المركز الوطني
للسلامة المعلوماتية
Oman National CERT

عمان الرقمية
e.oman

التصيّد الإلكتروني

نصائح لكشف محاولات التصيّد والوقاية منها

المحتوى

- تعريف التصيّد الإلكتروني
- علامات البريد الإلكتروني المزور
- هدف المتصيد
- الحماية من التصيّد
- اختيار مضاد الفيروسات
- التصيّد الهاتفي
- الوقاية من التصيّد الهاتفي
- إفعل ولا تفعل

تعريف التصيّد الإلكتروني

هو محاولة سرقة البيانات الشخصية، باستخدام رسائل الكترونية ومواقع انترنت زائفة تقلد مؤسسات مالية وحكومية موثوقة، كخدمات المصارف الالكترونية.

علامات البريد الإلكتروني المزور

- البريد الإلكتروني المرسل ليس معنوناً إليك تخصيصاً (لا يحوي اسمك ولا رقم الزبون).
- آت من طرف من المستغرب أن يعرف بريدك الالكتروني.
- تبدو الرسالة عاجلة.
- عادة ما تحوي أخطاء إملائية ونحوية.
- تطلب منك النقر على وصلة لتقديم معلومات شخصية.
- تقود الوصلة إلى موقع وهمي يقلد شركة موثوقة.

هدف المتصيد

- يأخذ المتصيد معلوماتك الشخصية:
  - إما لينتحل شخصيتك.
  - أو ليحتال عليك مالياً ليسرقك.

هل تعلم؟

بدأت ظاهرة جديدة تتشكل من التصيد تسمى التزريع وهي إنشاء مواقع للسرقة، فبينما هدف التصيد شخصاً واحداً يكون هدف الاستزراع توجيه أكبر عدد ممكن من المستخدمين للإنترنت إلى مواقع وهمية مماثلة لمواقع رسمية موثوقة، بفرق واحد فقط أن هذه المواقع هدفها سرقة المعلومات الشخصية للزائرين، فتستثمر هذه المعلومات من بعد بطرائق مختلفة، من ضمنها بيعها للصوص آخرين.

الحماية من التصيّد

- حذار من رسائل البريد الإلكتروني التي تطلب معلومات شخصية.
- تجنب النقر على الروابط في رسائل البريد الإلكتروني.
- استخدام عامل تصفية الخداع، الذي يحدد المواقع الاحتيالية.
- عند الشك، اتصل هاتفياً مباشرة بالمؤسسة المعنية.
- لا تصدق العروض الخرافية.

تنبيه

المؤسسات الموثوقة لا تطلب معلومات عبر البريد الإلكتروني.

كن شديد الحذر من وصلات المواقع المرسلة بالبريد الإلكتروني

اختيار مضاد الفيروسات

من ضمن الحماية من رسائل التصيد تنصيب برنامج مكافحة فيروسات جيد يوفر حماية ضد التصيد، وبعض محركات البريد بها حماية من التصيد. هذه الحماية وإن لم تكن واقية تماماً إلا أنها توفر طبقة جيدة من الدفاع لحاسوبك.

التصيد الهاتفي

التصيد المعتاد يأتي عبر الإيميل لزيارة مواقع مشبوهة، لكن يمكن أن يقع عبر رسالة هاتف أو بريد إلكتروني أو رسالة فاكس يطلب منك الاتصال برقم إذا اتصلت به يخبرك بأن حسابك سيغلق ما لم توفر لهم بعض المعلومات الشخصية.

الوقاية من التصيد الهاتفي

- عامل كل رسالة لم تطلبها بريبة وحذر، ولا تضغط على أي وصلة.
- تأكد من رقم الهاتف المحلي عبر شركة الاتصالات، ولا تتصل اتصالات دولية.
- تأكد من المؤسسة المعنية التي تتعامل معها عبر مصادرها الموثوقة.
- راجع وثائقك ووصولاتك فعادة فيها الأرقام الموثوقة.
- أبلغ السلطات عن أي تصيد وقع لك.

إفعل ولا تفعل

إفعل:

- أحرص على أن مكافح الفيروسات الخاص بك يوفر حماية ضد التصيد.
- استخدام عامل تصفية الخداع، الذي يحدد المواقع الاحتيالية.
- تأكد من أرقام الهواتف عبر مزود الخدمة في بلدك, ولا تتصل أتصالات دولية.
- اتصل هاتفياً مباشرة بالمؤسسة المعنية, لستيضاح ما هو وارد في الرسالة البريدية, أذا شككت بالأمر.
- تأكد من المؤسسة المعنية التي تتعامل معها عبر مصادرها الموثوقة.
- راجع وثائقك ووصولاتك فعادة فيها الأرقام الموثوقة والبيانات المعتمدة وقم بمقارنتها.
- أبلغ السلطات عن أي حادثة تصيد وقعت لك.

إفعل ولا تفعل

لا تفعل:

- لا ترد على الرسائل التي تأتيك من جهة من المستغرب أن تعرف بريدك الإلكتروني.
- لا تستجيب لمطالب مستغربة من شخص تعرفة حتى تتأكد بطرق موثوقة منه, فقد يكون تم أنتحال شخصيته.
- تجنب النقر على الروابط في رسائل البريد الإلكتروني.
- لا تتأثر بالرسائل على أنها عاجلة وضرورية, فهو أحد أساليب التصيد.
- لا تتحمس للفرص التي تبدوا لك بأن بها فرصة فوز مغرية, فهي تحاول أن تدفعك للرد عليها.
- لا تعتمد على المضهر الخارجي للمواقع لكي تثق بها, فمن السهل تصميم صفحات مشابهة للمواقع الموثوقة.
- لا ترسل معلوماتك الشخصية قبل أن تتأكد أن القفل في أسفل المتصفح يعمل وأنه مقفل، فهذا يعطيك أماناً أكبر.