

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

التصيُّد الإلكتروني

+218 21 361 4115
+218 21 361 4127
+218 21 361 4177
info@nissa.gov.ly
www.nissa.gov.ly
www.cert.gov.ly

التعرف على التصيُّد الإلكتروني

المواقع المزيفة

- غياب علامة القفل بجوار رابط الموقع المزيف المُرسل من المهاجمين.
- خلو رابط الموقع المزيف من اختصار بروتوكول الويب الآمن (https) وبدلاً منه يظهر الرابط بهيئة (http) فقط.
- اختلاف اسم الموقع المزيف عن اسم الموقع الصحيح بشكل بسيط وغير ملاحظ من الوهلة الأولى، مثل www.amazonx.com كبديل مزيف عن الموقع المعروف www.amazon.com.

البريد المزيف

- تأتي الرسائل المزيفة غالباً مخاطبةً العميل باسمه الأول فقط أو تخاطبه بـ"عميلنا العزيز" (Dear our valued customer)، بينما الرسائل المرسلة من المواقع الرسمية تخاطب العميل باسمه الكامل الحقيقي.
- يطلب أحياناً بريد التصيُّد الإلكتروني سرعة تحديث بياناتك عن طريق رابط معين، أو نموذج جاهز في البريد وهذا ما لا تفعله المواقع الرسمية كمواقع المصارف ومواقع التسوق الإلكتروني.
- أغلب صيغ هذا النوع من الرسائل يأتي لتخويفك أن حسابك في خطر وعليك تحديث وتغيير بياناتك تفاديا للسرقة، وهذا النوع من الرسائل مصمم أصلاً لسرقة بياناتك.
- قد يكون عنوان البريد المُرسل منه (Sender E-mail Address) غريباً وليس لموقع رسمي، أو هو لموقع لا يمت بصلة لمحتوى الرسالة.

التصيُّد الإلكتروني

ما هو؟

هو أحد طرق الاحتيال التي يستخدمها قراصنة الإنترنت، يعتمد على الهندسة الاجتماعية وهدفه الحصول على بيانات المستخدمين الخاصة مثل الأسماء وكلمات المرور أو البيانات المصرفية عن طريق انتحال صفة كيان وجهة موثوقة وشرعية. وغالباً ما يتم هذا النوع من الاحتيال عن طريق روابط لمواقع مزيفة تُرسل عبر البريد الإلكتروني أو مواقع التواصل الاجتماعي وغيرها من وسائل الاتصال.

نشأته

في تسعينات القرن الماضي كانت شركة AOL الامريكية رائدة في تقديم خدمات الانترنت ولديها الملايين من الزبائن، جلب هذا النشاط انتباه قراصنة البرمجيات والمتاجرة الغير مشروعة بها وتم إطلاق البرنامج AOHell في العام 1995 وتم تصميمه لاقتناص مستخدمي شبكة AOL عن طريق تنكر القراصنة بصفات أعضاء فريق الشركة وإرسال رسائل تطالب المستخدمين بتأكيد كلمات مرورهم.

مراحل الهجوم



أنواعه

Phishing الصيد بالشبكة

أكثر أنواع التصيُّد الإلكتروني شيوعاً ويعتمد على إرسال كم هائل من الرسائل الإلكترونية، يتظاهر فيها المهاجم بأنه جهة ذات اعتبار عن طريق تمويه جهة الإرسال ويسعى الى دفع الضحايا للقيام بفعل ما مثل إدخال اسم المستخدم وكلمة المرور في صفحة مزيفة أو تحميل ملفات خبيثة.

Spear phishing الصيد بالرمح

بعكس النوع السابق الذي يستهدف العموم، يعمد المهاجمون في هذا النوع من التصيُّد الى استهداف من لهم قيم عالية فقط من الأفراد والمؤسسات، يتميز هذا الهجوم بنسب نجاح عالية نتيجة لقضاء المهاجمون وقتاً طويلاً في جمع المعلومات عن الهدف وصياغة الفخ.

Whaling صيد الحيتان

يذهب المهاجمون هنا الى مستوى أعلى حيث يستهدفون رؤساء إدارة المؤسسات العملاقة وعينهم على بيانات المؤسسة والمعلومات الحساسة والأموال. يتطلب منهم الأمر مجهوداً أكبر حيث يبحث المهاجمون عمَّن يتواصل مع الهدف ومشاكله الخاصة والقانونية وما الى ذلك.