إلدار كودينوف • ميشيل دياكوف • فاسيلي يالتونسكي • دينيس فيشر

العالم الرقمي

نصائح عملية للحفاظ على حياتك على الانترنت آمنة

الناجين

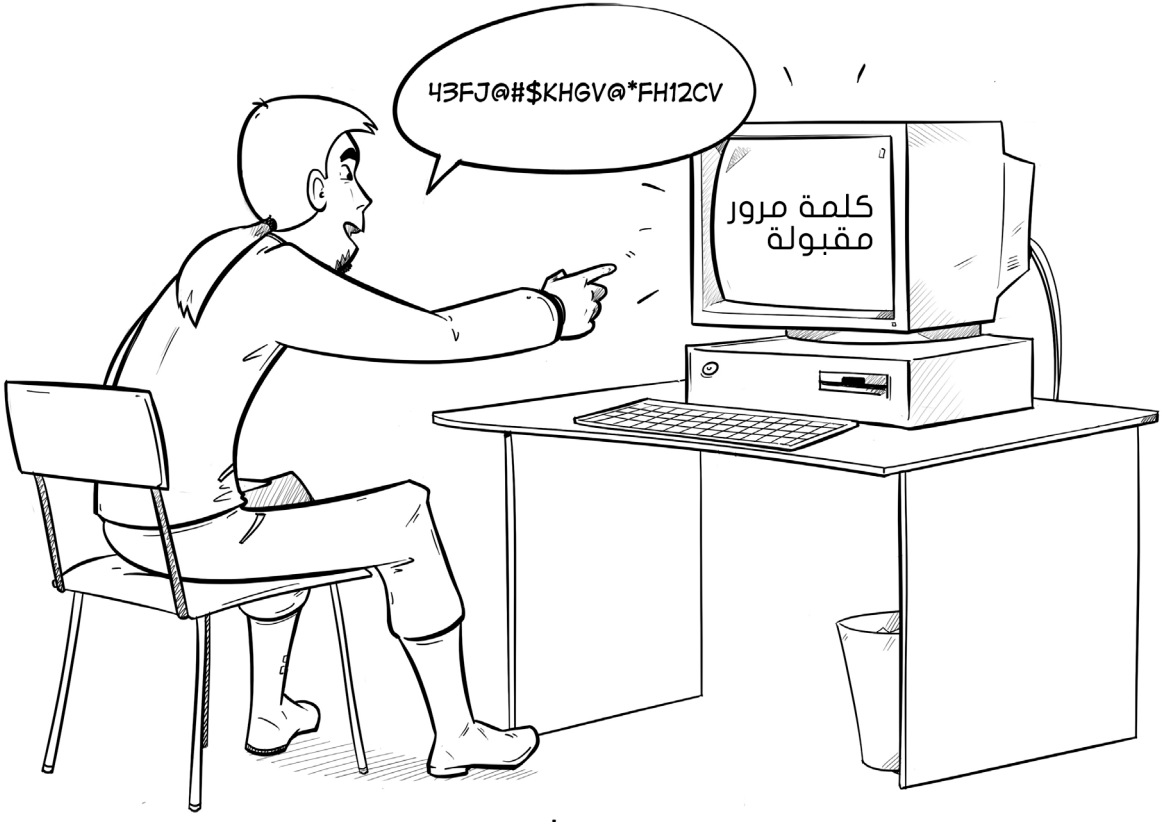
KASPERSKY lab

المقدمة

فجر العصر الرقمي لا يبدو كما توقعنا. أجهزة الكمبيوتر والهواتف المحمولة منحت الناس الوصول إلى كميات هائلة من المعرفة وطرق جديدة لا نهاية لها ؛ حياتنا هي أسهل وأفضل بفضل التكنولوجيا الجديدة والإنترنت. ومع ذلك، جاءت كل هذا الخير أيضا مع الجانب السلبي الكامل من سرقة المعلومات الشخصية، والبرمجيات الخبيثة، ومجموعات من المجرمين الذين يستخدمون الويب وملعبهم الشخصي. والخبر السار هو أن هناك أشخاصا يقاتلون هذه الفوضى، وهم على استعداد لتقاسم خبراتهم ومعرفتهم مع الجيل القادم. لذا ينتهي الجزء المظلم من الأسطورة وتبدأ قصتنا ...

نصيحة ١: معلومات مفيدة

مجرد تخيل: فيروس يتسلل جهاز الكمبيوتر الخاص بك عن طريق شبكة الهاتف، يتحول في منتصف الليل ويرسل أمر لإطلاق صاروخ. انه سيناريو هوليوود ولكن في العالم الحقيقي، والبرمجيات الخبيثة عادة ما تعمل بطريقة مختلفة جدا ولها غرض مختلف. ضعف أنظمة الكمبيوتر وحقيقة أن المستخدمين لا يعرفون المبادئ الأساسية لأمن المعلومات هي المكونات الرئيسية لنجاح أي جهاز من البرمجيات الخبيثة. قد يبدو الامر لا يصدق، ولكن القراصنة لا تحتاج إلى كتابة الكثير من المعلومات الغريبة بينما يلعب الموسيقى مخيفة في الخلفية إذا كان يريد أن تصيب جهاز الكمبيوتر الخاص بك. هناك بريد إلكتروني واحد يحتوي على ملف ضار مرفق. إذا اعتقد الضحية الرسالة مشروعة، وقالت انها سوف تبدأ التطبيق الخبيثة نفسها. لذلك من أجل الدفاع ضد مجرمي الإنترنت، يجب أن نفهم ما هي التهديدات.



كن مبدعا حقا عند إنشاء كلمات المرور ...

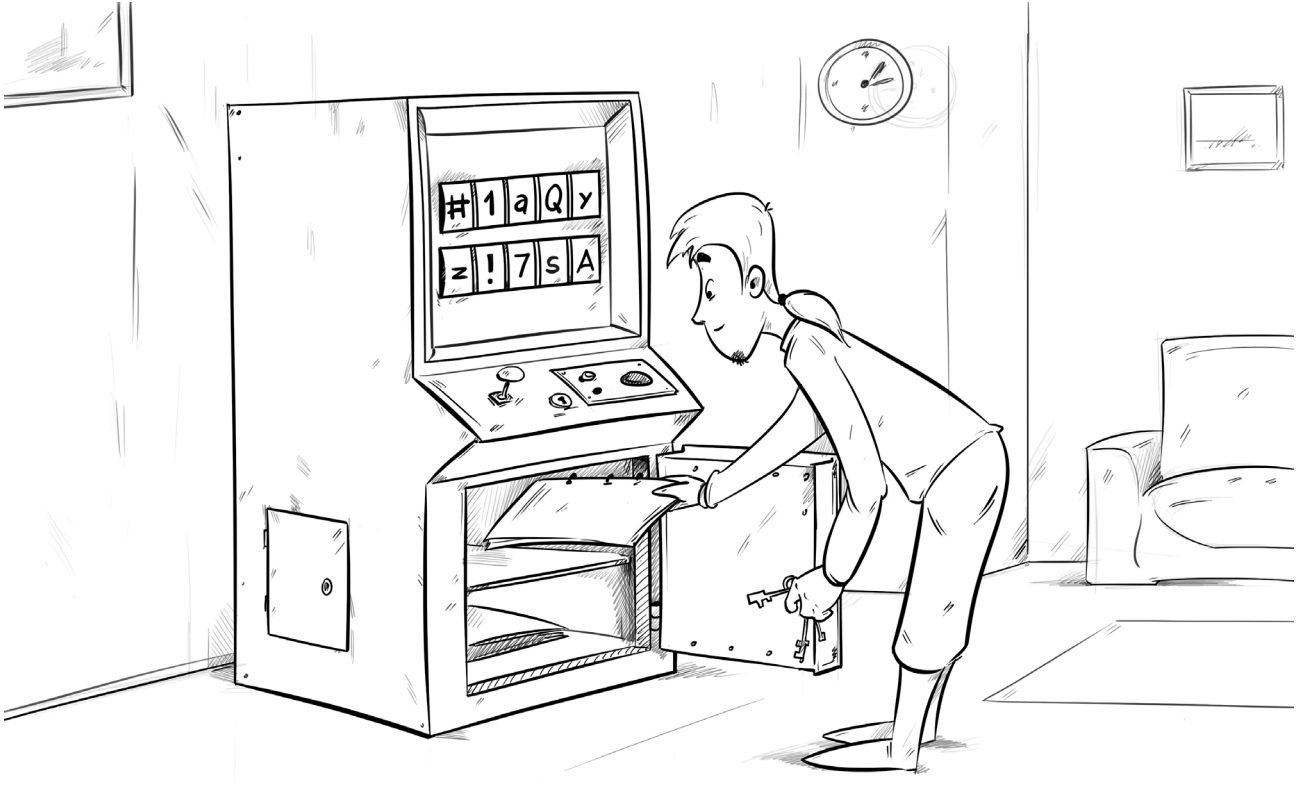
نصيحة ٢: قوة كلمة المرور

عادة ما يبدأ الهاكرز عملهم باستخدام مفردات خاصة تحتوي على ملايين كلمات المرور التي كانت تستخدم سابقا أو تسربت عبر الإنترنت. هناك العديد من الناس على هذا الكوكب الذين يعتقدون تماما مثلك، لذلك قد تكون كلمة المرور الخاصة بك على تلك القائمة. يجب ألا تستخدم الكلمات الشائعة أو كلمات الأغنية أو عنوان الفيلم أو اسم القط أو تاريخ ميلادك أو أي نوع من المعلومات التي يمكن تخمينها أو العثور عليها بسهولة على مواقع التواصل الاجتماعي ككلمة مرور.


كلمات السر القوية
تهزم وتجعلهم غير اقوياء
تم
الرفض

نصيحه ٣: كلمه مرور قويه

الاقترانات هي أسهل طريقه لإنشاء كلمه مرور صعبه. خذ عبارة مقترنة بالخدمة أو موقع ويب الذي تقوم بتسجيل الدخول له ، واكتبه ، وأضف بعض الأرقام والحروف. الآن هذه كلمه مرور قويه. هذه كلمه السر من السهل ان نتذكر ويجعل من المنطقي تكون فقط لك.

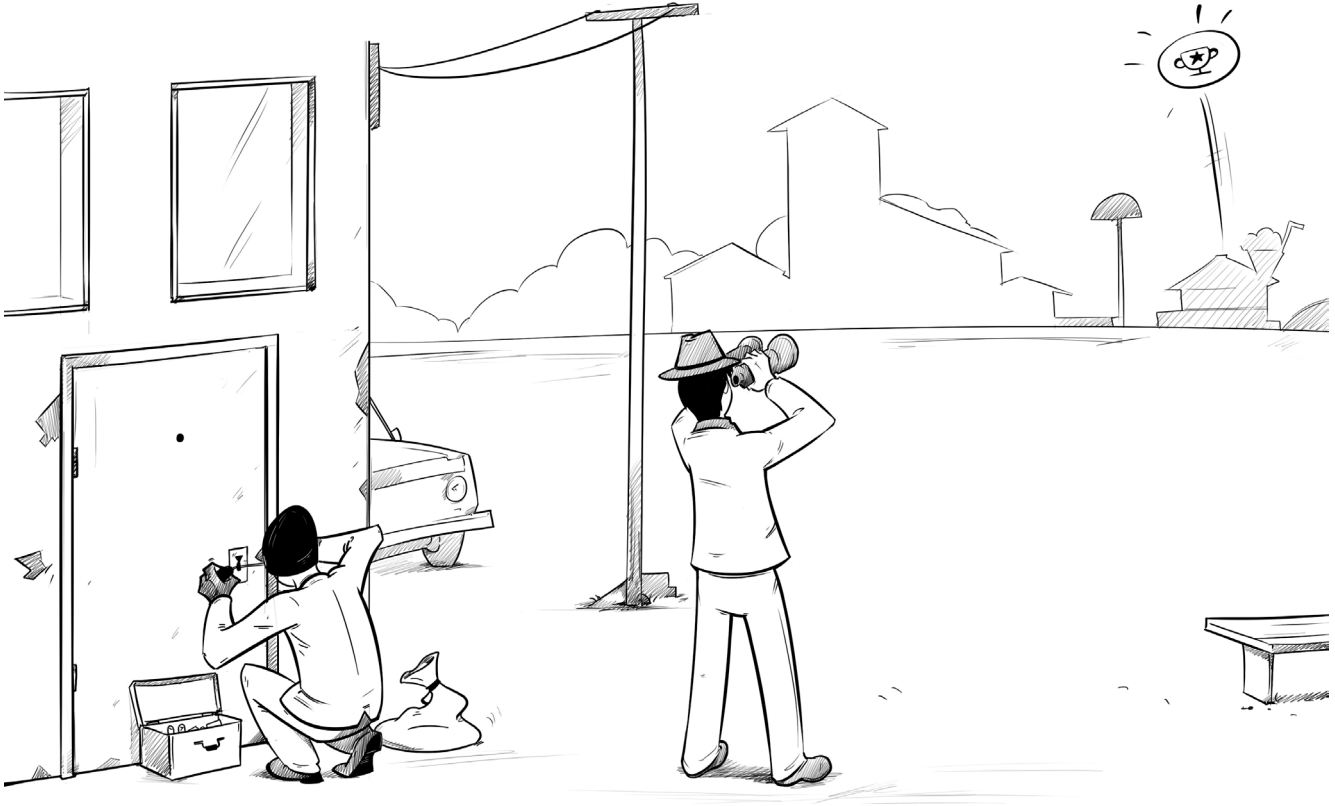


استخدم **ادارة كلمة السر** لتخزين كلمات السر الخاصة بك ،وليس الحفظ في مذكرة

نصيحة ٤: تخزين كلمه السر

كلما كانت كلمه المرور أكثر صعوبة ، سيكون من الصعب تخمينها. أسهل كلمه السر ، وأسهل هو ان نتذكر. لذلك ينبغي ان يكون من الصعب والسهل علي حد سواء--وليس الجميع قادره علي التذكر. إذا كان التلميح 3 لا يناسبك ،قم استخدام كلمه السر الخاصة مدير التطبيق. وسوف تخلق هذه التطبيقات صعبه ، وكلمات السر الفريدة لخدمات الإنترنت ، ووسائل التواصل الاجتماعية ، والتطبيقات وما إلى ذلك ، ثم حفظها في قاعده البيانات المشفرة. الشيء الوحيد المتبقي لك هو إنشاء كلمه مرور رئيسيه واحده للمدير. تذكر: كلمه السر يجب ان تكون صعبه حتى لا يمكن لأحد ان يخمن ذلك ، وانه من السهل ان نتذكر!

هل تعلم ان التسجيل بوجودك في المقهى ليست خاصه



نصيحة ٥: التجسس الظاهري

في الماضي المجرمين سوف تري عن بعد ، شقتك ، منزل البلد أو السيارة. ولكن كل هذا ليس كل ما يثير الاهتمام والخروج من التاريخ. لصوص اليوم يمكن فقط الاشتراك في الاخبار الخاصة بك في وسائل التواصل الاجتماعية لمعرفه أين أنت لا ينبغي لك جعله عاده اتسجيل وجودك في كل مكان. فكر في عدد الأصدقاء الحقيقيين والقدامى الموجودين في حساب الفيسبوك في المرة القادمة التي تقوم فيها بالتسجيل.


تقاسم ممتلكاتك الشخصية
بشكل متزايد يمكن أن يؤدي
إلى السرقة
١٢٠٠ $
٣٤٠ $
٢٧٠٠ $

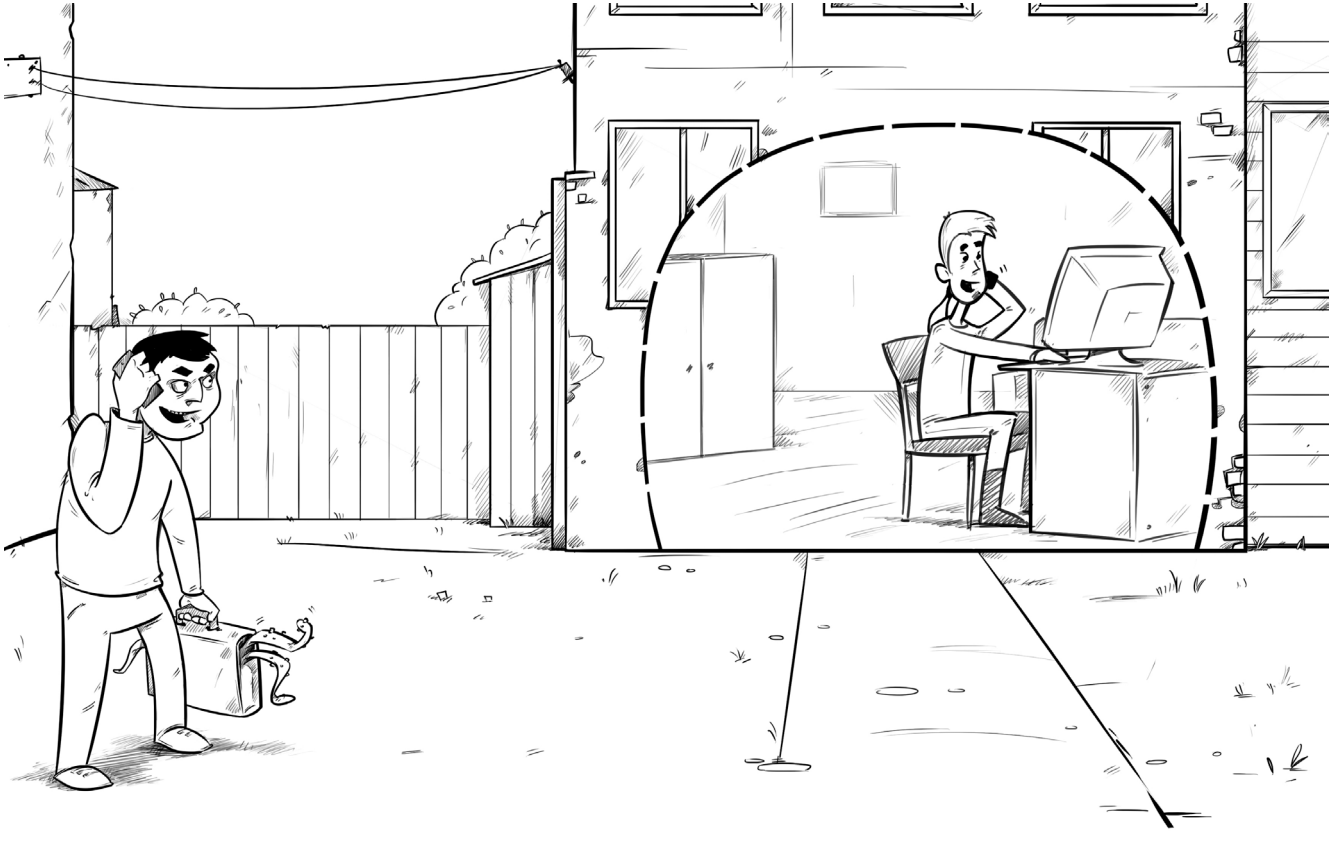
نصيحة ٦: حياة جميلة

يمكن للمجرمين استخدام وسائل التواصل الاجتماعية وربما أفضل لأن هذه المهارات مفيدة حقا في جعلها مربحه واسهل. يجب أن تكون أكثر تواضعا في الحياة الافتراضية لسلامتك الخاصة كصور لك شقة فاخرة، سيارة جديدة أو كمبيوتر محمول باهظ الثمن على شبكة الإنترنت أو المعلومات التي عليك أن تكون في إجازة مع أحد أفراد أسرتك الأسبوع المقبل يمكن أن تجعلك هدفا.

قد تستخدم كاميرا الويب للتجسس عليك

نصيحة ٧: الجاسوس لا يمكن تفسيره

كاميرات الويب مثالية للأشخاص الذين يعيشون أصدقاؤهم أو أقاربهم بعيدا. ولكن، من فضلك، تأكد من أن الكاميرات الخاصة بك لن تظهر المتجاوزين لك الحياة الخاصة. يمكن للقراصنة استخدامها بطرق مختلفة. كل هذا يتوقف على الخيال والقصة . يمكنهم بيع الصور والفيديو إلى موقع إباحية أو ابتزاز المستخدم. إذا كنت لا تريد مثل هذه المشكلة أن يحدث لك قم باستخدام تطبيق مكافحة الفيروسات التي من شأنها السيطرة على الوصول إلى الكاميرا.



مدير دعم ويندوز هو شخصية شعبية المستخدمة من قبل المحتالين

نصيحة٨: تليفون الاحتيال

"مرحبا، أنا متخصص من ويندوز الدعم الفني. هناك فيروس خطير جدا على جهاز الكمبيوتر الخاص بك، "- وهذا هو بداية ممكنة للحديث مع المخادع عبر الهاتف. كل شيء سهل الآن: يقنع المتعاقد المستخدم بأن جهاز الكمبيوتر الخاص به مصاب، ثم يوصي للقيام ببعض الإجراءات التي من شأنها أن تساعد بالتأكيد. ولكن البرمجيات الخبيثة الحقيقية هي الإجراءات التي ""ينصح"" من قبل ""المتخصص"". لذا تذكر مرة واحدة وإلى الأبد: ميكروسوفت الدعم الفني لاتقوم بالاتصال بغض النظر عن عدد الفيروسات الموجوده على جهاز الكمبيوتر الخاص بك.