Australian Banking Association

# حافظوا على سلامتكم:
# كونوا على معرفة بعمليات الاحتيال والغش

**من المرجح أن تزداد عمليات الاحتيال والغش التي تتمحور حول كوفيد-19 خلال الأشهر القادمة.**

**حيث يستخدم المحتالون رسائل البريد الإلكتروني أو المكالمات الهاتفية أو الرسائل النصية المُزيّفة بهدف الحصول على المعلومات الشخصية. فهم يتظاهرون بأنهم من المصرف الذي تتعاملون معه، أو من منظمة الصحة العالمية، أو الحكومة، أو المؤسسات الخيرية، أو الأعمال التجارية الشرعية مثل وكلاء السفر، أو شركة الكهرباء أو الهاتف أو مزوّدي الإنترنت أو السوبر ماركت المحلي.**

## احموا أنفسكم

لن يقوم المصرف الذي تتعاملون معه أبدًا بإرسال بريد إلكتروني أو رسالة نصية يطلب فيها معرفة التفاصيل حول أي حساب أو تفاصيل مالية، وهذا يشمل تحديث عنوانكم أو تفاصيل تسجيل الدخول الخاصة بكم عبر الهاتف أو الهاتف المحمول/الموبايل أو الخدمات المصرفية عبر الإنترنت.

لن تطلب منكم الحكومة والمنظمات الشرعية الأخرى أبدًا تحديث تفاصيلكم بالنقر على أحد الروابط. إذا كانت لديكم أي شكوك، فتحدثوا إلى صديق أو أحد أفراد العائلة، أو اتصلوا بالمنظمة مباشرة واسألوها.

إذا تلقيتم مكالمة هاتفية من شخص لا تعرفونه يطلب منكم معلومات شخصية، فقوموا بإقفال الخط. اتصلوا بالشركة مباشرة وتحققوا مما إذا اتصلوا بكم.

لا تفتحوا أبدًا المُرفقات من الأشخاص أو المنظمات التي لا تعرفونها. احذروا دائمًا من العروض التي تفوق حدّ التصديق أو التي تطلب معلومات أكثر من اللازم.

## يمكن لمصرفكم المساعدة، اتصلوا به على الفور إذا:

- شاركتم تفاصيلكم المصرفية استجابةً لمكالمة هاتفية أو بريد إلكتروني أو رسالة نصية خادعة
- نقرتم من غير قصد على أي روابط أو قمتم بتنزيل أي مُرفقات
- لاحظتم أي معاملات غير عادية على حساباتكم.

## كيفية اكتشاف عملية احتيال

- يُطلب منكم تحديث أو تأكيد تفاصيلكم الشخصية، بما في ذلك العنوان وتاريخ الميلاد وتفاصيل الحساب المصرفي ورقم الملف الضريبي أو أي رقم تعريف شخصي أو كلمة سر.
- يحتوي البريد الإلكتروني أو الرسالة النصية على روابط مشكوك فيها. إذا كنتم غير متأكدين، فاطلبوا المساعدة من صديق أو أحد أفراد العائلة.
- يُطلب منكم أن تدفعوا على الفور أو تدفعوا عربون/وديعة مُقدّمًا.
- إذا كان العرض يفوق حدّ التصديق، فربما هو كذلك.
- لا يتطابق عنوان البريد الإلكتروني مع الشركة.
- يطلب المتصل بكم الوصول إلى جهاز الكمبيوتر الخاص بكم والتحكّم به عن بُعد.

Australian Banking Association

www.ausbanking.org.au

## أهم النصائح لحماية معلوماتكم المالية من عمليات الاحتيال والغش

- أقفلوا الخط إذا كانت المكالمة الهاتفية مشبوهة، وبدلاً من ذلك اذهبوا إلى موقع الشركة الإلكتروني أو ابحثوا عن رقم هاتفها واتصلوا بها مباشرةً.
- لا تشاركوا أبدًا كلمات السر أو أرقام التعريف الشخصية. احموا أجهزتكم باستخدام كلمة سر. إذا كنتم تستخدمون جهاز كمبيوتر مشترك، فلا تقوموا أبدًا بحفظ كلمات السر وقوموا بتسجيل الخروج دائمًا من حسابكم.
- تحققوا بانتظام من حساباتكم المصرفية حتى تلاحظوا المعاملات المشبوهة بسرعة.
- تجنبوا تمرير بطاقتكم المصرفية لإجراء عمليات الشراء. غالبًا ما يكون نقر البطاقة وإدخالها أكثر أمانًا.
- قوموا بحظر السلفة النقدية على بطاقات الائتمان.
- تحدثوا مع المصرف الذي تتعاملون معه حول أفضل طريقة لحماية حسابكم.
- إذا كنتم تعتقدون أنه تم خداعكم، قوموا بإبلاغ المصرف على الفور.

## هناك العديد من الوسائل التي سيحاول المحتالون استخدامها لسرقتكم، وإليكم الوسائل الرئيسية.

**التصيد الاحتيالي –** يتم استخدام بريد إلكتروني أو رسالة نصية للحصول على معلوماتكم الشخصية من خلال التظاهر بأنهم من مصدر موثوق به مثل مصرف أو مؤسسة خيرية أو الحكومة. تبدو الرسالة صادقة وستطلب منكم غالبًا إدخال معلوماتكم الشخصية على مواقع إلكترونية مزيّفة أو تطلب منكم النقر فوق رابط - وهذا سيسمح للمحتال بالوصول إلى جهاز الكمبيوتر الخاص بكم ومعلوماتكم الشخصية.

**حيل التسوّق عبر الإنترنت –** يتظاهر المحتالون بأنهم متاجر حقيقية عبر الإنترنت، إما من خلال موقع إلكتروني مزيّف أو إعلان زائف على موقع إلكتروني حقيقي لأحد المحلات التجارية. غالبًا ما تطلب مواقع التسوّق المزيّفة عبر الإنترنت الدفع بطرق غير عادية مثل الدفع مُقدّمًا عن طريق حوالة بريدية أو تحويل إلكتروني أو تحويل أموال دُوليًا أو بطاقات هدايا.

**عمليات الاحتيال الاستثمارية –** يدعي المخادع أنه وسيط مالي أو مدير سندات تجارية يقدّم نصائح مالية أو استثمارية. وسيطلب منكم إعطاؤه الأموال لفرصة استثمارها وقد تكون أو لا تكون حقيقية، ثم يحتفظ بأموالكم.

**حيل التحكّم عن بعد –** سيزعم المخادع أن هناك عطل ما في جهاز الكمبيوتر أو الإنترنت، أو أن فيه برامج ضارة. وسيحاول إقناعكم بتثبيت تطبيق أو منحه حق الوصول إلى جهاز الكمبيوتر الخاص بكم. وسيستخدم هذا للوصول إلى معلوماتكم الشخصية أو طلب "رسوم" لحلّ المشكلة.

**حيل المواعدة وإقامة العلاقات –**يُقيم المخادع علاقة معكم لأخذ الأموال أو الهدايا. فهو يطوّر العلاقة بمرور الوقت وقد يطلب منكم نقل الممتلكات إلى إسمه أو يطلب منكم أن يصبح أحد المستفيدين في وصيّتكم. غالبًا ما يطلب المال لحل مشكلة صحية أو عائلية أو بهدف السفر.

## روابط مفيدة:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/

**ملاحظة مهمة:** تقدّم صحيفة الحقائق هذه معلومات ذات طبيعة عامة وليس المقصود منها الاعتماد عليها كنصيحة في أي مسألة مُعيّنة. يجب عليكم الاتصال بالمصرف الذي تتعاملون معه لمعرفة كيف تنطبق هذه المعلومات على ظروفكم.