عمليات الاحتيال ومشروعك الصغير:

دليل للأعمال التجارية

Arabic

عندما يستهدف المحتالون عملك التجاري أو مؤسستك غير الربحية، فقد يؤدي ذلك إلى التأثير سلبًا على سمعتك وأرباحك. فما أفضل حماية بالنسبة لك؟ تعرّف على العلامات التي تدل على عمليات الاحتيال التي تستهدف الأعمال التجارية. وبعد ذلك، أخبر موظفيك وزملاءك بهذه العلامات لكي يتمكنوا من تجنب عمليات الاحتيال.

تكتيكات المحتالين

- **المحتالون يتظاهرون بأنهم شخص موثوق.** ينتحلوا صفة شركة أو وكالة حكومية تعرفها ليقنعوك بالسداد لهم. ولكنها عملية احتيال.
- **المحتالون يدفعونك للشعور بوجود ضرورة ملحة ويلجؤون إلى ترهيبك وتخويفك.** فهدفهم هو دفعك للتصرف قبل أن تحظى بفرصة للتأكد من مزاعمهم. لا تسمح لأحد باستعجالك للسداد أو الإفصاح عن معلومات حساسة حول عملك التجاري.
- **يطلب المحتالون منك السداد بطرق محددة.** فغالبًا ما يطالبون بالسداد من خلال الحوالات المصرفية أو العملات المشفرة أو بطاقات الهدايا. لا تدفع المال لأي شخص يطالبك بالسداد بهذه الطريقة. فهي عملية احتيال.

احم عملك التجاري

درب موظفيك

- أفضل وسيلة للدفاع هي تحصين موظفيك بالمعلومات. درب الموظفين على عدم إرسال كلمات مرور أو المعلومات الحساسة عبر البريد الإلكتروني، حتى لو بدا أن المدير هو من أرسل البريد الإلكتروني. اشرح لموظفيك كيفية حدوث عمليات الاحتيال وشجعهم على التحدث مع زملائهم في العمل إذا اشتبهوا في حدوث عملية احتيال. اطلب نسخًا مجانية من هذا الكتيب على **ftc.gov/bulkorder** وشاركها مع موظفيك.

تحقق من الفواتير وعمليات الدفع

- تأكد من أن الإجراءات واضحة للموافقة على المشتريات والفواتير واطلب من موظفيك التحقق من جميع الفواتير بشكل مكثف. انتبه إلى الوسيلة التي يطلب منك الأشخاص السداد بها وأخبر موظفيك أن يفعلوا الشيء نفسه. إذا طلب منك أحد الأشخاص أن تدفع من خلال حوالة مصرفية أو عملة مشفرة أو بطاقات هدايا، فلا تدفع. فهي عملية احتيال.

اكتشاف عمليات الاحتيال المتعلقة بالتقنية

- غالبًا ما يُزَوِّر المحتالون أرقام هواتفهم، فلا تثق في معرف المتصل. إذا تلقيت رسالة نصية أو بريدًا إلكترونيًا غير متوقع، فلا تضغط على أي رابط أو تفتح المرفقات أو تنزل الملفات. هذه هي الطريقة التي يلجأ إليها المحتالون لتحميل البرامج الضارة على شبكتك أو محاولة إقناعك بإرسال الأموال أو مشاركة المعلومات الحساسة. في بعض الأحيان، يخترق المحتالون حسابات وسائل التواصل الاجتماعي

- للأشخاص الذين تعرفهم، ويرسلون رسائل تبدو حقيقية - لكنها ليست كذلك. تعرّف على المزيد حول حماية مشروعك الصغير أو مؤسستك غير الربحية من محتالي الإنترنت والمتسللين: اطلع على الأمن **السيبراني للمشروعات الصغيرة على الموقع ftc.gov/cybersecurity**.

تحقق من هوية الأشخاص الذين تتعامل معهم

- قبل التعامل مع شركة جديدة، ابحث عن اسم الشركة على الإنترنت وضع إلى جانبه كلمة "احتيال" أو "شكوى". اقرأ ما يقوله الآخرون عن تلك الشركة. اسأل الأشخاص الذين تثق بهم للحصول على توصيات. ويمكنك أيضًا الحصول على نصائح واستشارات مجانية حول تطوير الأعمال من خلال برامج مثل **SCORE.org**.

◀ عمليات الاحتيال الشائعة التي تستهدف المشروعات الصغيرة

الفواتير المزيفة والسلع التي لم يتم طلبها

يقوم المحتالون بإنشاء فواتير مزيفة تبدو وكأنك طلبت منتجات أو خدمات لنشاطك التجاري. ويأملون أن يفترض الشخص الذي يدفع فواتيرك أن الفواتير حقيقية ويقوم بالسداد. ولكنها فاتورة مزيفة. أو قد يتصل محتال مدعيًا أنه يريد "تأكيد" طلب أو "التحقق" من عنوان أو تقديم كتالوج أو عينة "مجانية". إذا وافقت على أي من هذه الأمور، فستصلك سلع لم تطلبها تليها مطالب شديدة الإلحاح لدفع ثمنها. لا تقم بالسداد. وتذكر، إذا تلقيت سلعة لم تطلبها، فلديك الحق القانوني في الاحتفاظ بها واستخدامها مجانًا.

عمليات الاحتيال المتعلقة بقوائم الشركات والإعلانات عبر الإنترنت

يحاول المحتالون خداعك لدفع ثمن إعلان غير موجود أو إدراج شركتك في دليل أعمال مزيف. وقد يطلبون منك منحهم معلومات الاتصال الخاصة بك لإدراج شركتك في قائمة "مجانية"، أو يقولون إن الغرض من المكالمة هو "تأكيد" معلوماتك. ستصلك بعد ذلك فاتورة باهظة، وقد يستخدم المحتال تفاصيل المكالمة السابقة - أو حتى تسجيلها - للضغط عليك للدفع.

عمليات الاحتيال التجارية وانتحال الصفة الحكومية

يتظاهر المحتالون بأنهم شخص تعرفه أو تثق به ويحاولون إخافتك أو دفعك إلى الدفع أو إعطائهم معلومات. على سبيل المثال:

- يقول المحتالون إنهم يتصلون من شركة مرافق وأن خدمة الغاز أو الكهرباء أو المياه على وشك الانقطاع بسبب التخلف عن سداد فاتورة (وهمية).
- يقول المحتالون إنهم موظفون حكوميون ويهددونك بتعليق تراخيص عملك أو تغريمك أو حتى مقاضاتك. وقد يقولون إنك مدين بدفع ضرائب أو عليك تجديد ترخيص أو تسجيل.
- يقنعك بعض المحتالين بشراء ملصقات الامتثال الخاصة بمقر العمل والتي يمكنك الحصول عليها مجانًا من وزارة العمل الأمريكية.

- يخدعك بعض المحتالين للسداد مقابل التقدم للحصول على ما يزعمون أنها منح للأعمال التجارية من البرامج الحكومية، ويتضح بعد ذلك أنها مزيفة.
- ينتحل المحتالون صفة مكتب الولايات المتحدة لبراءات الاختراع والعلامات التجارية ويهددونك بأنك ستفقد علامتك التجارية إذا لم تدفع رسومًا على الفور. وفي أحيان أخرى، يكذبون ويقولون إنك مدين بالمال مقابل خدمات التسجيل الإضافية.
- يقول بعض المحتالين إنهم يتصلون من شركة تقنية، ويهددونك بأن نشاطك التجاري سيفقد عنوان URL للموقع الإلكتروني إذا لم تسدد على الفور.

عمليات الاحتيال المتعلقة بالدعم الفني

تبدأ عمليات الاحتيال المتعلقة بالدعم الفني بمكالمة أو رسالة منبثقة على شاشتك. يتظاهر المحتالون بأنهم يعملون في شركة تقنية معروفة، ويخبرونك أن هناك مشكلة تتعلق بأمان جهاز الكمبيوتر لديك. ويكون هدفهم هو الحصول على أموالك أو الدخول إلى جهاز الكمبيوتر لديك أو القيام بالأمرين معًا. قد يطلبون منك الدفع لإصلاح مشكلة ليست لديك فعليًا أو تسجيل عملك التجاري في برنامج غير موجود أو عديم الفائدة لصيانة الكمبيوتر أو يتسللون إلى شبكة الكمبيوتر الخاص بك للحصول على بيانات سرية يمكنهم استخدامها في سرقة الهوية.

الهندسة الاجتماعية والتصيد الاحتيالي وبرامج الفدية

يمكن للمحتالين على الإنترنت خداع الموظفين لدفعهم لإرسال الأموال إليهم أو الإفصاح عن معلومات سرية أو حساسة، مثل كلمات المرور أو المعلومات المصرفية. وغالبًا ما تبدأ عملية الاحتيال برسالة بريد إلكتروني للتصيد الاحتيالي أو بجهة اتصال على وسائل التواصل الاجتماعي أو مكالمة يبدو أنها تأتي من مصدر موثوق - مشرف أو موظف آخر كبير على سبيل المثال — ما يؤدي إلى الشعور بالتعجل أو الخوف. وقد تبدو رسائل البريد

الإلكتروني الأخرى كطلبات روتينية لتحديث كلمة المرور أو رسائل آلية أخرى، ولكنها في الواقع محاولات لسرقة معلوماتك. ويمكن للمحتالين استخدام البرامج الضارة أيضًا لقفل ملفات المؤسسات والمطالبة بالحصول على فدية.

عمليات الاحتيال المتعلقة بالتدريب التجاري

يبيع بعض المحتالين برامج تدريب تجارية مزيفة، وغالبًا ما يستخدمون شهادات ومقاطع فيديو وعروضًا تقديمية مزيفة ويلجأون إلى مكالمات التسويق عبر الهاتف. ويعدونك كذبًا بالحصول على نتائج مذهلة إذا دفعت مقابل نظامهم "المثبت" والحصري للنجاح في العمل. وقد يستدرجك المحتالون أيضًا من خلال التكاليف الأولية المنخفضة، ليطلبوا آلاف الدولارات بعد ذلك. ما يحدث في الواقع هو أن المحتالين لا يقدمون لرواد الأعمال المبتدئين المساعدة التي حاولوا الحصول عليها ويكون عليهم تحمل عبء آلاف الدولارات من الديون.

تغيير التقييمات عبر الإنترنت

يزعم بعض المحتالين أن بإمكانهم استبدال التقييمات السلبية لمنتجك أو خدمتك أو إضافة تقييمات إيجابية أو تعزيز درجاتك على مواقع التقييم. ولكن نشر التقييمات الزائفة غير قانوني. تنص إرشادات FTC على أن الدعم - بما في ذلك التقييمات - يجب أن يعكس الآراء والتجارب الصادقة للداعم.

عمليات الاحتيال المتعلقة بمعالجة بطاقة الائتمان وتأجير المعدات

يعد بعض المحتالين بالحصول على أسعار منخفضة لمعالجة معاملات بطاقات الائتمان أو تأجير المعدات. يلجأ هؤلاء المحتالون إلى الطباعة الدقيقة وعدم ذكر الحقائق كاملة والأكاذيب الصريحة للحصول على توقيع صاحب العمل على العقد. يطلب بعض وكلاء المبيعات معدومي الضمير من أصحاب الأعمال التوقيع على مستندات فارغة. (لا تفعل ذلك) فمن المعروف أنه يتم تغيير البنود بعد ذلك. واطلب من مندوب المبيعات أن يعطيك نسخًا من جميع المستندات في حينه. فإذا رفض أو أجّل الأمر بوعدك بإرسالها لاحقًا ، فقد تكون هذه علامة على أنك تتعامل مع محتال.

عمليات الاحتيال المتعلقة بالشيكات المزيفة

يمنحك بعض المحتالين ما يبدو وكأنه سبب معقول لسداد مبالغ زائدة لك باستخدام شيك. ثم يطلبون منك بعد ذلك إعادة الأموال الإضافية إليهم أو إلى شخص آخر. لكن الشيك سيكون مزيفًا، على الرغم من أنه قد يظهر على أنه قد تم إجراء "مقاصة" له في حسابك. وعندما يدرك البنك أن الشيك كان مزيفًا، يكون المحتال قد حصل بالفعل على الأموال التي أرسلتها إليه. وسيكون عليك السداد للبنك.

◄ الممارسات المريبة الأخرى

في بعض الأحيان، يلجأ المحتالون إلى ممارسات أخرى مريبة، مثل ادعاء توفير وظائف بدوام جزئي ذات عائد ضخم، ولكنهم لا يوفون بوعودهم بكسب المال. أو قد يحاول المحتالون بيعك خدمات غير ضرورية بمزاعم كاذبة بأن عليك الدفع لهم لتحسين التقرير الائتماني لنشاطك التجاري. وبعد وقوع الكوارث الطبيعية، قد يظهر المتعاقدون والمحتالون غير المرخص لهم بوعود كاذبة بأنهم سيعيدون مشروعك إلى العمل من خلال الإصلاحات السريعة أو التنظيف أو إزالة الحطام ولا يوفون بوعودهم أبدًا.

اعرف المزيد

- للاطلاع على المزيد من النصائح حول حماية مؤسستك من عمليات الاحتيال، تفضل بزيارة **ftc.gov/SmallBusiness**.
- يمكنك البقاء على تواصل مع FTC من خلال الاشتراك في مدونة أعمال FTC على الرابط التالي **ftc.gov/subscribe**.

الإبلاغ

- إذا اكتشفت عملية احتيال، فاتصل بالرقم 877-382-4357، ثم اضغط على 3 للغات الأخرى، ثم 5 للغة العربية — أو تفضل بزيارة الموقع **ReportFraud.ftc.gov**.
- قم بتنبيه المدعي العام لولايتك. يمكنك العثور على معلومات الاتصال على **NAAG.org**.

شارك

- تذكّر: أفضل وسيلة للدفاع هي تحصين موظفيك بالمعلومات. تحدث إلى موظفيك حول كيفية حدوث عمليات الاحتيال.
- شارك هذا الكتيب مع موظفيك.
- يمكنك طلب نسخ مجانية من هذا الكتيب باللغة الإنجليزية على **ftc.gov/bulkorder** وباللغة الإسبانية على **ftc.gov/ordenar**.

نبذة حول لجنة التجارة الفيدرالية (FTC)

تعمل لجنة التجارة الفيدرالية (FTC) على مساعدة أصحاب المشروعات الصغيرة على تجنب عمليات الاحتيال وحماية أجهزة الكمبيوتر والشبكات والحفاظ على أمان بيانات العملاء. للحصول على معلومات حول المشروعات الصغيرة، تفضل بزيارة الموقع **ftc.gov/SmallBusiness.** ستجد معلومات حول عمليات الاحتيال التي تستهدف المشروعات الصغيرة وكيفية تجنبها، ومعلومات حول الأمن السيبراني للمشروعات الصغيرة لمساعدة أصحابها في الحفاظ على أمان شبكاتهم.

للحصول على أحدث المعلومات حول المشروعات الصغيرة، اشترك في مدونة الأعمال التابعة للجنة التجارة الفيدرالية (FTC) على الرابط التالي **ftc.gov/subscribe.**

This brochure is part of the FTC's efforts to help small business owners avoid scams. It explains common scams that target small businesses and non-profit organizations, describes scammers' tactics, and provides steps business owners can take to protect their company from scams. Order print copies for free at **ftc.gov/bulkorder**.

FEDERAL TRADE COMMISSION

business.ftc.gov

2023 يوليو