



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

كتيب الشركات الصغيرة

تم إنشاء هذا الدليل لمساعدة الشركات الصغيرة في الدفاع عن نفسها ضد الهجمات السيبرانية الأكثر شيوعًا قم بالاطلاع على النصائح الإرشادية للأمان في هذا الدليل لحماية مشروعك من المخاطر.



ما مدى جاهزية مشروعك للتصدي
للتحديات السيبرانية الشائعة

الفهرس	
01	01 حماية البيانات باستخدام كلمات المرور
02	02 النسخ الاحتياطي للبيانات/المعلومات الخاصة
03	03 هجمات التصيد وكيفية تجنبها
04	04 منع البرامج الضارة
05	05 حماية الهواتف الذكية (والأجهزة اللوحية)
06	06 جمع السجلات الأمنية



النسخ الاحتياطي للبيانات/ المعلومات الخاصة



قم بعمل نُسخ احتياطية بانتظام للمعلومات المهمة وتحقق من إمكانية استعادتها، حيث سيؤدي ذلك إلى تقليل التأثير الناجم من فقدان البيانات بسبب السرقة أو الحريق أو أي أضرار مادية أخرى، بالإضافة إلى المخاطر الناتجة. من برامج الفدية.

لضمان بقاء بيانات العملاء/البيانات الهامة بأمان وحمايتها من أن يتم العبث بها، يُنصح بتشفير النسخ الاحتياطية/القرص الصلب المخصص للنسخ الاحتياطي.

يجب تحديد ما يستوجب حفظه كنسخة احتياطية. عادةً ما يتم الاحتفاظ بالمستندات والصور ورسائل البريد الإلكتروني وجهات الاتصال والتقويمات في بضع المجلدات المشتركة. اجعل من عملية النسخ الاحتياطي جزءًا منتظمًا من روتينك من خلال تفعيل خاصية النسخ الاحتياطي التلقائي.

عندما تستخدم جهاز حفظ الذاكرة الخارجي (الهاردسك ذو وصلة ال USB) لعمل النسخ الاحتياطي، فيجب التأكد من أن الجهاز الذي يحتوي على النسخ الاحتياطية يكون مفصلاً تماماً عن الجهاز الذي يحتوي على النسخة الأصلية عندما لا تقوم بعملية النسخ.

حماية البيانات باستخدام كلمات المرور



تجنب استخدام كلمات مرور يسهل تخمينها (مثل أسماء أفراد العائلة أو الحيوانات الأليفة أو تواريخ الميلاد). ضع في اعتبارك بأنه ليس كل كلمات المرور المعقدة توفر الحماية وذلك لأنها معروفة ومتداولة على نطاق واسع كما إنها ليست فريدة، مثل P@ssw0rd أو Abc@123

إذا كان هنالك شك في أن شخصًا آخر يعرف كلمة المرور أو تم ملاحظة أي نشاط مريب على حسابك، فاحرص على تغيير كلمة المرور على الفور وإخطار قسم تقنية المعلومات أو بإشعار المعنيين معك بذلك.

استخدم دائماً المصادقة الثنائية (2FA) على جميع الحسابات.

عند إعداد أجهزة جديدة (مثل جهاز الراوتر أو البصمة، إلخ..) في بيئة العمل، قم بتغيير كلمات المرور الافتراضية أو إعدادات المصنع الافتراضية التي حدتها الشركة المصنعة قبل توفير الاتصال أو استخدام تلك الأجهزة من قبل الموظفين.

فكر في استخدام تطبيق لإدارة كلمات المرور، وهي عبارة عن برامج تنشئ وتخزن كلمات المرور وتمنحك الوصول إليها من خلال كلمة مرور رئيسية. ونظرًا إلى أن كلمة المرور الرئيسية تحمي جميع كلمات المرور الأخرى، فلا تنسى أن تجعلها قوية وفريدة حيث يجب عدم استخدام كلمات المرور القديمة (أو المخترقة) لكلمات المرور الرئيسية أبدًا.

لحماية بيانات العميل بشكل أفضل، تأكد من استخدام منتجات التشفير على أجهزة الحاسوب المحمولة والشخصية حيث تعتبر هذه البيانات بيانات تشغيل يومية.



منع البرامج الضارة



من خلال تنفيذ ما يلي، بالإمكان حماية مشروعك من الضرر الناجم عن "البرامج الضارة"

يجب الحرص على تثبيت برامج موثوقة لمكافحة الفيروسات على جميع الخوادم وأجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة ويجب تثبيت البرامج المعتمدة فقط على الأجهزة اللوحية والهواتف الذكية، كما يجب على المستخدمين تجنب تحميل تطبيقات الطرف الثالث من مصادر غير معروفة.

قم بالتأكد من تحديث نظام التشغيل وبرنامج التطبيق وقم بتفعيل خاصية "التحديث التلقائي".

يمكن الحد من استخدام الوسائط القابلة للإزالة مثل بطاقات USB و SD وإيصالها على أجهزة الكمبيوتر والخوادم استخدم طرق أكثر أماناً لتبادل الملفات والمجلدات وقم بتطبيق إجراءات الأمان المطلوبة.

إن لم يكن هناك جدار حماية يوفره برنامج مكافحة الفيروسات أو مثبناً على الشبكة، فيجب التأكد من إبقاء جدار حماية نظام التشغيل على جهازك "قيد التشغيل" لأنه يعمل كحاجز بين النظام والاتصالات الضارة الخارجية.

هجمات التصيد وكيفية تجنبها

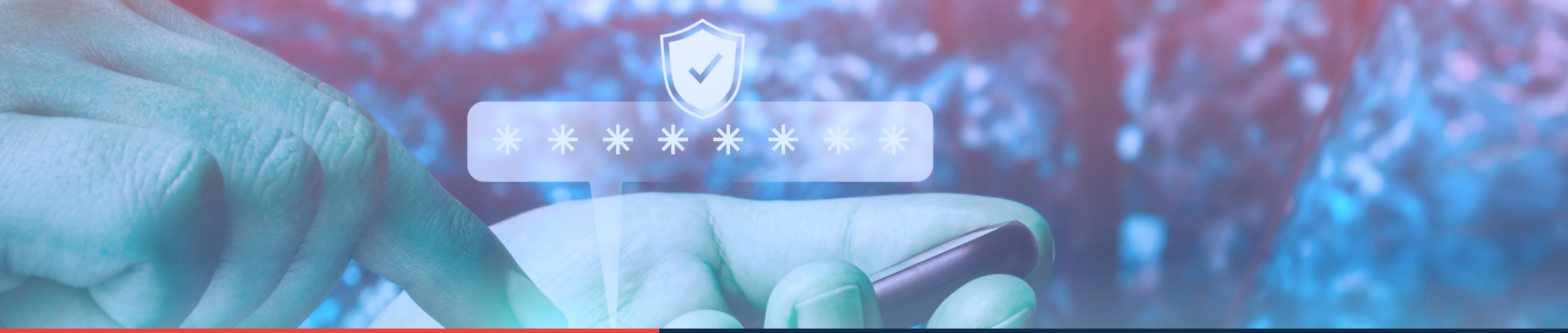


يستخدم المخترق أساليب الهندسة الاجتماعية لتنفيذ هجمات التصيد الاحتيالي من خلال إرسال رسائل البريد الإلكتروني، أو ومن خلال وسائل التواصل الاجتماعي أو الرسائل النصية القصيرة. وبالرغم بأن أساليب الاحتيال مكررة إلا أن المخترقين يزدادون مهارة في طرق إنشاء وإرسال المستندات مزيفة، ورسائل البريد الإلكتروني والمرفقات والتعليمات التي تبدو وكأنها طبق الأصل.

إذا شككت بأن الجهاز مخترق، فقم بالمسح الأمني والكشف عن البرامج الضارة وقم بتغيير كلمات المرور في أسرع وقت ممكن شجع الموظفين على الإبلاغ عن الحوادث السيبرانية أو الأنشطة المشبوهة.

قم بالتعرف على العلامات المحتملة على التصيد الاحتيالي. الاستدلالات قد تكون أخطاء إملائية والنحوية أو الإصدارات منخفضة الدقة من الشعارات الرسمية المعروفة يجب التحقق مما إذا كان عنوان البريد الإلكتروني الخاص بالمرسل حقيقياً أم أنها محاولة لانتحال شخصية شخص تعرفه.

استخدم مبدأ "أقل امتياز" عندما تنشئ حساب مستخدم للموظفين. يجب أن تقتصر امتيازات المسؤول على حساب واحد أو حسابين وقم بالإشراف على الأنشطة.



جمع السجلات الأمنية



في حال الاستعانة بمصادر خارجية لخدمة تقنية المعلومات أو في حال تواصلك بفريق الدعم للبنية التحتية لتقنية المعلومات، تأكد من طلب المراقبة الأمنية الدورية وجمع السجلات الأمنية الخاصة بالأنشطة المهمة من أجهزة أو جدار الحماية سيكون ذلك مفيداً عند وقوع حادثة أمنية **على سبيل المثال:** إذا كان هنالك عدة عمليات لتسجيل الدخول فيتم تجميع محاولات تسجيل الدخول الفاشلة من عناوين البروتوكول المشبوهة.

حماية الهواتف الذكية (والأجهزة اللوحية)



- قم بتفعيل رقم التعريف الشخصي للجهاز المحمول/حماية كلمة المرور/التعرف على بصمات الأصابع.
- قم بضبط إعدادات الأجهزة بحيث يمكن تعقبها أو مسحها أو قفلها عن بُعد في حالة فقدانها أو سرقتها.
- حافظ على إبقاء الأجهزة وجميع التطبيقات المثبتة محدثة، وفعل خاصية "التحديث التلقائي".
- استخدم نقاط اتصال الهاتف المحمول بدلاً من شبكة العامة Wi-Fi عند إرسال/استلام البيانات حساسة.
- لا تضغط على الروابط التي يقوم بإرسالها أشخاص غير معروفين من خلال وسائل التواصل الاجتماعي أو الرسائل المشبوهة عبر البريد الإلكتروني، ولا تضغط على اشعارات برامج الإعلانات أثناء تصفح الإنترنت.

مع تحيات
المركز الوطني للأمن السيبراني

www.ncsc.gov.bh
#الأمن_السيبراني



