هجمات التصيد الاحتيالي

إعداد وتقديم: سارة البوعينين

محاور العرض

- التصيد الاحتيالي وأشكاله
- كيف تتعرف عليه
- طرق التعامل معه و الحماية منه

ماهي هجمات التصيد الاحتيالي؟

التصيد الاحتيالي (Phishing)

هو احد انواع هجمات **الهندسة الاجتماعية (Social Engineering)**، حيث يزعم المهاجم بأنه جهة رسمية أو شخص تعرفة بغرض جمع معلوماتك الشخصية والحساسة لإستعمالها بإتخراق حساباتك وغيرها.

يعتبر التصيد الاحتيالي من أسهل الهجمات **تنفيذاً**، وذلك لأن المهاجم **لايحتاج لأن يكون مبرمج أو مخترق محترف**.

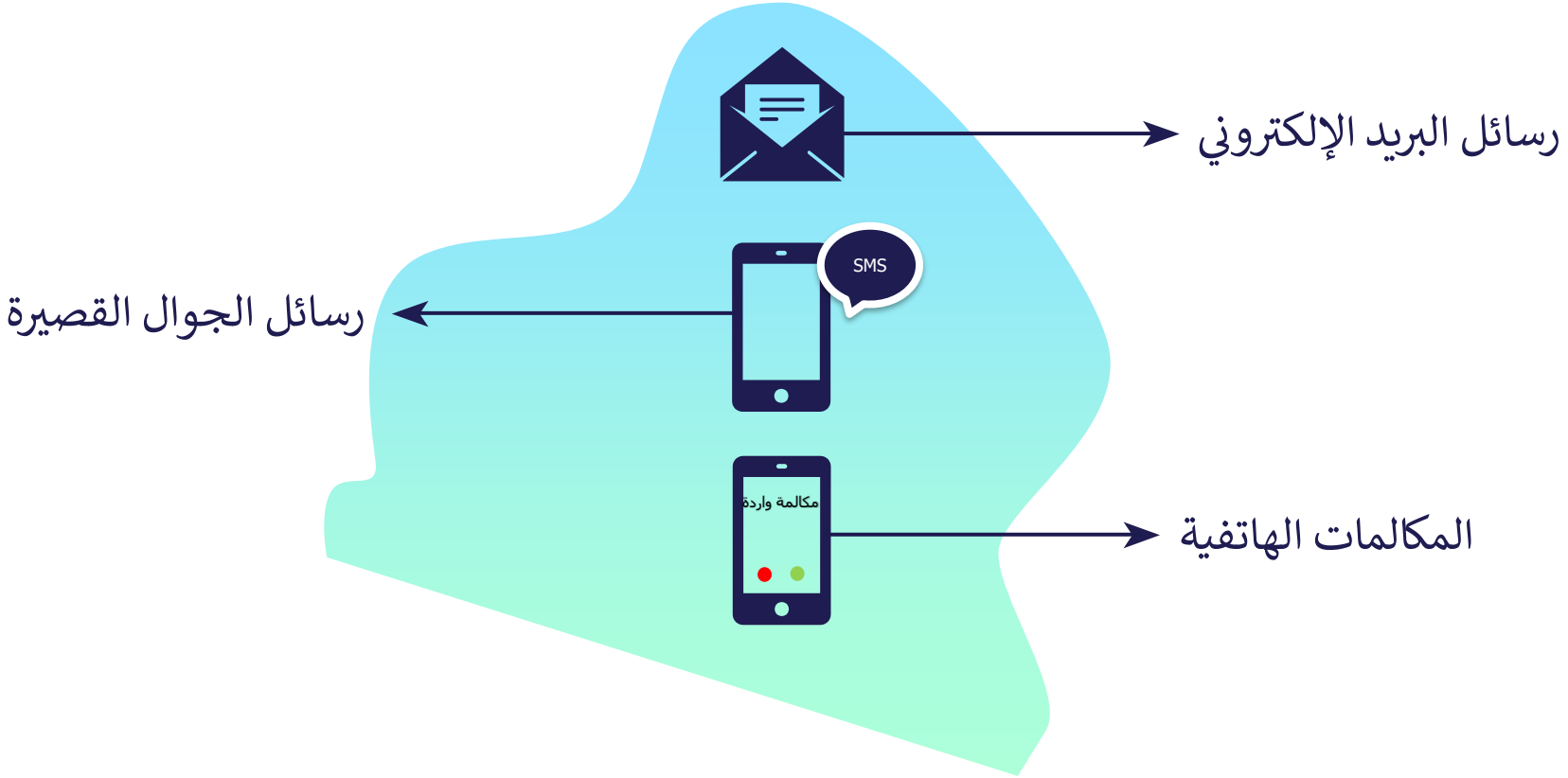
التصيد الاحتيالي (Phishing)

تعتمد أغلب هجمات التصيد الإحتيالي على أسلوب **الإلحاح** وأنه في حال عدم التجاوب حالاً سيحدث شيء لا ترغب به، مثل تجميد حسابك البنكي وغيره.
وقد يتم إستخدام اكثر من وسيلة ليكون الاحتيال أكثر أقناعاً.

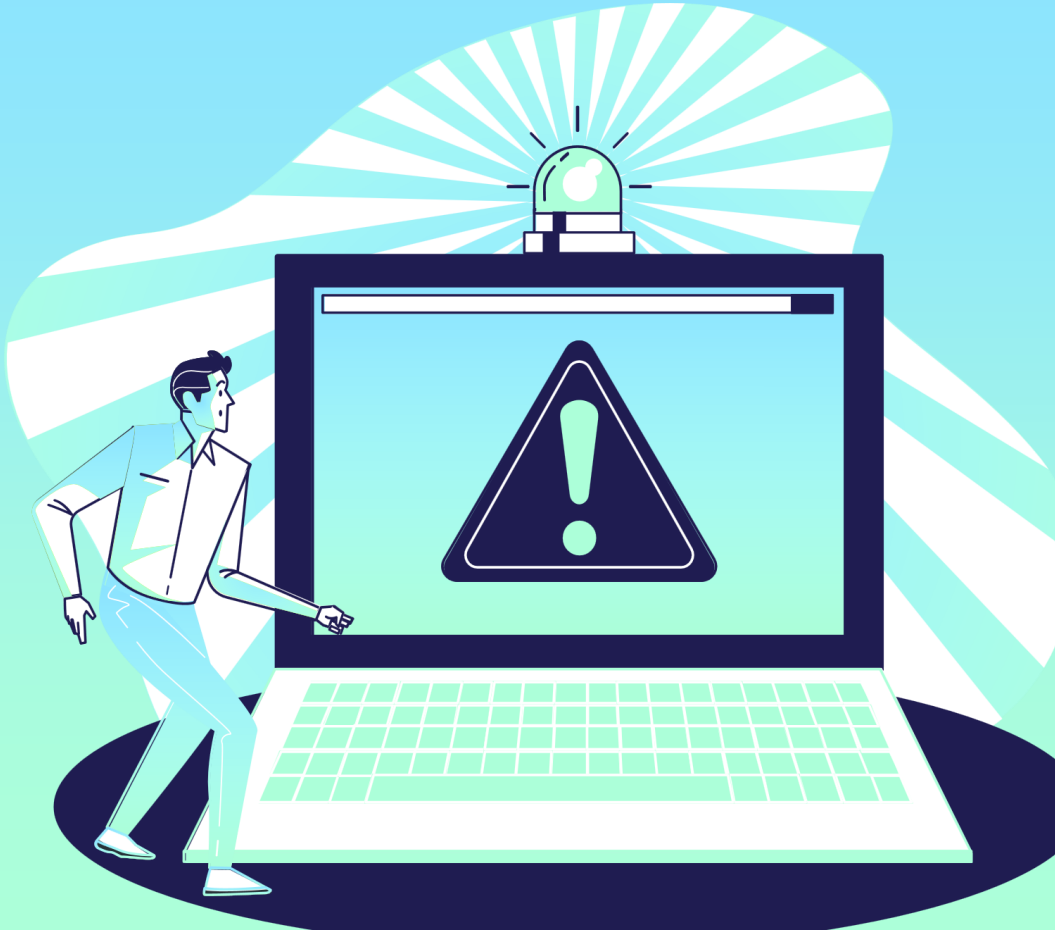
قد يكون التصيد الاحتيالي أحد خطوات **التهديد المتقدم والمستمر (Advanced Persistent Threat)**

بحيث إذا نجح المهاجم بإقناع الهدف يضمن استمرارية وجودة وتزويدة بالمعلومات لمدة أطول و وصولة لمدى ابعد.

للتصيد الاحتيالي أشكال كثيرة أشهرها:



كيف تتعرف على هجمات التصيد الاحتيالي؟



علامات واضحة تدل على التصيد الاحتيالي

1

طلب تحديث البيانات بشكل مستعجل

مثل تأكيد أسم المستخدم وكلمة المرور أو بياناتك البنكية

2

عروض خيالية

تقديم عروض خيالية وصعبة التصديق

3

الأخطاء اللغوية

كثرة الأخطاء اللغوية الإملائية

4

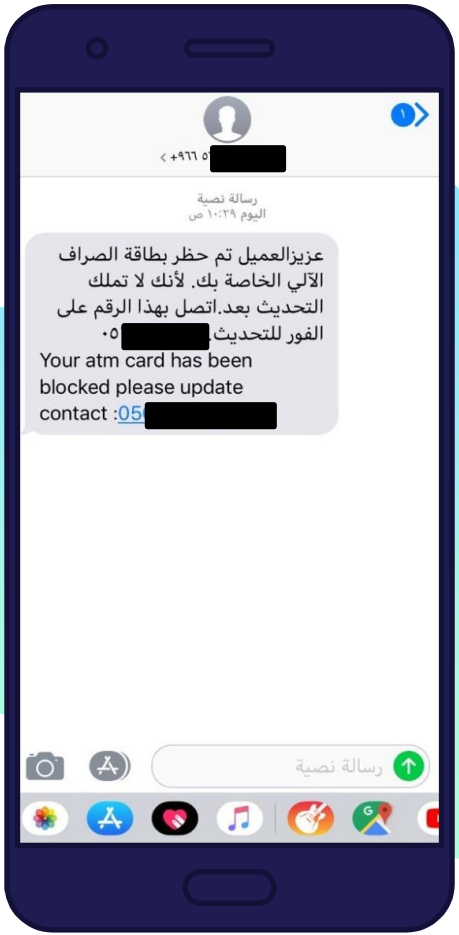
ملفات أو روابط مشبوهة

إرفاق ملفات مدمجة ببرمجيات خبيثة او روابط لمواقع مشبوهة غالباً منتحلة لجهة رسمية

المكالمات الهاتفية

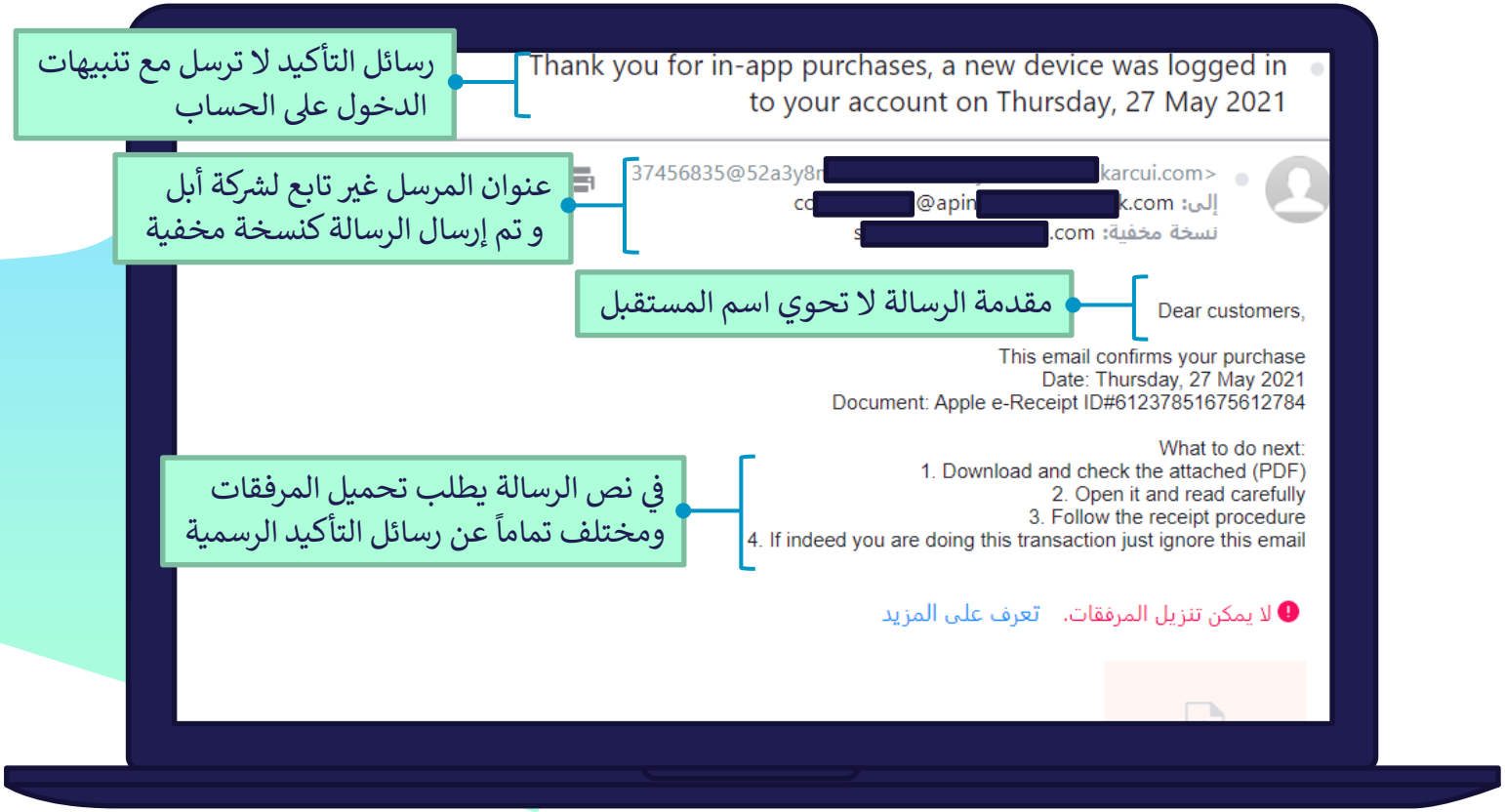
- إدعاء المتصل بانه من البنك وانك تحتاج إلى تحديث بياناتك فوراً واثناء هذة المكالمة وإلا سيتم تجميد حسابك.
- إدعاء المتصل بانه ممثل لشركة خدمات ويقوم بالترويج لها فيطلب عنوان البريد الالكتروني ، فيرسل رسالة تتضمن مرفقات مدمجة ببرمجيات خبيثة.

الرسائل النصية القصيرة



- الرقم المرسل مجهول
- البنك لا يطلب الاتصال على رقم جوال عادي أبداً
- أخطاء نحوية
- إختلاف النص العربي عن الانجليزي

رسائل البريد الإلكتروني



كيفية التعامل مع التصيد الاحتيالي والحماية منه

التعامل مع التصيد الاحتيالي

تأكد

تأكد من المصدر الاساسي عن الرسالة او المكالمة من خلال وسائل التواصل الرسمية

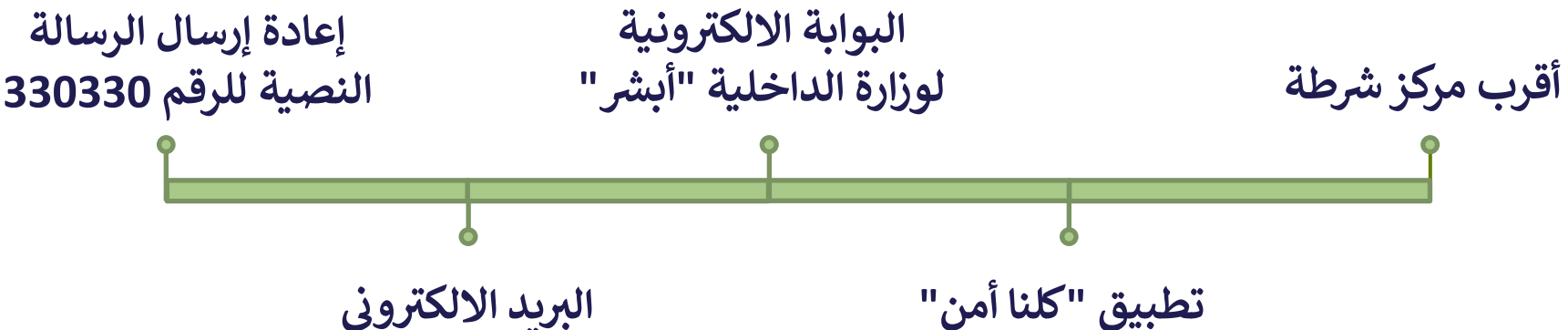
لا تتجاوب

لا تقم بتزويد اي معلومات حساسة او فتح وتحميل الملفات او الروابط المرفقة

بلغ

قم بإبلاغ الجهات المعنية في حال تعرضك للاحتيال

وسائل الإبلاغ للجرائم المعلوماتية



التبليغ عن رسائل التصيد الاحتيالي لمزود الخدمة

- تعليم الرسالة كتصيد إحتيالي يسمح لفريق مزود الخدمة بتتبع المهاجم وإتخاذ الإجراءات ضدة، بعد تعليم الرسالة يتم تحويلها والرسائل المستقبلية (لنفس المرسل) للبريد الغير مهم (Spam/Junk mail).

إرشادات الحماية

- تفعيل خاصية التحقق الثنائي لجميع حساباتك إن أمكن.
- عدم إعادة إستخدام كلمة المرور لأكثر من حساب.
- إستخدام كلمة مرور قوية.
- تثبيت برنامج حماية على أجهزتك.
- تجنب نشر معلوماتك الشخصية قدر المستطاع، خصوصا في مواقع التواصل الاجتماعي.
- تجنب تثبيت التطبيقات مجهولة المصدر.

شكراً لحضوركم

للتواصل

cs95.sarah@gmail.com

linkedin.com/in/cs95-sarah/