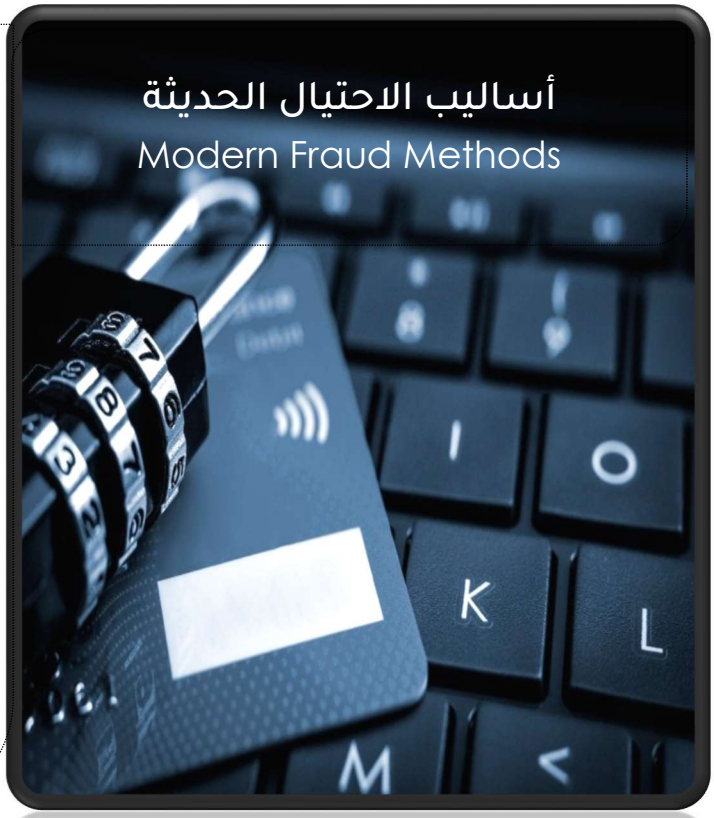
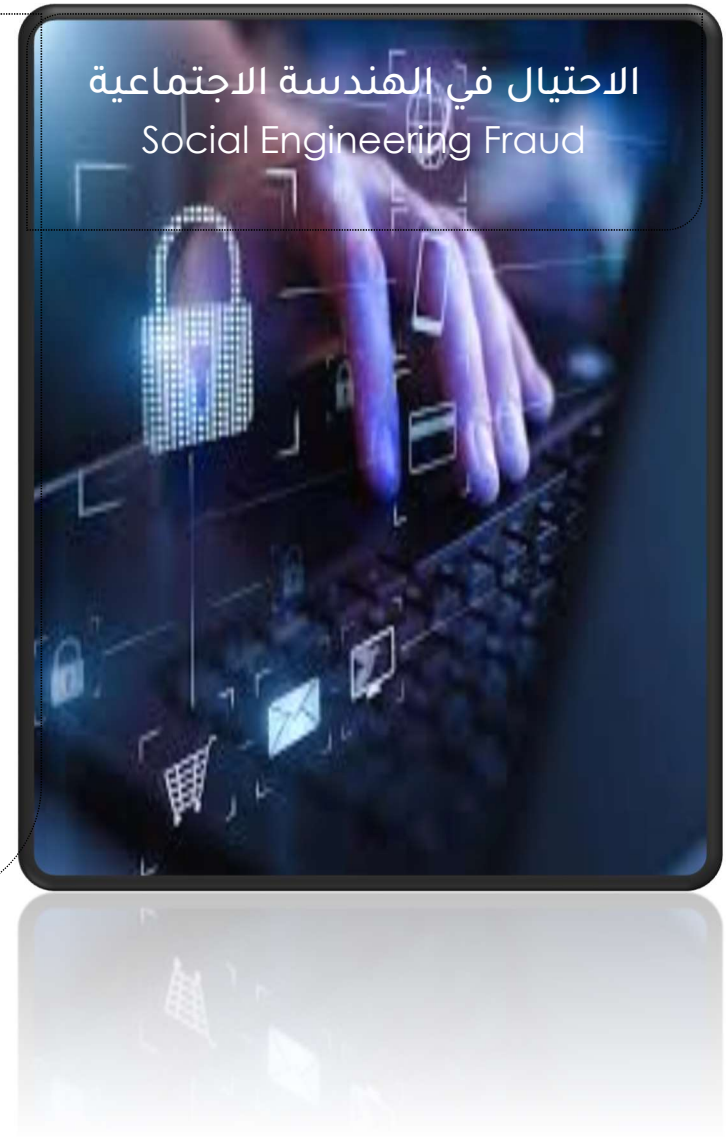
التوعية من الاحتيال الحديث عبر الهندسة الاجتماعية

Awareness of Modern Social Engineering Fraud



طرق المحتالين الحديثة غير مسبوقة لأن عصر اليوم الحديث يشهد تطورًا سريعًا في مجال التقنية ووسائل الدفع الإلكتروني، ومع هذا التقدم الهائل يأتي تزايد الاحتمالات للوقوع ضحية للأنشطة الاحتيالية. علاوة على ذلك، قد يحصل هؤلاء المحتالون على بعض معلوماتك الشخصية من وسائل التواصل الاجتماعي لجعل مطالبهم تبدو أكثر مصداقية.

The modern methods of fraudsters are unprecedented because today's modern era is witnessing rapid development in the field of technology and electronic payment methods, and with this tremendous progress comes an increased possibility of falling victim to fraudulent activities. Moreover, these fraudsters may obtain some of your personal information from social media to make their demands seem more trustiness



ما هو الاحتيال بالهندسة الاجتماعية؟

الاحتيال باستخدام الهندسة الاجتماعية إحدى طرق الاحتيال التي يُعتمد فيها على التلاعب النفسي لكسب ثقة الضحايا وإقناعهم بالقيام بعمل ما أو الإفصاح عن معلومات سرية مثل المعلومات الشخصية والمصرفية، وكلمات المرور، ورموز التحقق، وغيرها. وللإحتيال بالهندسة الاجتماعية العديد من الأساليب والوسائل، من أكثرها شيوعاً التصيّد الاحتيالي.

What is social engineering fraud?

Social engineering fraud is a form of fraud that relies on psychological manipulation to gain the trust of victims and convince them to take action or disclose confidential information such as personal and banking information, passwords, verification codes, etc. Social engineering fraud has many methods and means, the most common of which is phishing.

التصيّد الاحتيال في الهندسة الاجتماعية

Fraud Phishing in Social Engineering

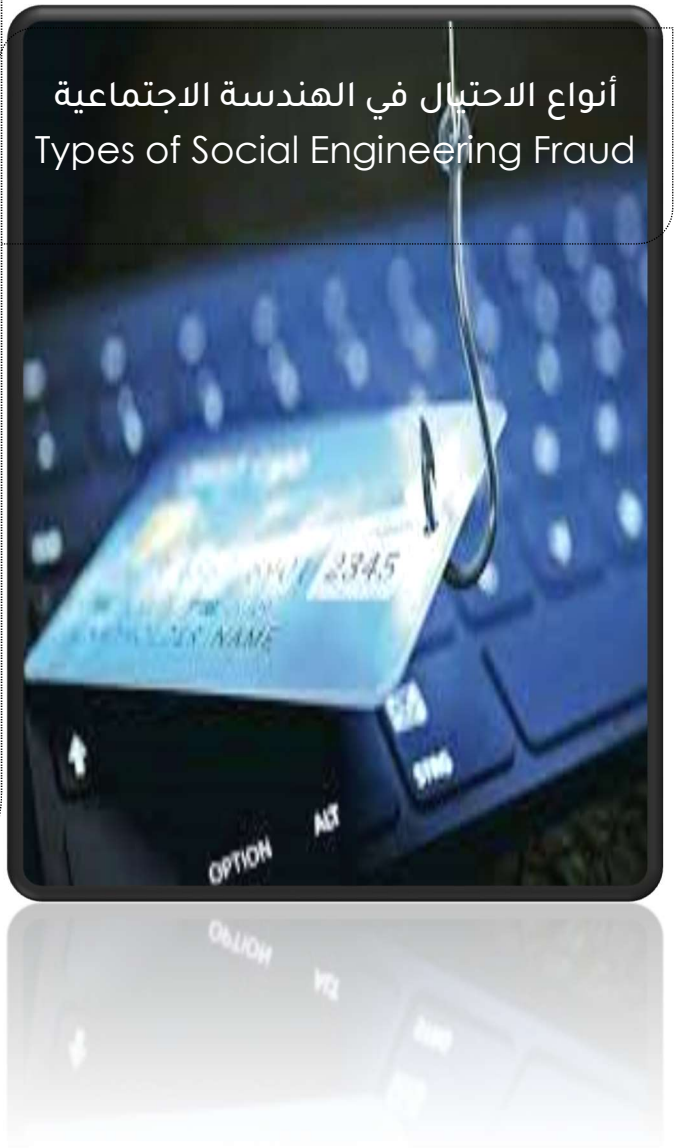
ما هو التصيّد الاحتيالي؟

التصيّد الاحتيالي من أساليب الاحتيال باستخدام الهندسة الاجتماعية التي يستخدم فيها المحتال وسائل التواصل المختلفة من رسائل نصية وبريدية ومكالمات هاتفية مدعياً أنه جهة رسمية أو شخصية اعتبارية ليخدع الضحية ويصل إلى معلوماته السرية. وعادةً ما يُستخدم في رسائل التصيّد الإلكترونية العناوين المضللة، واللغة الطارئة، والعروض الجذابة. وللتصيّد الاحتيالي العديد من الأنواع، هي:

What is fraud phishing?

Phishing is a form of social engineering fraud in which a fraudster uses various communication methods, including text messages, emails, and phone calls, pretending to be an official entity or legal entity, to deceive the victim and obtain their confidential information. Phishing emails usually use misleading titles, urgent language, and attractive offers. There are many types of phishing, including:

أنواع الاحتيال في الهندسة الاجتماعية
Types of Social Engineering Fraud



التصيّد الاحتيالي عبر البريد الإلكتروني:
يُرسل بريد إلكتروني مزيف وكأنه من شركة أو مؤسسة مالية موثوقة يُطلب فيه من الضحية مشاركة معلوماته الشخصية أو اتخاذ أي إجراء آخر يمكّن المحتال من الوصول إليها.

التصيّد الاحتيالي عبر الرسائل النصية:
تُرسل رسالة نصية مزيفة وكأنها من شركة أو مؤسسة مالية موثوقة يُطلب فيها من الضحية مشاركة معلوماته الشخصية أو اتخاذ أي إجراء آخر يمكّن المحتال من الوصول إليها.

التصيّد الاحتيالي عبر الهاتف:
يتلقى الضحية مكالمة هاتفية من شخص محتال يدّعي أنه من شركة أو مؤسسة مالية موثوقة ويطلب منه مشاركة معلوماته الشخصية أو اتخاذ أي إجراء آخر يمكّن المحتال من الوصول إليها.

التصيّد الاحتيالي عبر وسائل التواصل الاجتماعي:
يُنشأ حساب مزيف على وسائل التواصل الاجتماعي يبدو كأنه حساب رسمي لشخص أو شركة أو مؤسسة مالية موثوقة ويُطلب من خلاله من الضحية مشاركة معلوماته الشخصية أو اتخاذ أي إجراء آخر يمكّن المحتال من الوصول إليها.

تذكر!

أياً كانت الطريقة التي يتبعها المحتال فإنّ غايته سرقة أموالك أو انتحال شخصيتك لتنفيذ عمليات غير مشروعة.

Remember!

Whatever method the scammer uses, his goal is to steal your money or impersonate you to carry out illegal operations.

المؤشرات التحذيرية التي تساعدك على التعرف على محاولات التصيّد الاحتيالي

Fraud Warning signs to help you identify phishing attempts

عنوان بريد إلكتروني غير رسمي أو مكتوب بشكل سيئ

غالباً ما يستخدم المحتالون عناوين بريد إلكترونية مشبوهة تبدو وكأنها من شركة أو مؤسسة معروفة، فإذا لاحظت أنّ عنوان البريد الإلكتروني غير رسمي أو مكتوب بشكل سيئ فهذه علامة تحذيرية تشير إلى أنه محاولة احتيال.

رسالة بريدية أو نصية غير شخصية

غالباً ما تكون رسائل التصيّد الإلكتروني موجهة بشكل جماعي إلى عدد كبير من الأشخاص، فكونها عامة ولا تحتوي على أي من معلوماتك أو اهتماماتك الشخصية فهذه علامة تحذيرية تشير إلى أنها محاولة احتيال

طلب إجراء تحويل مالي أو تقديم معلومات حساسة

غالبًا ما تحاول رسائل التصيّد الإلكتروني خداعك وإقناعك بتحويل مبلغ مالي أو تقديم معلومات حساسة، مثل معلومات حسابك المصرفي أو أي معلومات شخصية أخرى. فإذا تلقيت رسالة نصية أو بريدية تطلب منك القيام بذلك، فكن حذراً.

الأخطاء الإملائية أو النحوية

غالبًا ما تكون رسائل التصيّد الإلكتروني مكتوبة بشكل سيئ ومليئة بالأخطاء الإملائية والنحوية، فإذا لاحظت أي خطأ لغوي في الرسالة، فهذه علامة تحذيرية تشير إلى أنها محاولة احتيال

رابط أو مرفق غريب

غالبًا ما تتضمن رسائل التصيّد الإلكتروني روابط أو مرفقات توجهك إلى مواقع إلكترونية وهمية أو تنزيل برامج ضارة. فإذا تلقيت رسالة بريد إلكتروني تحتوي على رابط أو مرفق مريب، فلا تنقر عليه أو تفتحه.

- تجنب إدخال معلوماتك الشخصية أو المصرفية على موقع إلكتروني لا تعرفه. وإذا كنت بحاجة إلى إدخال معلومات حساسة، فتحقق من موثوقية وأمان الموقع باستخدام شريط العناوين في متصفحك.
- احذر من الرسائل الإلكترونية الغريبة، فإذا تلقيت رسالة من شخص أو جهة لا تعرفها، فلا تفتحها، أو تنقر على روابطها، أو تقوم بتنزيل مرفقاتها.
- تحقق دائماً ما إذا كان عنوان البريد الإلكتروني المرسل صحيح أم لا.
- لا تقم بمشاركة أي معلومات سرية عبر الهاتف أو الرسائل النصية أو الرسائل الإلكترونية لأي شخص أو جهة تحت أي ظرف من الظروف..
- حماية حساب البريد الإلكتروني
- لا تفتح الروابط المرسلة عبر رسائل البريد الإلكتروني من مصادر غير معروفة.
- تجنب فتح رسائل البريد الإلكتروني على الشبكات العامة.
- لا تخزن بياناتك المالية/كلمات المرور، وما إلى ذلك في رسائل البريد الإلكتروني
- أمن كلمة المرور
- استخدم مزيجًا من الأحرف الأبجدية الرقمية والأحرف الخاصة في كلمة المرور الخاصة بك، ويجب ألا يقل طولها عن (14) حرفًا.
- احتفظ بالمصادقة الثنائية لجميع حساباتك، إذا كانت متاحة.
- غيّر كلمات المرور الخاصة بك بشكل دوري.
- تجنب اختيار أي بيانات شخصية عند اختيار كلمة المرور الخاصة بك
- مثل تاريخ ميلادك واسم أحد أفراد الأسرة.


ماذا أفعل إذا تعرضت لعمليات احتيال؟
1. قم بإبلاغ شركة مال للوساطة الرقمية فوراً وذلك من خلال:
2. الاتصال برقم الهاتف من داخل المملكة
3. الاتصال برقم الهاتف من خارج المملكة
4. رفع بلاغ احتيال من خلال الصفحة المخصصة للإبلاغ عن حالات الاحتيال التي تتطلب دعم فوري. لرفع البلاغ، اضغط هنا
What should I do if I am exposed to fraud?
1. Report the fraud to Mal Digital Brokerage Company immediately by:
2. Calling the phone number from within the Kingdom
3. Calling the phone number from outside the Kingdom
4. Submitting a fraud report through the page dedicated to reporting fraud cases that require immediate support. To submit a report, click here