Göteborgs Stad

الأمن الرقمي

Äldre samt vård- och omsorgsförvaltningen

هل أنت أيضاً تخشى أن تتعرّض للخديعة على شبكة الإنترنت؟

الاحتيالات على الإنترنت تتزايد على نحو مستمر. وإليك نصائح هامة بكيفية حماية نفسك.

احتيالات شائعة

» **تستلم بريداً إلكترونياً بأن هناك مشكلة في حسابك** أو أنك ربحت في اليانصيب. يريد منك المُحتال أن تجيب على البريد الإلكتروني أو أن تنقر على رابط في البريد الإلكتروني وتملأ بيانات حسابك.

كيفية حماية نفسك:
قم بتمرير الفأرة على حقل العنوان فترى ما إن كان عنوان البريد الإلكتروني يبدو غريباً. احذر أن تنقر على مثل هذه الروابط، وانتبه إلى الأماكن التي تذكر فيها بيانات حسابك.

» **يتصل بك شخص ويذكر بأنه من مصلحة الضرائب** ويقول بأنك سوف تحصل على فائض الضريبة. ويطلب منك تسجيل دخولك إلى بنكك عن طريق الإنترنت.

كيفية حماية نفسك:
إذا اتصل بك شخص لا تعرفه وكنت غير متأكد: أغلق السماعة أو اطلب منه إعادة الاتصال على رقم يمكنك أن تتأكد منه بنفسك. ويسري ذلك بغض النظر عمّا إذا كان الشخص يقول بأنه أحد أقربائك أو من إحدى السلطات أو يتصل من بنك أو شركة.

» **تستلم رسالة هاتفية (إس إم إس/ sms) تبدو أنها من شركة بريد** وتطلب منك دفع رسم استلام طرد.

كيفية حماية نفسك:
لا تنقر على الرابط ولا تملأ بيانات حسابك. وإذا كنت قد طلبت طرداً فانتبه إذا ما كان يجب عليك فعلاً أن تدفع أي مبلغ.

كيفية حماية نفسك

يجب عليك حماية بيانات تسجيل الدخول

» إن كلمة السر خاصة بك ويجب عليك ألا تعطيها لأحد أبداً.

» استخدم وظيفة قفل الشاشة في هاتفك الجوال وفي كمبيوترك وفي لوح تصفّح الإنترنت، بواسطة رمز رقمي مثلاً أو نظام بصمات الأصابع.

» استخدم كلمات سر مختلفة للتطبيقات والحسابات التي عندك على شبكة الإنترنت.أمثلة عن كلمات السر الشائعة والسيئة: 1234، 9999، Pelle19، Fatima82، Tusse2

يجب عليك حماية الهوية الإلكترونية المصرفية (BankID) والبريد الإلكتروني

» لا تعطي أي شخص أبداً بيانات بطاقتك المصرفية أو رمز هويتك الإلكترونية، مثل الهوية الإلكترونية المصرفية (BankID) وغير ذلك من البيانات الأخرى الحسّاسة.

» علماً بأن البنوك والسلطات لا تقوم أبداً بالاتصال الأول عن طريق الهاتف أو رسالة هاتفية (إس إم إس) لكي تطلب منك تسجيل دخولك بواسطة الهوية المصرفية (BankID) أو بواسطة جهاز التعريف الرقمي (säkerhetsdosa).

» لا تنقر أبداً على روابط من مُرسلين مجهولين في البريد الإلكتروني أو الرسالة الهاتفية (إس إم إس). فقد يحتوي الرابط على فيروسات مؤذية.

قم دائماً بتقديم بلاغ إلى الشرطة إذا تعرّضت إلى جريمة، اتصل بالرقم 14 114.

في حال وقوع جريمة جارية، اتصل بالرقم 112.

اقرأ المزيد عن الأمان على الإنترنت

نصائح الشرطة

تقدّم الشرطة نصائح وإرشادات حول كيفية حماية نفسك من الاحتيالات الرقمية:
https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/

مزيد من النصائح من مدينة يوتيبوري

لدى مدينة يوتيبوري معلومات ونصائح لمن يريد أن يزيد من معلوماته الرقمية:
goteborg.se/blimerdigital

قم بمسح ضوئي للرمز (QR-kod) بواسطة هاتفك الجوال لكي تنتقل إلى الموقع الصحيح.

هل تريد معرفة المزيد من المعلومات؟

قم بزيارة أقرب مكتبة عامة أو مكتب خدمات المواطنين أو ملتقى (منتدى اللقاء) لكبار السنّ.

Göteborgs Stad 220308-001-160 Foto: Vladimir Voronin Tryck: Lenanders Grafiska AB April 2022