

3 طرق يستولي بها الهاكرز على حسابك .. كيف تحمي نفسك منها؟



الاثنين 10 أبريل 2017 07:04 م

تستيقظ في الصباح، وترغب بإلقاء نظرة على بريدك الإلكتروني أو حسابك على إحدى الشبكات الاجتماعية أو الولوج لحسابك في إحدى المواقع لتفاجئ برسالة مفادها أن كلمة المرور الخاصة بحسابك تم تغييرها، ودون أن تكون أنت من قام بذلك

السيناريو السابق قد مر على الكثير من مستخدمي الإنترنت في مرحلة من المراحل، لكن إن كنت ترغب بعدم تكرار هذا السيناريو أو تجنبه إن لم يكن قد مر عليك سابقاً فإليك 3 طرق لكيفية استيلاء الهاكرز على حسابك وكيفية حماية نفسك منها

تدوير كلمات المرور

أحد الطرق المعروفة لاستيلاء القراصنة على الحسابات، هي الحصول على كلمات المرور من خلال عمليات تسريب البيانات لمواقع وخدمات مختلفة وتبادلها فيما بينهم

فمثلاً عند تمكن الهاكرز من الوصول إلى قاعدة بيانات خدمة أو موقع معين فإنهم يقومون بنشر معلومات المستخدمين بما في ذلك الأرقام السرية لحساباتهم، وبالطبع إن كنت أحد الهاكرز وتقرأ هذا المقال فأنت تعرف جيداً من أين تحصل على هذه البيانات

وبالطبع تسارع هذه الخدمات (التي تم الوصول إلى قواعد بياناتها من قبل الهاكرز) بالطلب من المستخدمين تغيير كلمة المرور الخاصة بهم

لكن المشكلة لا تكمن في اختراق الخدمة نفسها فقط، فبعد أن يتم مشاركة هذه البيانات بين الهاكرز، فإنهم يقومون بتجربة هذه الحسابات على خدمات ومواقع أخرى بنفس البريد وكلمة المرور

كيف تحمي نفسك؟

ببساطة شديدة لكي تتجنب هذه المشكلة يجب عليك استخدام كلمات مرور مختلفة لحساباتك على شبكة الإنترنت، بحيث تضمن عدم الوصول إلى حساباتك الأخرى نتيجة اختراق حساب على خدمة مختلفة

شبكات واي فاي غير الآمنة

أنت في مكان عام، تريد استخدام الإنترنت، أخرجت هاتفك الذكي وقمت بالبحث عن الشبكات اللاسلكية المتاحة، وفجأة ظهرت لك شبكة لا تحتاج إلى كلمة مرور

يا إلهي ستقوم بالاتصال بها على الفور والسعادة الغامرة على وجهك، لكن قد تنقلب هذه السعادة إلى سرقة كافة بياناتك

الكثير من المستخدمين لا يولون أهمية لأمن شبكات واي فاي قبل الاتصال بها، وهي مسألة في منتهى الحساسية

فيمكن ببساطة تعقب موقعك وجمع بعض المعلومات عنك عند استخدام هذه الشبكات، أما السيناريو الأسوأ (لأصحاب الحظ العاثر) هو وصول أحد الهاكرز إلى كافة بياناتك بما فيها معلومات حساباتك على بعض المواقع والخدمات

كيف تحمي نفسك؟

قدر الإمكان لا تتصل إلا بشبكات واي فاي آمنة، كما يُنصح بتفعيل أحد تطبيقات VPN على هاتفك عند استخدام شبكة واي فاي في الأماكن العامة

يمكن أيضاً أن تعتمد على تطبيقات الهواتف الذكية المتخصصة في فحص شبكات واي فاي والتأكد من أمنها وتشفيرها

السؤال السري

هناك استهتار كبير من قبل المستخدمين بالسؤال السري الذي يظهر لهم عند تسجيل حساب في موقع أو خدمة معينة

السؤال السري وضع بالأساس كخطوة تساعدك على استرداد حسابك في حال عدم قدرتك على الوصول له، وبالتالي يجب أن تأخذ الأمر على محمل الجد

الهاكرز خصوصاً على بعض الشبكات الاجتماعية، يقومون باستخدام هذه الحيلة لإعادة تعيين كلمة المرور الخاصة بالمستخدم من خلال تخمين السؤال السري

فهناك بعض الأسئلة السرية السهلة للغاية مثل المدينة التي ولدت فيها، أو الكلية التي تخرجت منها؟ ويمكن للهاكرز الوصول إلى هذه الإجابات من خلال نظرة سريعة على حسابك على فيس بوك

كيف تحمي نفسك؟

قم باختيار أسئلة سرية صعبة للغاية بحيث يستحيل على الهاكرز تخمينها، وقم بتدوين الأسئلة والإجابات في مكان آمن إن كنت تخشى نسيانها

كانت هذه بعض الطرق التي يستخدمها الهاكرز للاستيلاء على حسابك، وستتعرف خلال النصائح القادمة على طرق أخرى إن شاء الله