

التصيد الاحتيالي

نصائح عملية لتجنب الوقوع ضحية له

1

تحسيس الموظفين

تحسيس الموظفين بانتظام على أساليب التصيد وطرق الحماية منه.

10

استخدام المصادقة الثنائية

قم بتفعيل المصادقة الثنائية لتأمين الولوج الى بريدك الالكتروني.

9

التخزين الاحتياطي للمعطيات الحساسة

قم بانتظام بتخزين نسخ من معطياتك الحساسة بطريقة مؤمنة لاستعادتها عند الحاجة.

2

مكافحة التصيد

قم بتثبيت برنامج أو خدمة تقوم بحجب رسائل البريد الإلكتروني المشبوهة ومنعها.

3

تحقق من عنوان البريد الإلكتروني للمرسل

تحقق دائماً من عنوان البريد الإلكتروني للمرسل للتأكد من تطابقه مع عنوان البريد الإلكتروني الذي تتوقعه.

7

احذر من الطلبات العاجلة

احذر من رسائل البريد الإلكتروني أو الرسائل التي تطلب إجراء عاجلاً أو معلومات حساسة.

8

مراقبة الحسابات

راقب بانتظام الحسابات المصرفية والحسابات عبر الإنترنت بحثاً عن أي نشاط مشبوه.

4

كن حذراً من الروابط

لا تنقر أبداً على الروابط في رسائل البريد الإلكتروني المشبوهة.

5

تحديثات البرامج

حافظ على تحديث مضاد الفيروسات والبرمجيات وأنظمة التشغيل والمتصفحات بأحدث التحديثات الأمنية.

6

التحقق من عنوان URL وشهادة SSL لمواقع الويب

قبل إدخال المعلومات الحساسة، تحقق من عنوان URL للموقع الإلكتروني للتأكد من مصداقيته وذلك بالاستعانة بمتصفح الويب وكذلك بمحرركات البحث.