البنك
السعودي
الفرنسي
Banque
Saudi
Fransi

الأمن السيبراني لا يكـون مكتمـلًا إلا بك!

الفهرس

نصائح أمنية عامة 01

• خطوات أمنية 02

• كيف تنشئ كلمة مرور قوية؟ 03

تعرف على عمليات الاحتيال والهندسة الاجتماعية 04

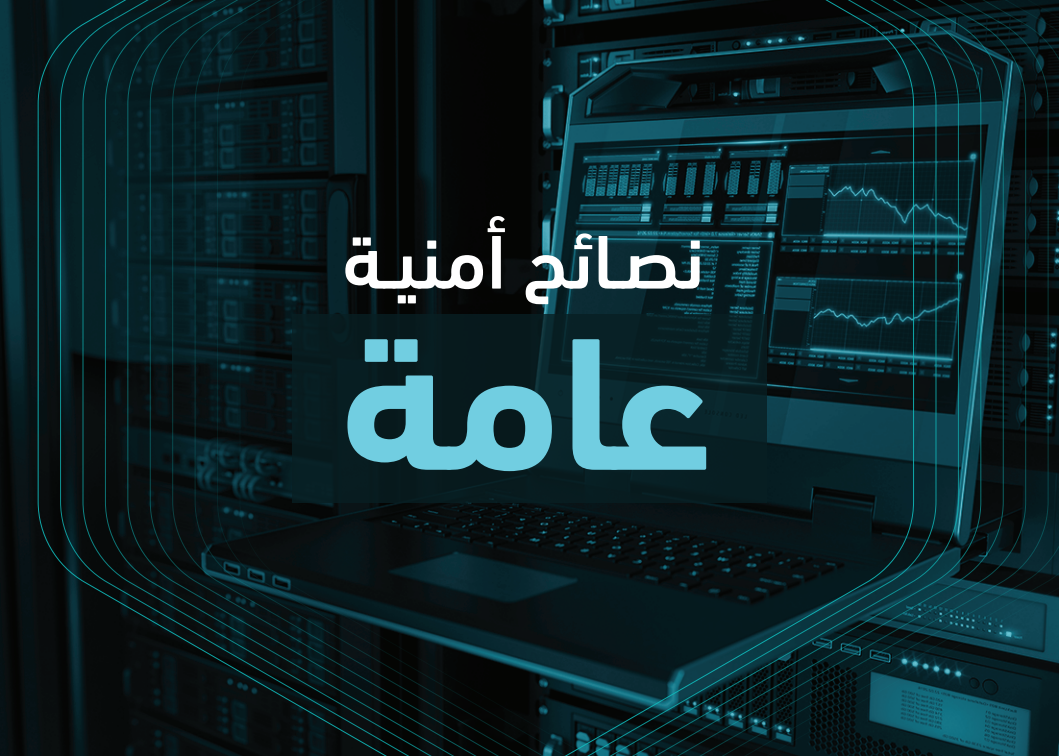
• ما هي عمليات الاحتيال (scam)؟ 05

• ما هو التصيّد الإلكتروني؟ 06

• علامات تحذيرية تساعدك في التعرف على حملات التصيد! 07

• ماذا تفعل إذا وقعت في عمليات احتيال؟ 08

• كيف تبلغ عن الأنشطة المشبوهة! 09


نصائح أمنية
عامة

النصيحة 01

خطوات أمنية

1

حدّث جميع أنظمة التشغيل لأجهزتك الإلكترونية بما في ذلك البرامج المثبتة عليها كالمتصفحات والتطبيقات ذات الأهمية كتطبيقات الخدمات المصرفية والحكومية وفق آخر تحديث رسمي من المصادر الموثوقة.

2

تجنّب استخدام أجهزة الجوال التي تم التعديل على أنظمة التشغيل فيها بطرق غير مشروعة لإزالة قيود الأمان المثبتة عليها أو ما يسمى بالـ Jailbreak أو Rooting.

3

فعّل التوثيق الثنائي المعتمد عبر استخدام جهاز المشفر أو تطبيق المشفر.

النصيحة 02

كيف تنشئ كلمة مرور قوية!

طول كلمة المرور! لتكن كلمة المرور مكونة من 8 إلى 10 أحرف على الأقل.

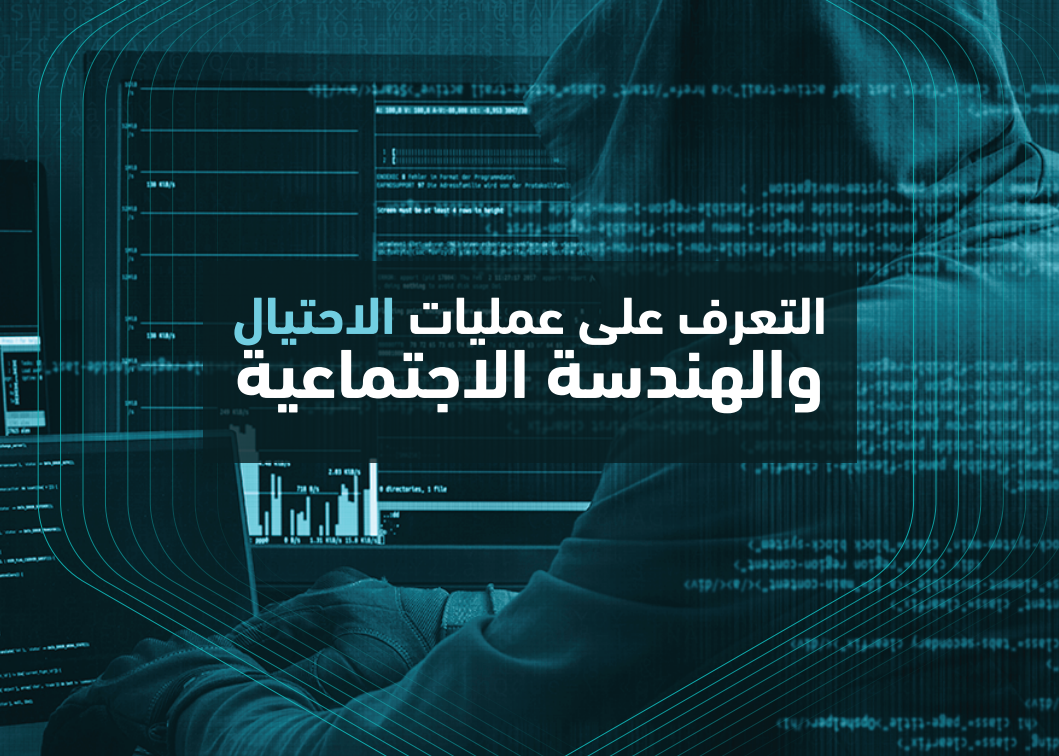
استخدام مجموعة من الرموز المتنوعة يعني كلمة مرور قوية! أضف على الأقل حرفًا كبيرًا واحدًا مع استخدام الأعداد (9-0)، وحرفًا خاصًا واحداً على الأقل مثل (@ أو # أو $ أو غير ذلك).

ليكن من الصعب تخمينها! تجنّب استخدام المعلومات الشخصية (رقم الهوية أو يوم الميلاد أو رقم الهاتف أو أسماء الزوج/الزوجة وأفراد الأسرة).

أنشئ كلمة مرور فريدة يسهل عليك تذكرها! تجنب كتابة كلمات المرور على الورق أو حفظها كنص عادي بدون تشفير على هاتفك أو حاسوبك.

الكلمات السرية ليست للمشاركة! لا تشارك أبدًا كلمات المرور مع الآخرين ولو كانوا أصدقاء أو من أفراد العائلة.

عدم تكرار كلمات المرور! في جميع التطبيقات كي لا يسهل على المحتال اختراق جميع التطبيقات


التعرف على عمليات الاحتيال
والهندسة الاجتماعية

النصيحة 01

ما هي عمليات الاحتيال (scam)؟

هي محاولة للتلاعب بشخص ما وخداعة حتى يقوم بمشاركة معلوماته الشخصية أو الإفصاح عن معلوماته السرية وذلك بقصد سرقة أمواله أو انتحال شخصيته في عمليات احتيال أخرى.

يسعى المحتالون للتواصل معك بقصد جمع معلومات عنك والحصول على معلومات سرية كاسم المستخدم أو كلمات المرور أو معلومات بطاقة الائتمان أو الصراف الآلي. ويقوم المحتالون بذلك مستخدمين أساليب مخادعة ومختلفة عبر رسائل نصية أو رسائل واتساب أو رسائل فورية زائفة، أو عبر وسائل التواصل الاجتماعي أو مكالمات الهاتف، أو حتى محاولة التواصل معك وجهاً لوجه.

النصيحة 02

ما هو التصيّد الإلكتروني؟

التصيّد الإلكتروني هو النوع الأشهر من عمليات الاحتيال الإلكترونية، وهو شكل من أشكال الرسائل الزائفة التي تدعي أنها تنتمي لجهات رسمية مثل المؤسسات الحكومية والشركات المشهورة أو الخدمات التي يشترك فيها عامة المستخدمين كخدمات البريد وخدمات التسوق الإلكتروني.

1

قد تصلك رسائل التصيّد عبر البريد الإلكتروني مع روابط للنقر عليها أو مرفقات تتضمن برمجيات خبيثة لتقوم بتحميلها.

2

قد تصلك رسائل التصيّد عبر الرسائل النصية القصيرة وتتضمن روابط للنقر عليها أو تعليمات لتتبعها

3

قد تصلك رسائل التصيّد عبر وسائل التواصل الاجتماعي، مثل تويتر وواتساب ولينكدإن وإنستغرام أو فيسبوك، بطرق احتيال مختلفة تطلب منك إرسال صورة أو معلومات بطاقة الصراف الآلي/الائتمانية أو مشاركة رمز التفعيل المؤقت المرسل إليك برسالة نصية.

النصيحة 03

علامات تحذيرية تساعدك للتعرف على حملات التصيد!

مرسل مشبوه:

رسالة آتية من رقم هاتف أو اسم حساب أو عنوان بريد إلكتروني لا تعرفه.

لغة غير مألوفة مشتملة على أخطاء نحوية:

رسالة تحتوي على أخطاء هجائية أو نحوية ولها تنسيق غير معتاد.

طلب يحثك على التصرف بطريقة عاجلة:

رسالة تحذرك بأن خدمة معينة على وشك أن تتعطل إذا لم تدفع غرامة أو تضغط على رابط على الفور!

رسالة تطلب منك مشاركة رمز التفعيل المستخدم لمرة واحدة الذي استلمته عبر الرسائل النصية أو البريد الإلكتروني على الفور لمساعدتك بخدمة أو تطبيق.

طلب غير متوقع:

رسالة تحاول إقناعك بتقديم معلومات شخصية لتصلك عروض خصم أو جوائز.

رسالة تطلب معلوماتك الشخصية لتأكيد شحنة أو طلب خدمة لم تقم بتقديم طلب عليها، ودون أي أرقام تأكيد حتى تتحقق منها!

رسالة تطلب منك قبول تحويل أموال إلى حسابك المصرفي ومنه إلى طرف آخر، مع الوعد بمنحك مبلغ مالي نظير هذه الخدمة.

رسالة تأتي من صديق أو فرد من العائلة أو شخص تعرفه تشتمل على طلب غير معتاد، مثل تحويل مال إلى شخص آخر غير معروف.

رسالة تستغل مواسم سنوية أو أحداث عالمية، مثل كوفيد-19، لتخدع الناس بمعلومات أو خدمات زائفة.

النصيحة 04

ماذا تفعل إذا تلقيت عمليات احتيال؟

1. لا تقم بالرد مطلقًا على أي رسائل إلكترونية مشبوهة أو مكالمات من مصادر غير معروفة.

2. لا تقم بمشاركة أي معلومات سرية عبر الهاتف أو الرسائل النصية أو الرسائل الإلكترونية.

3. لا تثق بالمتصل أو المرسل حتى لو زعم أنه موظف في مؤسسة موثوقة ما لم يتواصل معك من خلال أرقام الهواتف أو عناوين البريد الإلكترونية الرسمية الموثقة في موقع المؤسسة الرسمي.

4. ابحث لتتحقق من هوية المرسل، واسأل عن طريق الاتصال بالرقم الرسمي للمؤسسة أو زيارتها شخصيًا.

5. إذا كنت تعتقد أنك وقعت ضحية لعملية احتيال، أبلغ عن ذلك فوراً

النصيحة 05

كيف تبلغ عن الأنشطة المشبوهة!

إذا لاحظت أي أنشطة مشبوهة على حساباتك، أو شعرت بأنك وقعت ضحية لعملية احتيال وأرسلت أي معلومات سرية أو مصرفية للمحتالين، أبلغ عن هذا فورًا بالاتصال بفرنسي كير على:

البريد الإلكتروني :
SFLWhistle-Blowing@alfransi.com.sa

الاتصال على الرقم التالي:
0112997001