



هجمات التصيد الاحتيالي

إعداد وتقديم: سارة البوعينين

محاوَر 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 تعرفه بغرض جمع معلوماتك الشخصية والحساسة لإستعمالها بإتخراق حساباتك وغيرها.

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



التصيد الاحتيالي (Phishing)

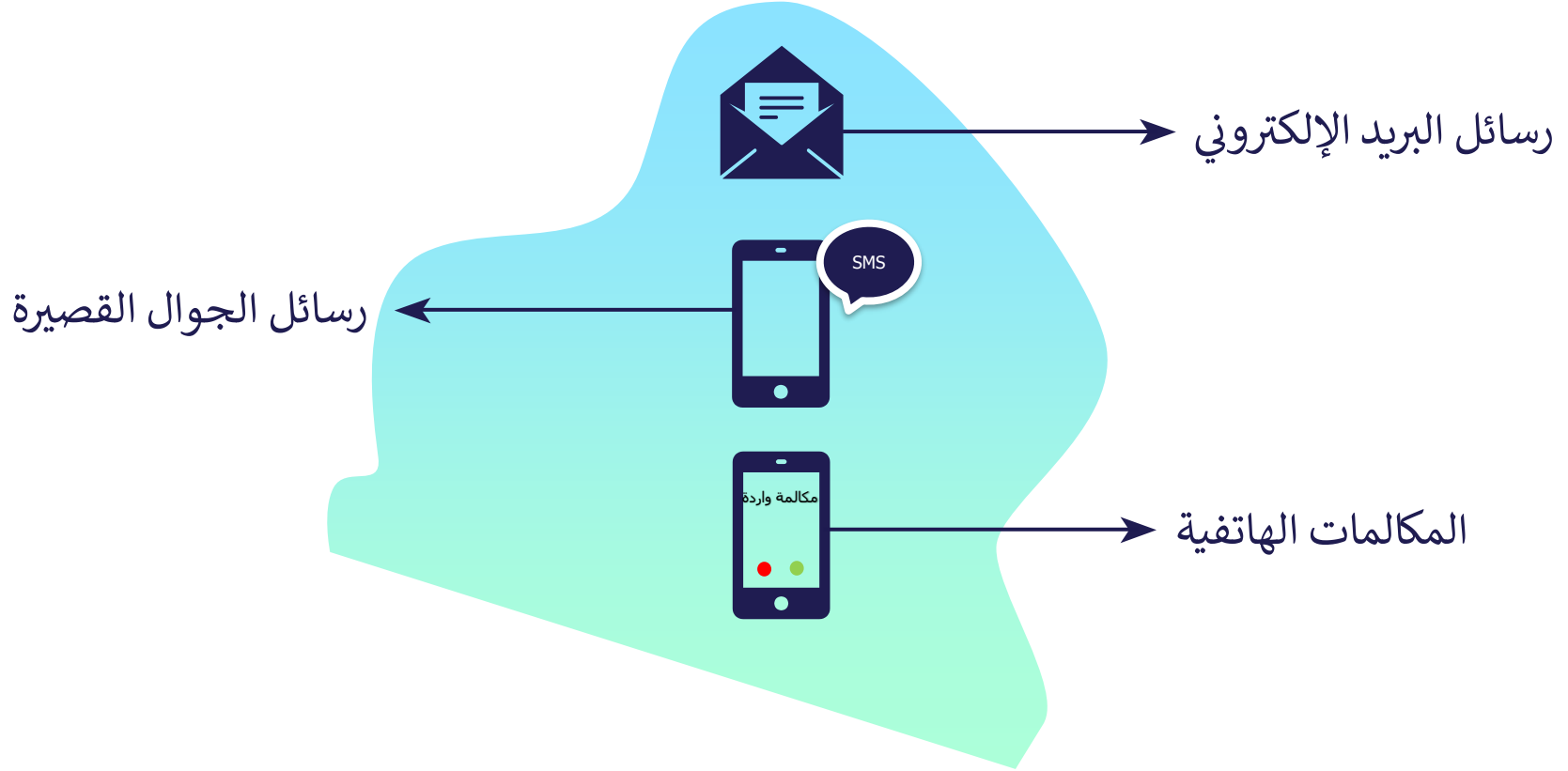
تعتمد أغلب هجمات التصيد الإحتيالي على أسلوب الإلحاح وأنه في حال عدم التجاوب حالاً سيحدث شيء لا ترغب به، مثل تجميد حسابك البنكي وغيره. وقد يتم إستخدام أكثر من وسيلة ليكون الاحتيال أكثر أقناعاً.

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 وصوله لمدى أبعد.



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

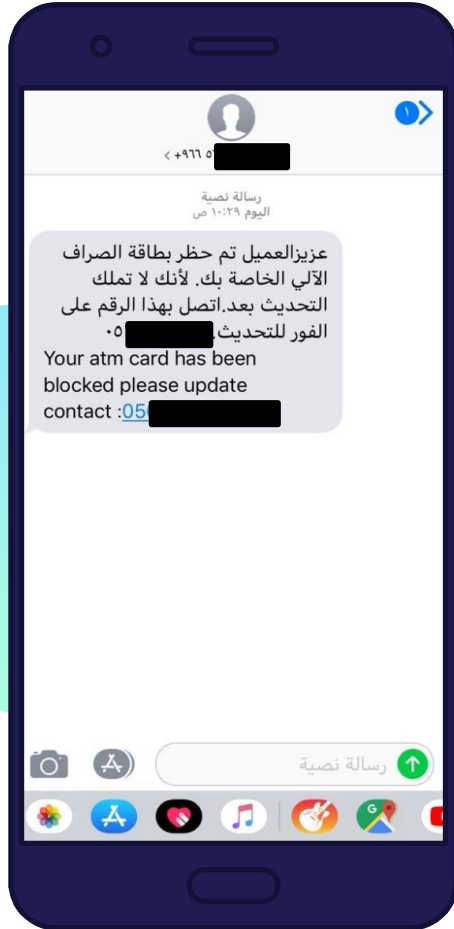
ملفات أو روابط مشبوهة
إرفاق ملفات مدمجة ببرمجيات خبيثة أو
روابط لمواقع مشبوهة غالباً منتحلة لجهة
رسمية

المكالمات الهاتفية

- إءءاء المتصل بانه من البنك وانك تحتاج إلى ءءءء بىاناتك فوراً واءناء هءة المكالمة وإلا سيتم ءءمىء ءسابك.
- إءءاء المتصل بانه ممءل لشركة ءءماء وىقوم بالءروىء لها فىطلب عنوان البرىء الالىءرونى ، فىرسل رساءة ءءضمن مرفقات مءمءة بىرمءىاء ءبىءة.



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

رسائل التأكيد لا ترسل مع تنبيهات
الدخول على الحساب

Thank you for in-app purchases, a new device was logged in
to your account on Thursday, 27 May 2021

عنوان المرسل غير تابع لشركة أبل
وتم إرسال الرسالة كنسخة مخفية

37456835@52a3y8r [redacted]@karcui.com>
إلى: [redacted]@apin [redacted]k.com
نسخة مخفية: [redacted].com

مقدمة الرسالة لا تحوي اسم المستقبل

Dear customers,

This email confirms your purchase

Date: Thursday, 27 May 2021

Document: Apple e-Receipt ID#61237851675612784

What to do next:

1. Download and check the attached (PDF)
2. Open it and read carefully
3. Follow the receipt procedure
4. If indeed you are doing this transaction just ignore this email

في نص الرسالة يطلب تحميل المرفقات
ومختلف تماماً عن رسائل التأكيد الرسمية

! لا يمكن تنزيل المرفقات. تعرف على المزيد

كيفية التعامل مع التصيد الاحتيالي والحماية منه



التعامل مع التصيد الاحتيالي



بلغ

قم بإبلاغ الجهات المعنية
في حال تعرضك للاحتيال



لا تتجاوب

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



تأكد

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

وسائل الإبلاغ للجرائم المعلوماتية

إعادة إرسال الرسالة
النصية للرقم 330330

البوابة الالكترونية
لوزارة الداخلية "أبشر"

أقرب مركز شرطة

البريد الالكتروني

Info.cybercrime@moisp.gov.sa

تطبيق "كلنا أمن"

التبليغ عن رسائل التصيد الاحتيالي لمزود الخدمة

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



Options>Security Options>Mark as Phishing

إرشادات الحماية



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



شكراً لحضوركم

للتواصل

cs95.sarah@gmail.com



linkedin.com/in/cs95-sarah/

