



Association Tunisienne
de Prévention Positive

الجمعية التونسية
للوقاية الايجابية

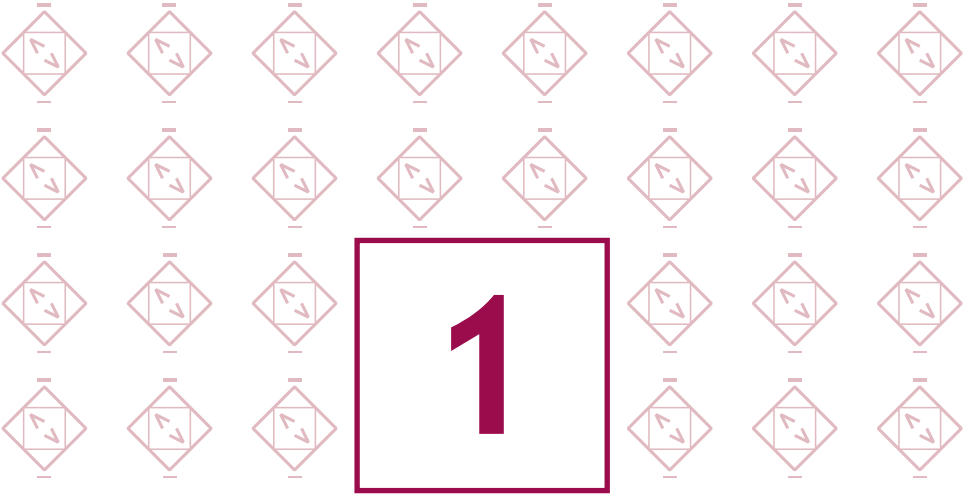
دليل تدابير الأمن السيبرني وحماية المعطيات الشخصية



فهرس

- 1 / إختبر كلمات المرور بعناية (3)
- 2 / تحديث البرامج المثبتة بانتظام (3)
- 3 / النسخ الاحتياطية (8)
- 4 / ثبت مضادات الفيروسات وقم بتأمين جهازك (10)
- 5 / تأمين الوصول إلى شبكة الواي فاي (12)
- 6 / أمن الهواتف المحمولة (14)
- 7 / حماية البيانات عند التنقلات (16)
- 8 / إلتزام الحذر عند إستعمل البريد الإلكتروني (18)
- 9 / تنزيل البرامج حصرياً من المواقع الرسمية للناشرين (20)
- 10 / كن يقظاً عند الدفع على الإنترنت (22)
- 11 / إفصل الاستخدامات الشخصية عن الاستخدامات المهنية (24)
- 12 / حماية معلومات الهوية الشخصية والتجارية والرقمية (26)
- ياختصار ... (28)
- مصادر للتعمق (28)
- قائمة المصطلحات (29)





إِخْتَرْ كَلِمَاتِ الْمُرُورِ بِعِنَايَةٍ

عند العمل أو استخدام عنوان بريد إلكتروني شخصي، يمكنك اختيار كلمة مرور ضعيفة: يمكن إختراق أو التكهّن بكلمة المرور هذه بسهولة أثناء الهجوم باستخدام . 12345678 أداة آلية: ينجر عنها خسارة المال أو بيانات حساسة يمكن بيعها

تعد كلمات المرور طريقة فعالة للتحكم في الوصول إلى بياناتك والأجهزة التي تخزنها عليها والخدمات التي تستخدمها عبر الإنترنت .
تحتوي هذه الصفحة على نصائح حول كيفية إنشاء كلمات مرور قوية وكيفية التعامل معها وماذا تفعل إذا كنت تعتقد أنها سُرقت .

أنشئ كلمات مرور قوية

قم بإنشاء كلمة مرور قوية لا تُنسى لحساب بريدك الإلكتروني وحسابات مهمة أخرى



- تجنب استخدام كلمات مرور يمكن التنبؤ بها مثل التواريخ وأسماء العائلات والحيوانات
تجنب كلمات المرور الأكثر شيوعًا التي يمكن للمجرمين تخمينها بسهولة مثل 'passw0rd'



- لا تعيد استخدام نفس كلمة المرور للحسابات المهمة. إذا سُرقت إحدى كلمات المرور الخاصة بك، فأنت لا تريد أن يتمكن المجرم أيضًا من الوصول على سبيل المثال إلى حسابك المصرفي



- لإنشاء كلمة مرور لا تُنسى يصعب تخمينها أيضًا، يمكنك دمج ثلاث كلمات عشوائية لإنشاء كلمة مرور واحدة على سبيل المثال cupfishbiro

احفظ كلمات المرور الخاصة بك في مكان آمن

إذا قمت بتخزين كلمات المرور الخاصة بك في مكان آمن، فلن تضطر إلى تذكرها بعد الآن



- يمكنك كتابة كلمات المرور الخاصة بك لتذكرها، ولكن احتفظ بها آمنة، بعيدًا عن الأنظار، و (الأهم من ذلك) بعيدًا عن جهاز الكمبيوتر الخاص بك



- قم بتخزين كلمات المرور الخاصة بك في المتصفح الخاص بك عند الطلب ؛ إنه أكثر أمانًا من إعادة استخدام نفس كلمة المرور. يمكن للمتصفحات أيضًا اكتشاف مواقع الويب «المشكوك فيها» التي تحاول رسائل البريد الإلكتروني الاحتيالية خداعك من خلال زيارتك



- يمكنك أيضًا استخدام مدير كلمات مرور مستقل لمساعدتك في إنشاء وتخزين كلمات مرور قوية

لحماية حسابك استخدم 2FA

يطلق عليه هذا الاسم لأنه يتضمن تسجيل الدخول إلى حسابك باستخدام كلمتين مرور أو رمزين، أحدهما تعرفه والآخر يتم إرساله عادةً إلى هاتفك



- الشكل الأكثر شيوعًا للمصادقة الثنائية هو عندما يتم إرسال رمز إلى هاتفك الذي تحتاج إلى إدخاله من أجل المضي قدمًا. تكون الحاجة إلى المصادقة الثنائية ملحة عند الولوج لمواقع مهمة مثل الخدمات المصرفية والبريد الإلكتروني



■ حتى لو كان المجرم يعرف كلمات السر الخاصة بك، وقال انه سوف تواجه مشكلة الوصول إلى الحسابات التي تحميها عن طريق تنشيط المصادقة الثنائية



■ المصادقة الثنائية مدعومة من الخدمات الشهيرة عبر الإنترنت مثل غوغل، فيسبوك و تويتر و لنكدين و اوتلوك و إنستجرام

ماذا لو سُرقت كلمة السر ؟



■ إذا كنت تشك في أن كلمة المرور الخاصة بك قد سُرقت، فيجب عليك تغييرها على الفور

■ إذا استخدمت نفس كلمة المرور في حسابات أخرى، فقم بتغييرها أيضًا، يمكنك استخدام

WWW.HAVEIBEENPWNER.COM



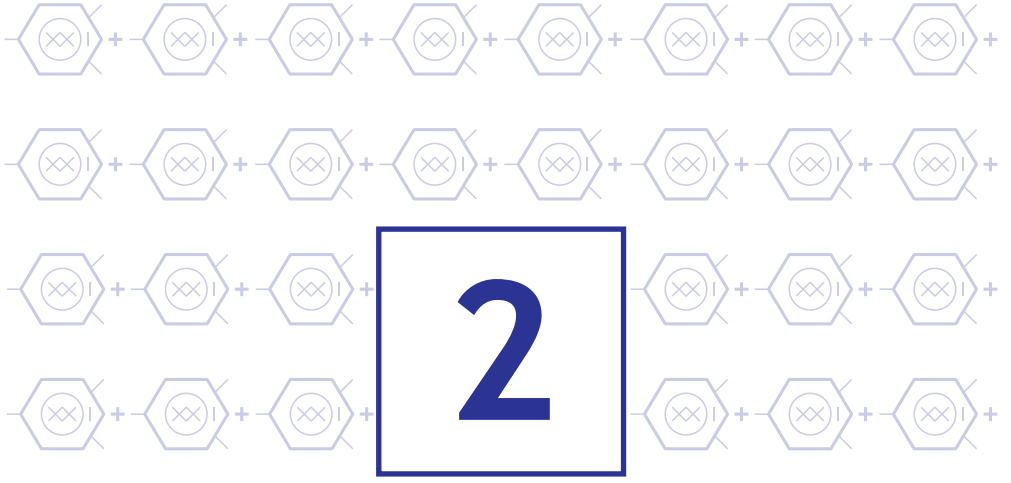
للتحقق مما إذا كانت معلوماتك قد تم نشرها بالفعل كجزء من خرق كبير للبيانات



حافظ كلمات مرور آمن ومجاني

يتيح لك هذا البرنامج الصغير المجاني ، تخزين كلمات المرور الخاصة بك بأمان لاستخدامها في تطبيقاتك كما أن له وظيفة لإنشاء كلمات مرور عشوائية معقدة

<https://keepass.info>



تحديث البرامج المثبتة بانتظام

إذا لم نقوم دائماً بتحديث البرامج، فإننا نخاطر بفتح مرفق يحتوي أو يستغل ثغرات حماية دون ملاحظة ذلك بعد هذا الخطأ، قد يستخدم المهاجمون اختراق ثغرة برنامج الكمبيوتر للتجسس على أنشطة المنظمة أو سرقة البيانات الشخصية

تعرض الأجهزة الرقمية والبرامج التي نستخدمها كل يوم لنقاط الضعف الأمنية. يمكن لمجرمي الإنترنت استخدام هذه العيوب للسيطرة على جهاز كمبيوتر أو معدات متنقلة أو ساعة ذكية. في مواجهة هذه المخاطر، يقدم الناشر والمصنعون تحديثات لتصحيح هذه العيوب. إذا كان يتم الشعور بعملية التحديث في كثير من الأحيان كعائق، فهي مع ذلك عمل أساسي لحماية نفسها. ولذلك ينبغي وضع قواعد معينة داخل الشركة

■ تذكر تحديث جميع أجهزتك وبرامجك على الفور



الحواسيب، الهواتف، أنظمة التشغيل، برامج معالجة النصوص، الكائنات المتصلة تستخدم عدداً كبيراً من الأجهزة والبرامج. لا يتطلب الأمر سوى واحدة قديمة وتعرض لخرق أمني لخرق بيتك الرقمية. من أجل منع مجرمي الإنترنت من استخدام نقاط الضعف الأمنية هذه لاختراقك وسرقة المعلومات الشخصية الحساسة منك من الضروري تحديث معداتك بمجرد توفرها .

■ يجب تحديث البرامج الخاصة بك من المواقع الرسمية فقط

فقط المواقع أو الأجهزة الرسمية للناشرين والمصنعين تضمن عدم إصابة التحديثات التي تقوم بتثبيتها بفيروس. عند تثبيت التحديثات الخاصة بك، انتبه إلى ظروف الاستخدام المحتملة أو الصناديق التي تم فحصها مسبقاً والتي يمكن قبولها لتثبيت برنامج آخر غير مرغوب فيه.



■ قم بتحديد خيار تنزيل التحديثات وتثبيتها تلقائياً

فقط المواقع أو الأجهزة الرسمية للناشرين والمصنعين تضمن عدم إصابة التحديثات التي تقوم بتثبيتها بفيروس. عند تثبيت التحديثات الخاصة بك، انتبه إلى شروط الاستخدام المحتملة أو الخيارات التي تم قبولها مسبقاً والتي تمكن تثبيت برنامج آخر غير مرغوب فيه (برامج إعلانية، على سبيل المثال).





النسخ الاحتياطية

هناك خطر كبير لفقدان جميع ملفات العملاء
أو ملفات داخلية للمنظمة بعد فشل حاسوبي أو
عدوى فيروسية إذا لم يتم عمل نسخة احتياطية

في استخداماتنا الشخصية أو المهنية، نستخدم العديد من الأجهزة الرقمية لإنشاء المعلومات وتخزينها ومع ذلك، قد تتضرر هذه الأجهزة أو تتلف، مما يؤدي إلى فقدان بياناتنا، وأحياناً لا يمكن استرجاعها من أجل منع مثل هذا الخطر، يُنصح بشدة بتسجيل نسخ للحفاظ على هذه البيانات على المدى الطويل .

■ قم بإجراء نسخ احتياطية منتظمة



في حالة الضياع أو السرقة أو القرصنة أو تدمير أجهزتك الرقمية ،ستفقد البيانات المسجلة على هذه الوسائط . فقد تكون هذه البيانات هي البيانات ، التي تعلق عليها أهمية خاصة أو تعتبرها ضرورية في سياق أنشطتك (سواء الشخصية أو المهنية (الصور ، مقاطع الفيديو ، من العمل ، وما إلى ذلك) قم بإجراء استباقي لحفظ نسخ احتياطية منتظمة .



■ توفر معظم حلول التخزين السحابي مساحة تخزين مجانية
قد يكون هذا كافياً لحفظ جميع ملفاتك المهمة .



■ يمكنك إنشاء نسخ احتياطية قائمة على السحابة تلقائياً، مما يعني أنه من المرجح أن يكون لديك نسخة محدثة من بياناتك .



■ يتطلب التخزين السحابي اتصالاً موثوقاً بالإنترنت، لذلك لا يكون مناسباً إذا كان التخزين بطيئاً أو غير موثوق به أو تم قياسه .

قم بحماية حساباتك السحابية (والوصول إلى نسخك الاحتياطية) باستخدام كلمات مرور قوية وتمكين المصادقة الثنائية .



يمكن أن تحتوي النسخ الاحتياطية للوسائط القابلة للإزالة على كميات كبيرة من البيانات، والتي قد تتجاوز سعة خيارات التخزين السحابية



احم نسخك الاحتياطية بكلمة مرور قوية في حالة فقدان الوسائط أو سرقتها
لا يمكن لأي شخص لديه وسائط الملتيميديا الوصول إلى بياناتك ما لم يكن يعرف كلمة المرور .





4

ثبت مضادات الفيروسات وقم بتأمين جهازك

عند توصيل القرص المحمول ، يلوث الفيروس الكمبيوتر الشخصي
ويدفع المستخدم إل إعادة تنسيق وسائط الكمبيوتر
،لإعادة استخدام نظام التشغيل الخاص به
مما يؤدي إلى فقدان البيانات، وهذا بسبب عدم
وجود مضاد فيروس يحمي الجهاز .

يمكن أن تصاب الأجهزة بالعدوى عن طريق تنزيل مرفق يحتوي على برامج ضارة عن طريق الخطأ أو توصيل محرك أقراص محمولة مصاب بالفعل. يمكنك حتى أن تصاب بالعدوى من خلال زيارة موقع ويب مشكوك فيه .
لهذه الأسباب، من المهم أن تستخدم دائماً برامج مكافحة الفيروسات على أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر والهواتف الذكية .

تأكد من تشغيل منتجك السمعي البصري وتحديثه. يحتوي ويندوز و أي -أو-س على أدوات مدمجة توفر مضادات فيروسية مناسبة .



غالبًا ما تأتي أجهزة الكمبيوتر الجديدة مع نسخة تجريبية من البرامج السمعية والبصرية الإضافية
يمكنك إجراء بحثك الخاص لمعرفة ما إذا كانت هذه المنتجات مناسبة لك .



تأكد من تهيئة برنامج مضاد الفيروسات الخاص بك لمسح جميع الملفات الجديدة تلقائيًا، مثل تلك التي تم تنزيلها من الإنترنت أو تخزينها على محرك أقراص محمولة أو قرص صلب خارجي أو أي نوع آخر من الوسائط القابلة للإزالة .



لا تحتاج إلى منتجات سمعية بصرية على هاتفك الذي أو جهازك اللوحي، طالما أنك تقوم فقط بتثبيت التطبيقات من المتاجر الرسمية .



قم بتنزيل تطبيقات الهواتف الذكية والأجهزة اللوحية فقط في المتاجر الرسمية مثل غوغل بلاي ثم التحقق من التطبيقات التي تم تنزيلها من المتاجر الرسمية لتوفير الحماية من الفيروسات والبرامج الضارة .



إذا تلقيت مكالمة هاتفية تقدم المساعدة في إزالة الفيروسات والبرامج الضارة من جهاز الكمبيوتر الخاص بك، فقم بإغلاق المكالمة على الفور (هذه عملية احتيال) .





5

تأمين الوصول إلى شبكة الواي فاي

راوتر الوصول إلى الإنترنت في متجر يستخدم تشفير واب بدون أن يلاحظه المدير، تمكن أحد الجيران من فك شفرة مفتاح الاتصال في أقل من دقيقتين باستخدام برنامج لقد استخدم نقطة اتصال الواي فاي هذه للمشاركة في هجوم على موقع ويب حكومي تبعاً لذلك، تم توريط مدير المتجر في تحقيق الشرطة

يعد استخدام شبكة الواي فاي أكثر سهولة و جاذبية. ومع ذلك، لا ينبغي أن ننسى أن شبكة الواي فاي بيئة التأمين يمكن أن تسمح للأشخاص باعتراض بياناتك واستخدام اتصال الواي فاي دون علمك لإجراء عمليات ضارة. لهذا السبب يجب تجنب الوصول إلى الإنترنت من خلال نقطة اتصال الواي فاي داخل الشركة: يظل الاتصال السلكي أكثر أماناً وكفاءة.

يمكن أن تكون شبكة الواي فاي بعض الأحيان هي الطريقة الوحيدة للوصول إلى الإنترنت، وفي هذه الحالة من الضروري تأمين الوصول عن طريق تكوين نقطة الوصول إلى الإنترنت الخاصة بك. للقيام بذلك :



في واجهة اختيارات الراوتر الخاص بك، تحقق من هاته الخصائص

جهازك يحتوي على بروتوكول التشفير و**WPA2** قم بتفعيله

خلاف ذلك، استخدم نسخة و**WPA2**-**AES** (لا تستخدم أبداً تشفير ويب القابل للكسر في دقائق) ؛

تغيير مفتاح الدخول الافتراضي الذي غالباً ما يتم عرضه على ملصق الراوتر بواسطة كلمة مرور يزيد عن **12** حرفاً من أنواع مختلفة ؛

عدم الكشف عن مفتاح تسجيل الدخول الخاص بك لأطراف أخرى وتغييره بانتظام ؛
تنشيط وظيفة الجدار الناري لجهازك ؛
عطل نقطة وصولك عندما لا تكون قيد الاستخدام



عدم استخدام شبكة الواي فاي «العامة» (الشبكات المتاحة في المحطات أو المطارات أو الفنادق) لأسباب تتعلق بالأمن والخصوصية ؛



المفضل استخدام نقطة اتصال مخصصة إذا كان يجب عليك توفير الاتصال للإنترنت لطرف ثالث. لا تشارك معلومات الإتصال على الشبكة .

6

أمن الهواتف المحمولة

مستخدم لديه هاتف ذكي يستخدمه في استعمالات شخصية و عملية عند قيامه بتثبيت تطبيق، لم يعطل خيار وصول التطبيق إلى بياناته الشخصية. الآن، يمكن لمحرر التطبيق الوصول إلى جميع الرسائل النصية على هاتفه .

على الرغم من تقديم خدمات مبتكرة، إلا أن الهواتف المحمولة (الهواتف الذكية) غير آمنة للغاية حاليًا. لذلك من الضروري تطبيق بعض القواعد الأساسية لأمن تكنولوجيا المعلومات:



قم فقط بتثبيت التطبيقات اللازمة والتحقق من البيانات التي يمكنهم الوصول إليها. قبل التنزيل مثل المعلومات الجغرافية، والاتصالات، والمكالمات الهاتفية، وما إلى ذلك تتطلب بعض التطبيقات الوصول إلى بيانات غير ضرورية لتشغيلها، ويجب علينا تجنب تركيبها ؛



بالإضافة إلى رمز بين الذي يحمي بطاقة هاتفك، استخدم مخططاً أو كلمة مرور لتأمين الوصول إلى جهازك وتهيئته للقفل تلقائياً ؛
قم بعمل نسخ احتياطية منتظمة من المحتوى الخاص بك على الوسائط الخارجية حتى تتمكن من الاحتفاظ به في حالة استعادة جهازك إلى حالته الأصلية ؛



تشفير بيانات الجهاز: في حالة الخسارة أو السرقة، فإن تشفير البيانات الموجودة في جهازك فقط سيضمن عدم تمكن المخترق من تجاوز رموز الوصول والاستمرار في الوصول إلى معلوماتك. تقدم جميع الأجهزة الحديثة هذا الخيار الذي يتم تمكينه فقط في الإعدادات والذي يكاد يكون شفافاً للاستخدام. إذا كنت تستخدم بطاقة تمديد الذاكرة لتخزين معلوماتك، فتأكد من تشفيرها أيضاً



لا تخزن المعلومات السرية دون حماية: لا تكتب أبداً معلومات سرية مثل كلمات المرور أو الرموز المصرفية في دليل الاتصال أو البريد الإلكتروني أو الملف غير المشفر على جهازك المحمول. يمكن لمجرم الإنترنت الذي سيطر على جهازك استعادته بسهولة. بالإضافة إلى ذلك، يمكن أيضاً لبعض التطبيقات التي قمت بتثبيتها الوصول إلى هذه المعلومات واستردادها والتي قد تفقد السيطرة عليها. لحماية معلوماتك السرية، استخدم حل التشفير بكلمة مرور قوية



قم بتثبيت فين للحفاظ على إخفاء هويتك

تثبيت تطبيق حماية مثل تطبيق كاسبرسكي على الهاتف المحمول



حماية البيانات عند التنقلات

في أحد المطارات، يتعاطف مسافر مع آخر يدعي أن لديه معرفة مشتركة. عندما سئل عما إذا كان بإمكانه استخدام جهاز الكمبيوتر الخاص به لشحن هاتفه، المسافر لم يشتبه في أي شيء مريب. فانتهاز المجهول الفرصة لتهريب البيانات المتعلقة بالمهمة المهنية فائقة السرية للمسافر .

يسهل استخدام أجهزة الكمبيوتر المحمولة أو الهواتف الذكية أو الأجهزة اللوحية السفر التجاري ونقل البيانات وتبادلها. ومع ذلك، فإن السفر مع هذه الأجهزة المحمولة بدون حماية فائقة يشكل تهديدات للمعلومات الحساسة التي سيكون لسرقتها أو خسارتها تأثير كبير على أنشطة المنظمة .

قبل الذهاب في مهمة عمل :

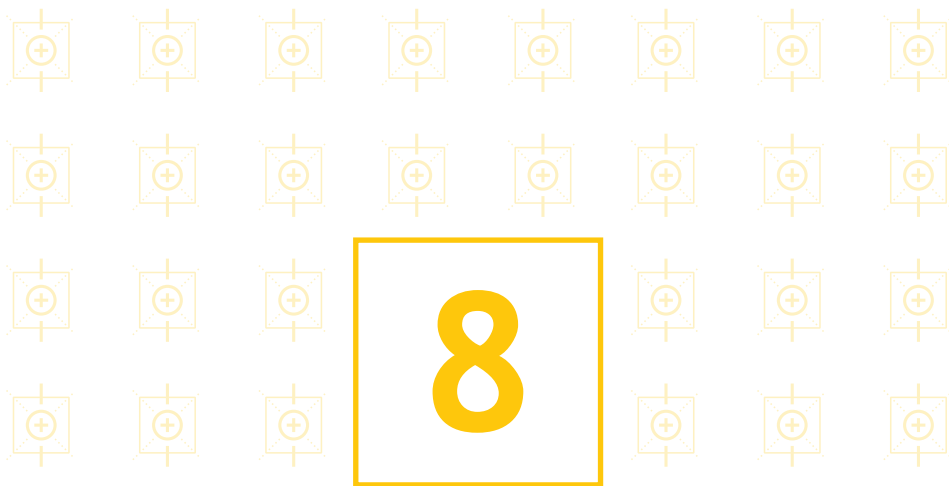
- استخدام أجهزة الحاسوب ، الأقراص المحمولة،الهواتف، والبيانات اللازمة لمهمة العمل فقط القيام بحفظ نسخة عن هذه البيانات لاستردادها في حالة الخسارة ؛
- إذا كنت تخطط للاستفادة من رحلات العمل، فاحصل على فلتز حماية الشاشة لجهاز الكمبيوتر الخاص بك من المتطفلين ؛
- ضع علامة مميزة (مثل نقطة ملونة) على أجهزتك لضمان عدم وجود تبادل أثناء النقل
- تأكد من عدم تسجيل كلمات المرور مسبق

خلال مهمات العمل

- احتفظ بأجهزتك ووسائطك وملفاتك معك، سواء أثناء رحلتك أو أثناء إقامتك لا تتركها في مكتب أو خزانة فندق؛
- عطل شبكة الواي فاي أو بلوتوث على أجهزتك ؛
- قم بإزالة بطاقة سيم والبطارية إذا اضطرت إلى الانفصال عن هاتفك ؛
- لا تستخدم المعدات المعروضة عليك إذا لم تتمكن من التحقق منها ؛
- تجنب توصيل معدّاتك بمحطات غير موثوقة. على سبيل المثال، إذا كنت بحاجة إلى تبادل المستندات أثناء عرض تجاري، فاستخدم مفتاح محمول أو قرص مدموج فقط لهذا الغرض ثم امسح البيانات باستخدام برنامج محو آمن ؛

بعد مهمة العمل

- مسح قائمة المكالمات والتنقلات ؛
- قم بتغيير كلمات المرور التي استخدمتها أثناء الرحلة ؛
- قم بتحليل معدّاتك بعد المهمة، إذا استطعت
- لا تستخدم أبداً محرّكات أقراص الفلاش التي ربما تم تقديمها لك أثناء رحلاتك



إلتزام الحذر عند إستعمل البريد الإلكتروني

بعد استلام رسالة بريد إلكتروني يبدو أنها تأتي من أحد زملائه، نقر المستخدم على رابط في الرسالة هذا الرابط يحمل برنامج ضار يمكن المخترق من التحكم في جهازه عن بعد بدون علمه، يتم استخدام جهاز الكمبيوتر الخاص به الآن لإرسال رسائل بريد إلكتروني ضارة تبث صورًا إباحية

غالبًا ما تلعب رسائل البريد الإلكتروني ومرفقاتها دورًا رئيسيًا في تنفيذ هجمات الكمبيوتر مثل رسائل البريد الإلكتروني الاحتيالية والمرفقات الملوثة بالفيروسات وما إلى ذلك .
عند تلقي رسائل البريد الإلكتروني، اتخذ الاحتياطات التالية:



■ هوية المرسل غير مضمونة بأي شكل من الأشكال: تحقق من التناسق بين المدعى ومحتوى الرسالة وتحقق من هويته. إذا كان هناك شك، فلا تتردد في الاتصال بمرسل البريد الإلكتروني مباشرة ؛

■ عدم فتح مرفقات من متلقين مجهولين أو يبدو أن عنوانهم أو شكلهم غير متناسقين مع الملفات التي ترسلها إليك جهات الاتصال الخاصة بك عادة ؛



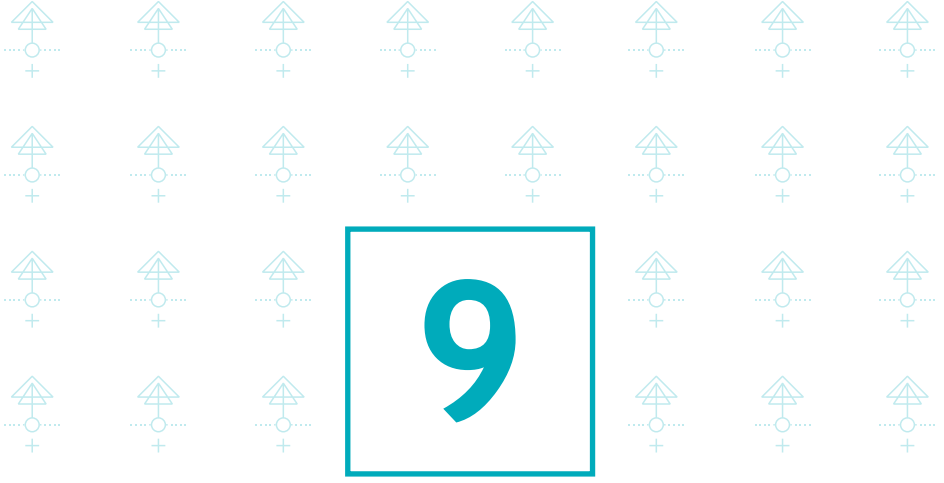
إذا ظهرت الروابط في رسالة بريد إلكتروني، فضع مؤشر الفأرة على الرابط قبل النقر عليه سيتم عرض عنوان الموقع الكامل في شريط حالة المتصفح أسفل يسار النافذة بشرط أن يكون قد تم تمكينه سابقًا. وبذلك ستتمكنون من التحقق من اتساقها ؛

■ لا ترد أبدًا عبر البريد الإلكتروني على طلب للحصول على معلومات شخصية أو سرية مثل الرمز السري ورقم بطاقتك الائتمانية في الواقع، تنتشر رسائل البريد الإلكتروني بألوان مؤسسات لاستعادة بياناتك. هذه هجمات تصيد * ؛

■ عدم فتح أو نقل رسائل مثل رسائل متسلسلة ، ومكالمات التضامن، والإنذارات الفيروسية، وما إلى ذلك ؛



■ قم بإيقاف تشغيل الفتح التلقائي للمستندات التي تم تنزيلها وتشغيل مسح مضاد للفيروسات * قبل فتحها للتحقق من أنها لا تحتوي على أي برنامج فيروسي معروف



تنزيل البرامج حصرياً من المواقع الرسمية للناشرين

قام مستخدم يريد حماية نفسه من برامج التجسس بتنزيل برنامج متخصص يقدمه محرك البحث الخاص به دون أن يعرف ذلك، قام بتركيب حصان طروادة .

إذا قمت بتنزيل محتوى رقمي من مواقع الويب غير الموثوقة، فإنك تخاطر بتسجيل برامج على جهاز الكمبيوتر الخاص بك لا يمكن تحديثها، وغالبًا ما تحتوي على فيروسات أو حصان طروادة* . يمكن أن يسمح هذا للأشخاص الخبيثين بالتحكم عن بعد في جهازك للتجسس، على الإجراءات التي يتم إجراؤها على جهاز الكمبيوتر الخاص بك، وسرقة بياناتك الشخصية وشن الهجمات، وما إلى ذلك .

في هذا السياق، لضمان أمن جهازك وبياناتك:



■ تحميل برامجك على مواقع ناشريها أو غيرها من المواقع الموثوق بها ؛

■ تذكر أن لا تنقر أو تختار على صناديق الاختيار التي تعرض تثبيت برامج إضافية ؛



■ كن يقظًا بشأن الروابط المدعومة وفكر قبل النقر فوق الروابط ؛

■ قم بإيقاف تشغيل الفتح التلقائي للمستندات التي تم تنزيلها وتشغيل مسح مضاد للفيروسات* قبل فتحها للتحقق من أنها لا تحتوي على أي برنامج فيروسي معروف.

10

كن يقظاً عند الدفع على الإنترنت

اشترى مسؤول لوازم مكتبية لشركته على الإنترنت
دون التحقق من الحالة الأمنية لموقع التجارة الإلكترونية.
هذا الأخير لم يكن آمناً.
فاعترض المهاجمون رقم بطاقة الائتمان الخاصة بالشركة
واستخدموها لتقديم طلبات لصالحهم

عند إجراء عمليات شراء على الإنترنت، عبر جهاز الكمبيوتر أو الهاتف الذكي، من المحتمل أن يتم إدخال التفاصيل المصرفية الخاصة بك بواسطة المهاجمين مباشرة، على جهاز الكمبيوتر الخاص بك أو في ملفات العملاء في موقع التاجر. وبالتالي، قبل إجراء الدفع عبر الإنترنت، من الضروري التحقق من نجاعة الحماية على الموقع الإلكتروني :



■ تحقق من وجود قفل في شريط العناوين أو أسفل يمين نافذة المتصفح

ملاحظة: هذا القفل غير مرئي على بعض المتصفحات

■ تأكد من ظهور «https://» في بداية عنوان الموقع

■ تحقق من دقة عنوان الموقع الإلكتروني من خلال الاهتمام

بالأخطاء الإملائية في إسم العلامة التجارية على سبيل المثال

إذا أمكن، عند الشراء عبر الإنترنت:



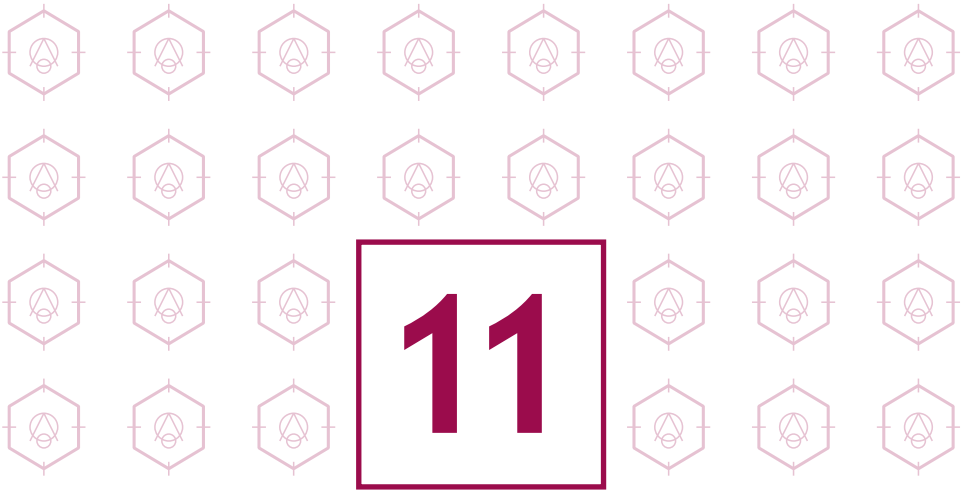
■ استعمل الطريقة التي تنطوي على إرسال رمز تأكيد الطلب بواسطة

الرسائل القصيرة ؛

■ بشكل عام، لا تفضي أبداً الرمز السري لبطاقتك المصرفية لشخص

آخر؛

■ لا تتردد في الاتصال بمصرفك لمعرفة واستخدام الوسائل الآمنة التي يقدمها



إفصل الاستخدامات الشخصية عن الاستخدامات المهنية

- غالبًا ما يجلب موظف العمل إلى المنزل ليلاً
- دون أن يلاحظ، تعرض جهاز الكمبيوتر الشخصي الخاص به للهجوم
- بفضل المعلومات التي احتوتها، تمكن المهاجم من اختراق
- شبكة شركة الموظف الداخلية.
- سُرقت معلومات حساسة ثم أعيد بيعها للمنافسة .

تختلف الاستخدامات وتدابير السلامة بالنسبة لمعدات الاتصال الشخصية والمهنية الحواسيب وما إلى ذلك.

The WITH: أحضر معدات الاتصال الشخصي الخاصة بك

BYOD: أحضر جهازك الخاص

هي ممارسة تعني الموظفين الذين يستخدمون معداتهم الشخصية (الكمبيوتر، الحاسوب والأجهزة اللوحية وما إلى ذلك في سياق مهني.

إذا تم استخدام هاته الممارسة أكثر فأكثر اليوم فإنه يطرح مشاكل من حيث أمن البيانات سرقة أو فقدان الأجهزة، والاقترام، وعدم التحكم في استخدام الأجهزة من قبل الموظفين، وتسريب البيانات عند مغادرة الموظف.

وفي هذا السياق، يوصى بالفصل بين استخداماتكم الشخصية والمهنية:



- لا ترسل رسائل البريد الإلكتروني الخاصة بعملك إلى خدمات الرسائل الشخصية ؛
- لا تستضيف بيانات مهنية عن معداتك الشخصية (مفتاح فلاش أو الهاتف وما إلى ذلك) أو على وسائل التخزين الشخصية عبر الإنترنت ؛



- تجنب ربط الوسائط الشخصية القابلة للإزالة (مفاتيح فلاش، محركات الأقراص الصلبة الخارجية، وما إلى ذلك) بأجهزة الكمبيوتر التابعة للشركة

إذا لم تطبق هذه الممارسات الجيدة، فإنك تخاطر بأن يسرق المخترقون معلومات حساسة من شركتك بعد أن يتمكنوا من السيطرة على جهازك الشخصي .

12

حماية معلومات الهوية الشخصية والتجارية والرقمية

يتلقى مستخدم الإنترنت عرضاً عبر البريد الإلكتروني للدخول في
مسابقة للفوز بجهاز كمبيوتر محمول. للقيام بذلك، يجب عليه
إرسال عنوان بريده الإلكتروني. أخيراً، لم يفز ولكنه
يتلقى الآن العديد من رسائل البريد الإلكتروني غير المرغوب فيها

البيانات التي تتركها على الإنترنت تفلت منك على الفور ولا يمكنك التحكم فيها
يمارس الأشخاص الخبيثون الهندسة الاجتماعية، أي جمع معلوماتك الشخصية
في أغلب الأحيان عن طريق الاحتيال ودون علمك، من أجل إستنتاج كلمات المرور
الخاصة بك، للوصول إلى نظام الكمبيوتر الخاص بك، أو حتى انتحال شخصيتك
أو الانخراط في التجسس الصناعي.
وفي هذا السياق، يُنصح بتوخي الحذر الشديد في نشر معلوماتكم الشخصية على
شبكة الإنترنت :



■ كن حذرًا مع النماذج التي تملأها: وتوفير المعلومات الضرورية فقط ؛

■ ضع في اعتبارك عدم التحقق من الإختيارات التي تسمح للموقع بتخزين أو مشاركة بياناتك ؛



وإتاحة إمكانية الوصول إلى الحد الأدنى من المعلومات الشخصية والمهنية على الشبكات

الاجتماعية، وتوخي اليقظة عند التفاعل مع المستخدمين الآخرين ؛



■ تذكر التحقق من إعدادات الأمان والخصوصية بانتظام ؛

■ أخيرًا، استخدم العديد من عناوين البريد الإلكتروني المخصصة لأنشطتك المختلفة على



الإنترنت: عنوان مخصص للأنشطة الجادة (المصارف، والبحث عن عمل، والنشاط

المهني، وما إلى ذلك) وعنوان للخدمات الإلكترونية الأخرى (المنتديات، وألعاب المنافسة

وما إلى ذلك،).

بإختصار ...

وبغية تعزيز أمن معدات الاتصالات وبياناتكم على نحو فعال، يمكنكم استكمال الممارسات الجيدة

الآتية عشرة الواردة في هذا الدليل بالتدابير التالية:

- تعيين مسؤول عن أمن تكنولوجيا المعلومات في الشركات
 - كتابة مرجع لتكنولوجيا المعلومات ؛
 - قم بتشفير تبادل البيانات والمعلومات باستخدام برنامج التشفير
 - قم بتشديد إعدادات محطة العمل الخاصة بك واستخدم حلول أمان مثبتة و جدران الحماية مضاد للفيروسات
 - قبل حفظ الملفات من وسائط قرص فلاش إلى جهاز الكمبيوتر الخاص بك، قم بمسحها ضوئياً بواسطة مضادات الفيروسات ؛
 - تعطيل التنفيذ التلقائي للوسائط القابلة للإزالة من جهاز الكمبيوتر الخاص بك ، إيقاف تشغيل جهاز الكمبيوتر الخاص بك خلال فترات الخمول المطول (الليل، عطلة نهاية الأسبوع ،...، العطلات)
 - مراقبة نظامك، بما في ذلك استخدام سجلات الأحداث، للرد على الأحداث المشبوهة
- اتصال مستخدم خارج ساعاته المعتادة، ونقل هائل للبيانات إلى خارج الشركة، ومحاولات الاتصال بحساب غير نشط، وما إلى ذلك

مصادر للتعمق ...

- <https://www.ansi.tn>
- <http://www.ssi.gouv.fr>
- <https://www.ncsc.gov.uk/cyberessentials/overview>
- <https://gdpr-info.eu/>
- <https://security.web.cern.ch>
- <https://www.ontario.ca/fr/document/manuel-sur-lacces-linformation-et-la-protection-de-la-vie-privée>

قائمة المصطلحات

- **antivirus :** **مضاد الفيروسات:** برامج حاسوبية مصممة لتحديد البرمجيات الضارة وتحييدها ومحوها
- **cheval de Troie :** **حصان طروادة:** برنامج يتم تثبيته عن طريق الاحتيال لإكمال مهمة عدائية دون علم المستخدم (التجسس، وإرسال الرسائل غير المرغوب فيها على نطاق واسع
- **chiffrement :** **التشفير:** عملية غلق ملفات تستخدم لجعل من المستحيل على أي شخص ليس لديه المفتاح لفتح محتوى الملف
- **compte d'administrateur :** **حساب المدير:** حساب يسمح بإجراء تغييرات للمستخدمين تعديل إعدادات الأمان، تركيب البرمجيات، إلخ
- **logiciel espion :** **برامج التجسس:** برامج ضارة مثبتة في جهاز كمبيوتر لجمع ونقل البيانات والمعلومات، دون علم المستخدم في كثير من الأحيان
- **Fournisseur d'Accès Internet (FAI) :** **مزود خدمة الإنترنت:** الشركة التي توفر لعملائها إمكانية الوصول إلى شبكة الإنترنت .
- **mise à jour :** **التحديث:** إجراء لتحسين أداة أو خدمة تكنولوجيا المعلومات عن طريق تنزيل إصدار جديد
- **pare-feu (firewall) :** **جدار الحماية:** برامج و أجهزة لحماية البيانات عن طريق تصفية المدخلات والتحكم في النواتج وفق القواعد التي يحددها مستخدموها
- **paquet :** **الحزمة:** وحدة إرسال البيانات المستخدمة للاتصال
- **phishing (hameçonnage) :** **التصيد الاحتيالي:** طريقة هجوم تحاكي منظومة مؤسسة أو شركة (مصرف، سلطات ضريبية) لتشجيع الطرف على تقديم معلومات شخصية
- **routeur :** **جهاز التوجيه أو الراوتر :** عنصر وسيط في شبكة حاسوبية تقوم بتوزيع حزم البيانات عن طريق تحديد عقدة الشبكة التالية التي يجب إرسال الحزمة إليها
- **système d'exploitation :** **نظام التشغيل:** برمجيات تتحكم في مكونات الأجهزة الإلكترونية وتتلقى تعليمات الاستخدام من المستخدم أو برمجيات أخرى

- **المستخدم:** الشخص الذي يستخدم نظاما حاسوبيا
- **ويب:** بروتوكول أمني لتوفير مستخدمى الشبكة المحلية والحماية اللاسلكية من القرصنة ؛
- **الواي فاي:** اتصال لاسلكي بالإنترنت
- **ويبياء 2:** معيار أمني يحمي المستخدمين من قرصنة الشبكات اللاسلكية
- **WPA 2 :** ليحل محل نظام ويب الذي يعتبر غير كاف


تم صياغة وترجمة هذا الدليل كوثيقة داعمة
للدورة التكوينية لتحسين المهارات في مجال
الأمن الرقمي و التحسيس بأهمية حماية
البيانات الشخصية.



Association Tunisienne de Prévention Positive
29 Rue Bichara Al Khouri, El Omrane
1005 Tunis - Tunisie

Tél : +216 71 896 901/ +216 71 896 023

Email : atpplus@atpplustunisie.com

 Association Tunisienne De Prévention Positive

 [atp.plus](https://www.instagram.com/atp.plus)