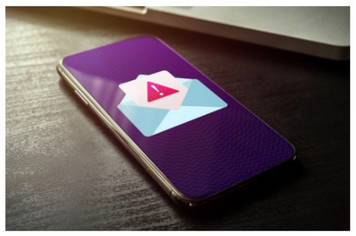
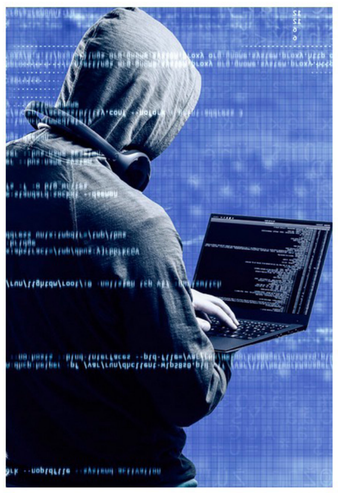
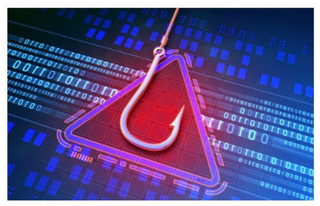
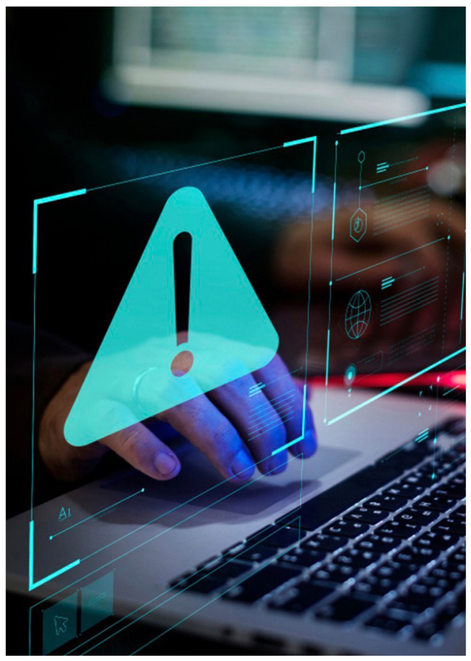
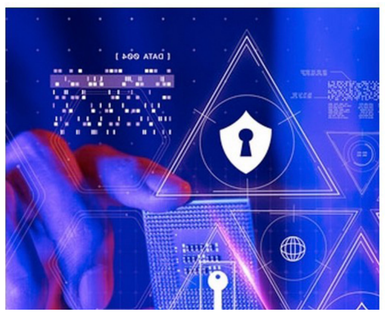
آمن وسليم: خطوات الأمان لضمان سلامتك











يمكن لأي شخص أن يكون ضحية للاحتيال. مع تزايد استخدامنا للإنترنت، أصبحت عمليات الاحتيال عبر البريد الإلكتروني (التصيد) تهديدًا شائعًا.

مواضيع ذات صلة

لقد قامت ديم بتنفيذ عدة تدابير أمنية لحماية حساباتك، ولكن يمكنك أيضًا حماية حساباتك من خلال الحفاظ على سرية بيانات اعتمادك واتباع النصائح التالية:

- لا تشارك أبداً كلمة مرور تطبيق ديم على هاتفك المحمول.
- تذكر دائماً أن ديم لن تطلب منك أبداً كلمة المرور أو الرقم السري (PIN) أو رقم CVC أو رمز OTP عبر الهاتف أو البريد الإلكتروني.
- تجنب استخدام كلمات مرور بسيطة أو أرقام مرتبطة بتواريخك الشخصية، مثل تاريخ ميلادك.
- قم بتعيين كلمات مرور قوية وقم بتغيير كلمات المرور والرموز السرية بانتظام.
- لا تنسَ مسح سجل كلمات المرور بعد استخدام الحواسيب العامة.
- لا تكتب كلمة المرور على الورق أو في البريد الإلكتروني أو في رسالة نصية، ولا تشارك هويتك مع أي شخص.
- تجنب استخدام الشبكات العامة غير المؤمنة وفضل استخدام شبكات الواي فاي الموثوقة بدلاً منها.
- احذر من الروابط التي تطلب تفاصيل بطاقة الائتمان على المواقع التي لا تثق بها.
- حافظ دائمًا على أمان بطاقتك الائتمانية، حيث يمكن نسخها بسهولة.
- تجاهل أي رسائل بريد إلكتروني تطلب تفاصيل حسابك.
- لا تشارك تفاصيل حسابك عبر مكالمة هاتفية.
- لا توقع شيكًا فارغًا.
- كن حذرًا من محيطك عند إدخال الرقم السري في جهاز الصراف الآلي أو لوحة مفاتيح جهاز نقاط البيع وتأكد من عدم وجود أجهزة إضافية ملتصقة بمنفذ قارئ البطاقة أو لوحة المفاتيح.

اكتب لنا للإبلاغ عن الاحتيال:

إذا لاحظت أي نشاط غير قانوني أو احتيالي (مثل خرق سلوكيات ديم المهنية، تدابير غير أخلاقية، جريمة جنائية أو خرق لأي قانون، أي فعل غير شريف أو محاولة فعل غير شريف، إلخ) يتضمن ديم أو موظفي ديم، يرجى ملء النموذج أدناه أو إرسال بريد إلكتروني إلى fraudalert@deem.io مع تفاصيل قلقك وإرفاق جميع المستندات الداعمة. يمكنك أيضًا الاتصال بمركز الاتصال لدينا المتاح على مدار الساعة طوال أيام الأسبوع على الرقم +971600525550