تفوق بذكائك على مجرمي الإنترنت

تفاد رسائل الاحتيال التصيدية بثلاث نصائح يسيرة

رسائل الاحتيال التصيدية من اسمها رسائل عبر الإنترنت مُصممة لتبدو أن مصدرها موثوق. لربما نقرنا على ما اعتقدناه بأنه بريد إلكتروني أو مرفق أو صورة آمنين لنفاجأ بأن أجهزتنا أصيبت ببرمجية خبيثة أو اخترقها مُحتال يريد بياناتنا الشخصية.

الخبر السار يتمثل في أنه باستطاعتنا أخذ الاحتياطات لحماية بياناتنا الشخصية. تعلم رصد عمليات التصيد والتبليغ عنها لحماية الجهزة والبيانات.

1 رصد السمات الشائعة

- لغة تتسم بإظهار الأهمية والاستعجال أو بالإثارة العاطفية
- طلبات لإرسال بيانات شخصية أو مالية
- مرفقات غير متوقعة
- روابط مختصرة غير موثوقة
- عناوين برائد إلكترونية غير متسقة مع الراسل المُفتَرَض
- ركاكة نحوية أو أخطاء إملائية (أقل شيوعًا)

2 قاوم وبَلِّغ

البريد العشوائي | الخداع الإلكتروني

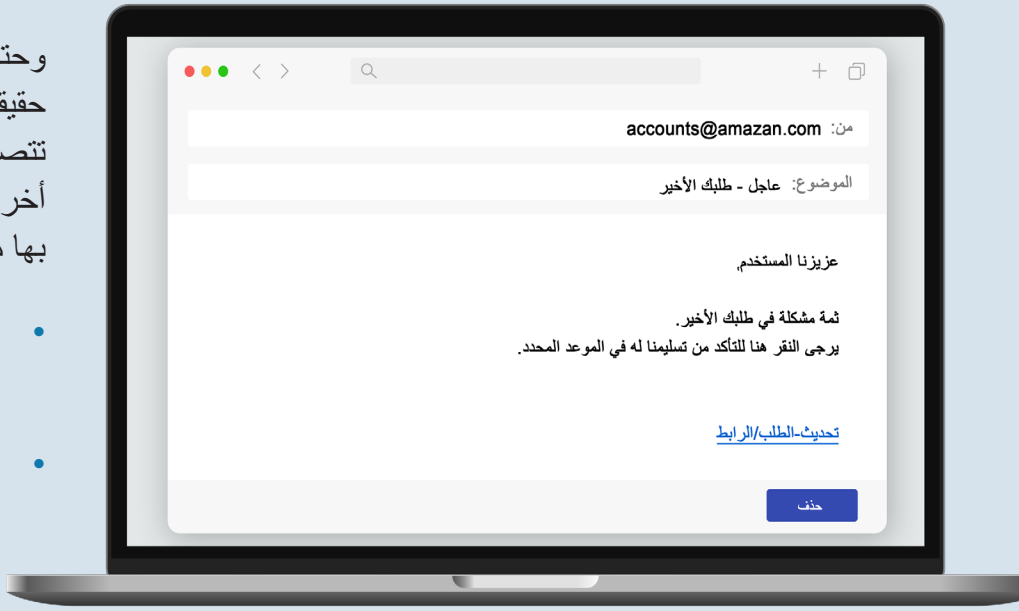
بَلِّغ عن الرسائل المشبوهة باستخدام خاصية "التبليغ عن رسالة عشوائية-report spam". إن كانت الرسالة مُصممة لتشبه منظمة موثوقة لديك، فبلِّغ عن الرسالة بتنبيه المنظمة مستخدمًا بيانات التواصل الموجودة على موقعهم الإلكتروني.

3 حذف

حذف الرسالة. لا ترد على أي رسالة أو تنقر على أي مرفق أو رابط لا سيما أي رابط "إلغاء الاشتراك". إذ إن زر إلغاء الاشتراك يحمل بدوره رابطًا يُستَخْدَم في التصيد. **احذفها فحسب.**

حذف

إن بدت أي رسالة مشبوهة لديك، فهي على الأرجح رسالة تصيدية.



وحتى إن كان ثمة احتمال بأنها قد تكون رسالة حقيقية، فلا تنقر على أي رابط أو مرفق بها أو تتصل على أي رقم تحويه. ابحث عن وسيلة أخرى للتواصل مع تلك الشركة أو شخص ما بها مباشرة:

- ادخل على موقع الشركة الإلكتروني لتحصل على بيانات الاتصال
- اتصل بالمسؤول عبر رقم رسمي وتأكد ما إذا كانوا قد أرسلوا الرسالة

إن تفادي التصيد إحدى الطرائق لتأمين عالمنا.

لكل منا مساعدة الآخر على
البقاء أمنين على الإنترنت، فشارك بهذه النصائح مع أفراد أسرتك وأصدقائك!

cisa.gov/SecureOurWorld