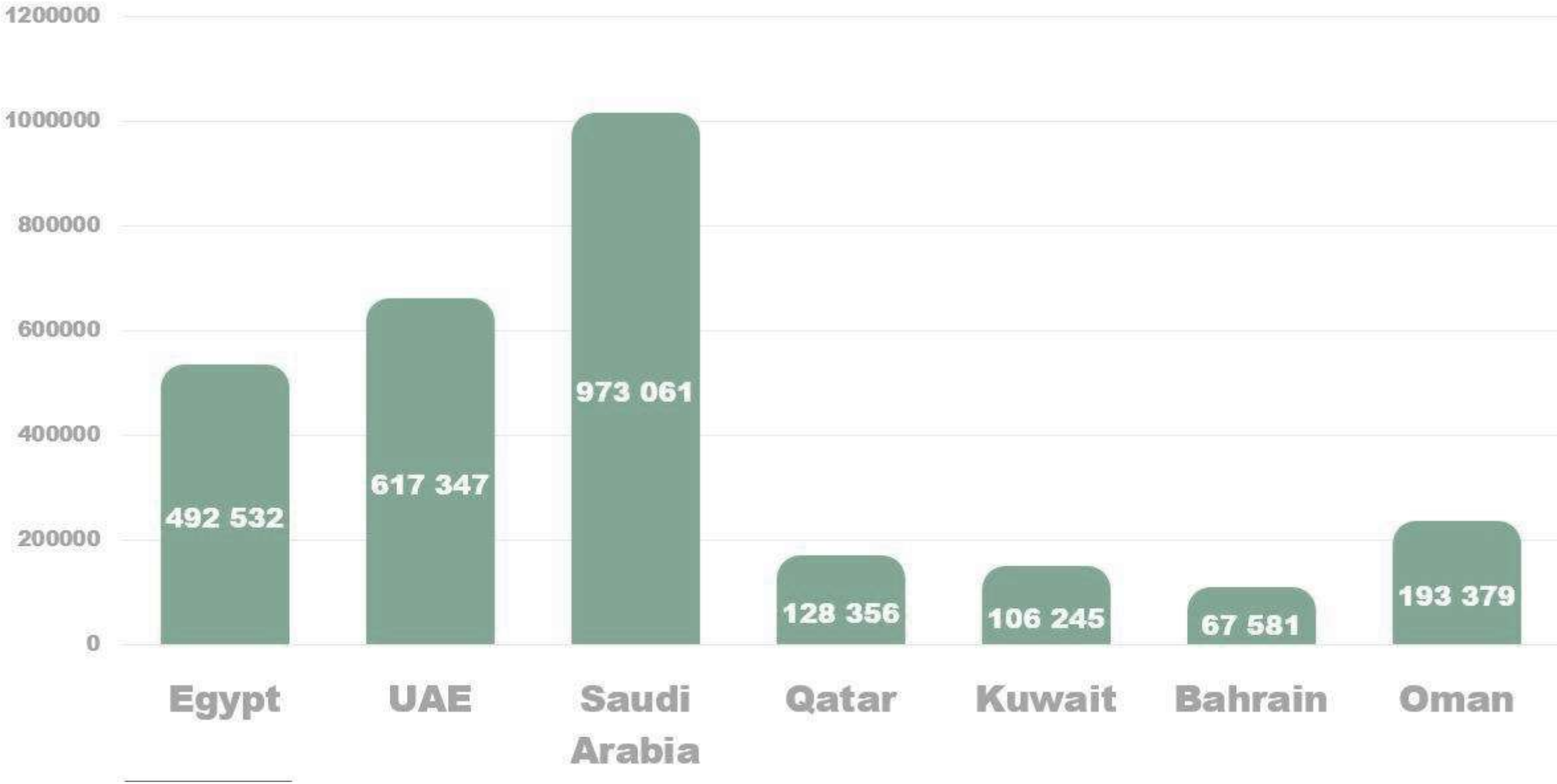


هذا التطبيق خان المستخدمين ، المسلمون بطبيعة الحال، وقام ببيع بياناتهم ومن بينها بيانات الموقع الجغرافي لجهات مثل الجيش الأمريكي والحكومة الأمريكية وغيرها!

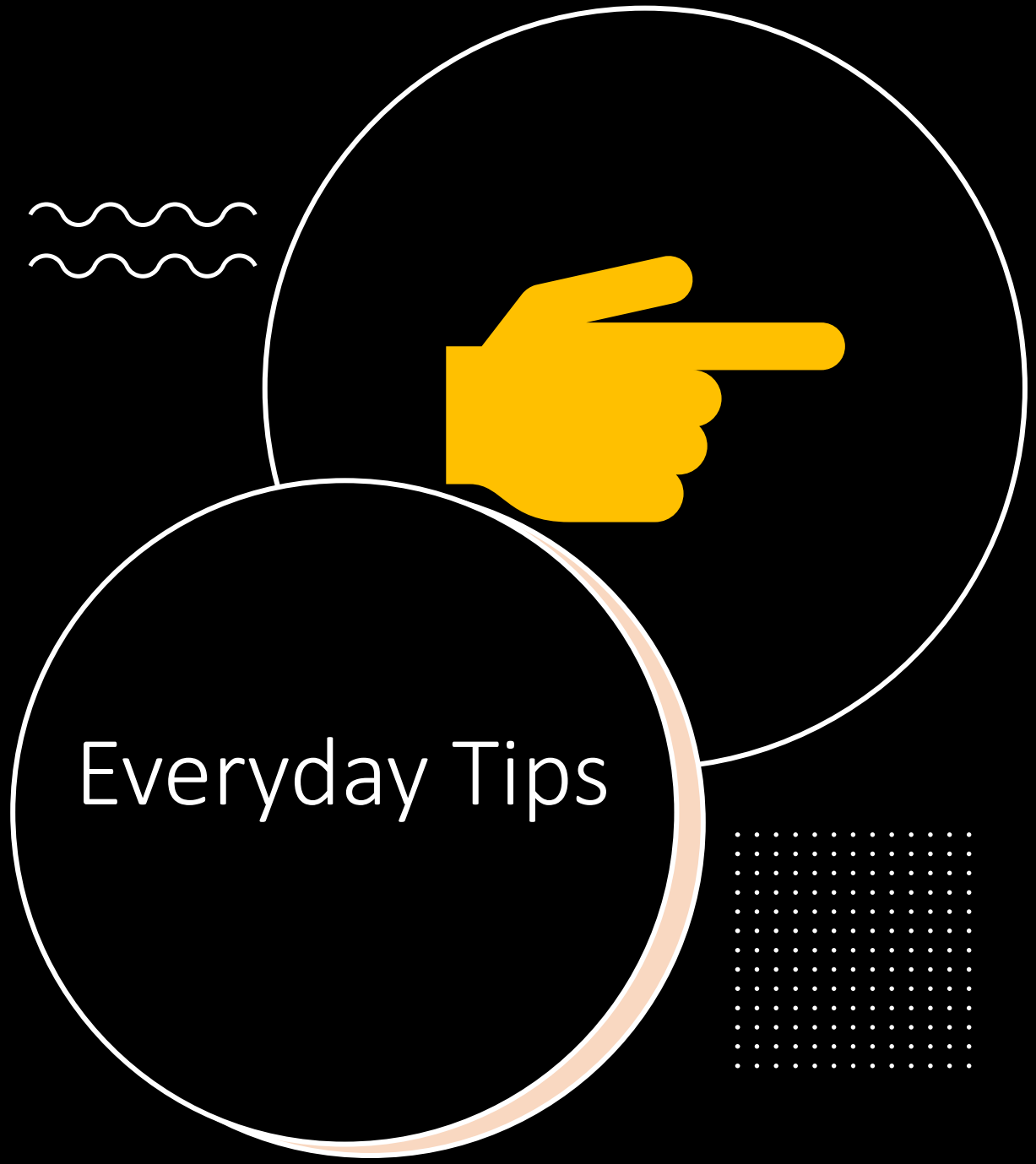
هذا التطبيق له قرابة 100 مليون عملية تحميل!

Email fishing

Phishing attacks in Q2



كيف نحمي أجهزتنا من هذه الهجمات؟



- احذر من المرفقات بالإيميل والروابط والمكالمات الصوتية من الاشخاص الغرباء
- لا تضغط على أي رابط ولا تفتح أي مرفقات لا تخصك
- استخدم [لابتوب , جوال , حسابات] منفصله للاستخدام الشخصي واخر للعمل
- فعل التحقق الثنائي لكل شيء
- لا تحمل برنامج من موقع غير موثوق او لا تعرفة
- استخدم تطبيقات ادارة كلمات المرور لتخزين الباسورد