NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

EG|CERT

# دليل الأمن السيبراني للموظفين

## أنت الهدف.. احمي نفسك لتحمي شركتك

تعتبر تهديدات الأمن السيبراني عائقا ومشكلة متزايدة عالمياً، وهي مجموعة من التهديدات تسعى لتدير البنى التحتية وتدمير وتخريب الاقتصاد.

وزادة تلك تهديدات مع جائحة كورونا، لاعتمادنا اليومي على الأنترنت في التواصل والعمل والتعلم، مما أدي إلي زايده المعلومات والبيانات المتداولة. ومن جهة أخري طور مجرمي الإنترنت الطرق وأساليب الهجوم على الأفراد والمؤسسات.

وعليك الأن اتخاذ خطوات سريعة تشعرك بالثقة لحماية نفسك عبر الإنترنت، سواء كنت مهتم بمعرفة وفهم أساسيات الأمن السيبراني أو تود وضع المزيد من الإجراءات المتقدمة لحماية نفسك من التهديدات السيبرانية الشائعة. يوجد بعض الخطوات البسيطة السهلة التي يجب اتباعها.

### ما هو الأمن السيبراني الشخصي؟

العالم اليوم يعتمد بشكل أساسي على تكنولوجيا المعلومات والخدمات الإلكترونية والأجهزة الكمبيوتر، التليفون المحمول ووغيرها من الأجهزة المتصلة بالإنترنت، والخدمات المصرفية، والتسوق، ووسائل التواصل الاجتماعي، والحسابات البريد الإلكتروني والألعاب التي تكون كلها عرضة للتهديدات السيبرانية كل يوم الأمن السيبراني الشخصي هو خطوات مستمرة يجب اتباعها لحماية حساباتك وأجهزتك من التهديدات السيبرانية.


### ما هي التهديدات السيبرانية؟

هي عمليات الاحتيال والبرمجيات خبيثة موجهة للأشخاص والمؤسسات.

والبرمجيات خبيثة هي مصطلح شامل يستخدم لوصف البرامج الضارة المصممة لإحداث ضرر، بما في ذلك الفيروسات والديدان وبرامج التجسس وأحصنة طروادة وبرامج الفدية. يستخدم مجرمو الإنترنت البرمجيات خبيثة لسرقة معلوماتك وأموالك، والتحكم في أجهزتك وحساباتك.

الرسائل الخادعة هي رسائل يرسلها مجرمو الإنترنت مصممة للتلاعب بك للتخلي عن معلومات حساسة أو لتنشيط البرمجيات خبيثة على جهازك.

دليل الأمن السيبراني هو خطوات أولية مصممة لمساعدك على فهم أساسيات الأمن السيبراني وكيفه اتخاذ إجراءات والتدابير الاحترازية لحماية نفسك من التهديدات السيبرانية الشائعة:

# ١ التحديثات التلقائية

التحديث هو نسخة محسنة من البرامج (البرامج والتطبيقات وأنظمة التشغيل) التي قمت بتثبيتها على جهاز الكمبيوتر والأجهزة المحمولة.

تساعد تحديثات البرامج على حماية أجهزتك عن طريق إصلاح "أخطاء" البرامج (أخطاء الترميز أو نقاط الضعف) التي يمكن لمجرمي الإنترنت والبرمجيات خبيثة استخدامها للوصول إلى جهازك وسرقة بياناتك الشخصية وحساباتك ومعلوماتك المالية وهويتك.

يتم العثور باستمرار على "أخطاء" البرامج الجديدة واستغلالها من قبل مجرمي الإنترنت، لذا فإن تحديث البرنامج على أجهزتك يساعد في حمايتك من الهجمات الإلكترونية.

اما التحديثات التلقائية هي إعداد افتراضي الذي يقوم بتثبيت التحديثات الجديدة بمجرد توفرها لدي المطور. قد تختلف طريقة تشغيل التحديثات التلقائية حسب البرنامج والجهاز.

١ **قم بتشغيل وتأكيد التحديثات التلقائية على جميع البرامج والأجهزة.**

٢ **حدد وقتًا مناسبًا للتحديثات التلقائية إن أمكن.**


إذا تلقيت مطالبة بتحديث برامج جهازك، فيجب عليك القيام بذلك في أقرب وقت ممكن.

## ماذا لو كان إعداد التحديث التلقائي غير متاح؟

إذا لم يكن إعداد التحديث التلقائي متاحًا، فيجب عليك البحث بانتظام عن التحديثات الجديدة وتثبيتها من خلال قائمة إعدادات البرنامج أو الجهاز.

## ماذا يحدث إذا لم يتلق جهازي القديم وبرنامجي أي تحديثات؟

إذا كان جهازك أو نظام التشغيل أو البرنامج قديمًا جدًا، فقد لا يكون مدعومًا من قبل الشركة المصنعة أو المطور.

عندما تصل المنتجات إلى مرحلة "نهاية الدعم" هذه، فإنها لن تتلقى تحديثات بعد الآن، مما يجعلك عرضة للهجمات الإلكترونية.

إذا وصل جهازك أو نظام التشغيل أو البرنامج الخاص بك إلى نهاية الدعم، فإننا نوصي بالترقية في أقرب وقت ممكن للبقاء في أمان.


# ٢ تنشيط المصادقة متعددة العوامل MFA

يمكنك استخدام المصادقة متعددة العوامل (MFA) لتحسين أمان عبر حساباتك يتطلب منك MFA إنتاج مزيج من نوعين أو أكثر من أنواع المصادقة التالية قبل منح الوصول إلى حساب.

## شيء تعرفه

مثل رقم التعريف الشخصي أو كلمة المرور
أو عبارة المرور

## شيء ما أنت عليه

(مثل بصمة الإصبع أو التعرف على الوجه
أو مسح قزحية العين)


## شيء تملكه

مثال بطاقة ذكية أو رمز مادي أو تطبيق مصدق أو
رسالة نصية قصيرة أو بريد إلكتروني

المصادقة الثنائية (2FA) هي النوع الأكثر شيوعًا من أسلوب المصادقة متعددة العوامل MFA، وتتطلب نوعين مختلفين من المصادقة.

# ٣ تنشيط المصادقة متعددة العوامل MFA

## ما هي النسخة الاحتياطية؟

النسخة الاحتياطية هي نسخة رقمية من أهم معلوماتك (مثل الصور أو المعلومات المالية أو السجلات) التي قمت بحفظها على جهاز تخزين خارجي أو على السحابة الإلكترونية. النسخ الاحتياطي هو إجراء احترازي حتى يمكن استعادة معلوماتك في حالة فقدها أو سرقتها أو تلفها.

## كيف يمكنني الاحتفاظ بنسخة احتياطية من أجهزتي وملفاتي؟

يجب عليك إجراء نسخ احتياطي لملفاتك وأجهزتك بانتظام. ما يبدو عليه الأمر، سواء

يوميًا

أسبوعيًا

شهريًا

الامر يعود إليك في النهاية.


تحقق من النسخ الاحتياطية بانتظام حتى تكون على دراية بعملية الاسترداد، وتأكد من عمل النسخ الاحتياطية بشكل صحيح.


# ٤ قم بتأمين جهازك المحمول

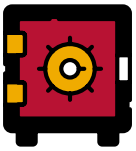
تُستخدم الهواتف الذكية والأجهزة اللوحية اليوم للاتصال والتسوق والعمل والبنوك والبحث وتتبع لياقتنا البدنية وإكمال مئات المهام الأخرى في أي وقت ومن أي مكان.

## ماذا يمكن أن يحدث إذا تعرض جهازي المتحرك للاختراق أو الضياع أو السرقة؟

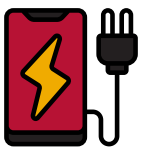
- قد يستخدمه مجرمو الإنترنت لسرقة أموالك أو هويتك، باستخدام المعلومات المخزنة على جهازك بما في ذلك حسابات وسائل التواصل الاجتماعي والبريد الإلكتروني.
- قد تفقد بيانات لا يمكن الاستغناء عنها مثل الصور أو الملاحظات أو الرسائل (إذا لم يتم نسخها احتياطيًا).
- قد يستخدم مجرم الإنترنت رقم هاتفك لخداع أشخاص آخرين.

## كيف أقوم بتأمين جهازي المحمول؟

قفل جهازك بكلمة مرور أو PIN أو رمز مرور. اجعل من الصعب التخمين

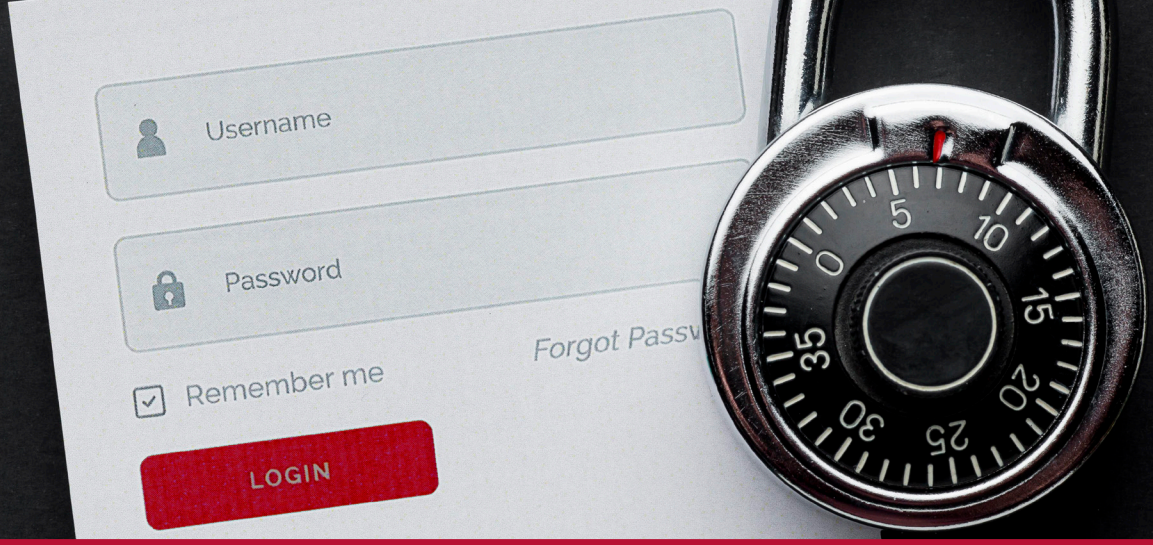


عامل هاتفك مثل محفظتك. احتفظ بها بأمان ومعك في جميع الأوقات



لا تشحن جهازك في محطة شحن عامة وتجنب أجهزة الشحن من جهات خارجية

تأكد من ضبط جهازك على القفل تلقائيًا بعد فترة قصيرة من عدم النشاط




# ٥ استخدم كلمة مرور قوية

كلمة المرور القوية هي خط الدفاع الأول ضد مهاجم الأمن السيبراني فهي الطريقة الأكثر استخداماً لحماية معلوماتك عند الدخول إلى جهازك وبريدك الإلكتروني. لذلك يجب عليك اختيار كلمة مرور قوية يمكنك تذكرها بسهولة ولا يستطيع الأخرون تخمينها. يسهل على مجرمي الإنترنت استنتاج تاريخ ميلادك ونمط القفل. استخدم عبارة مرور لتحقيق الأمان الأمثل. قد تفكر أيضًا في استخدام التعرف على الوجه أو بصمة الإصبع لإلغاء قفل جهازك.

## كيف تنشئ كلمه مرور قوية سهلة الحفظ بالنسبة لك؟

فكّر في كلمة ذات معني بالنسبة لك مثل:

**Password**

↓

اضِف بعض الأحرف الكبيرة

**PaSSwoRd**

↓

اضِف بعض الأرقام في بداية أو وسط أو نهاية الكلمة

**24 Pa12SSwoRd**

↓

زد من طول الكلمة بإضافة الرموز وعلامات الترقيم

**P@a12SSwoRd24!**

نصيحة

استخدم كلمات مرور مختلفة لكل حساب

**المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات**

القرية الذكية, مبنى ب ١٢٤ -الكيلو ٢٨- طريق القاهرة اسكندرية الصحراوى

ت: ٣٥٣٩٠١١١ (٢٠٢+) - ٣٥٣٩٤٤٤٤ (٢٠٢+) ف: ٣٥٣٩٠٤٤٤ (٢٠٢+) الخط الساخن 15315

www.egcert.eg