

كيف تمنع المتطفلين من استخدام حسابك على Gmail؟



الأحد 30 يوليو 2017 02:07 م

لو كنت تشك أن شخصاً اخترق حسابك على Gmail، وتتساءل كيف بإمكانك إيقاف الأمر، فهذا سؤال شائع نسبياً، ويأتي أحياناً بصيغ مختلفة، مثل: "كيف أتعامل مع المُخترق الذي يستعمل حساب Gmail الخاص بي، للاستيلاء على بيانات لعبتي ألعابها؟".

ولكن كيف علمت بالأمر؟

قد تكون مثلاً قد وجدت رسائل مجهولة في بريدك الصادر تعرف أنك لم ترسلها، لكن هذا احتمالٌ بعيدٌ بعض الشيء، فعادةً ما يجيد المخترقون إخفاء آثارهم بإلغاء أي نسخةٍ مُسجَّلة في الرسائل الصادرة

غير أن الرسائل الواردة ليست مؤشراً على أي شيءٍ ربما تعتاد على تلقي رسائل من إنستغرام، وآبل، وبرايفيل، وغيرها من المنظمات والشركات التي يُسجَّل فيها أشخاص البريد الإلكتروني - بالخطأ ربما! لكن هذا لا يعني هذا أنهم يستطيعون الدخول إلى حسابك

أفضل طريقة للتأكد من اختراق حسابك، أو أن شخصاً آخر قد استخدمه، هي بتحريك الفأرة إلى أسفل الشاشة الرئيسية للبريد الإلكتروني حتى تصل إلى "آخر نشاط للحساب - Last account activity"، في الركن الأيمن وبالضغط على "تفاصيل"، سيظهر لك جدول يُمكنك من معرفة كيف استطاع أي شخص الدخول إلى حسابك (سواء كان من مُتصفحٍ، أو هاتفٍ محمول، أو بروتوكول مكتب البريد، إلخ)، وسيتاح لك كذلك معرفة عنوان بروتوكول الإنترنت (IP address) الخاص بهم، وتوقيت وتاريخ دخولهم إلى حسابك بالتحديد يُمكنك أن تميِّز بالطبع أي نشاطٍ لا يخصك على الحساب الإلكتروني، بحسب صحيفة The Guardian البريطانية

ولكن هناك ميزة أخرى في Gmail، فهو يُنبِّهك عند حدوث أي نشاطٍ غير معتاد، وبالتالي قد يصلك أي إشعارٍ يتعلَّق بجهازٍ جديدٍ يُستخدم للدخول، أو بمحاولة الدخول من بلدٍ آخرٍ قد تجد هذه الإشعارات مُزعجة، لكنها شديدة الأهمية لضمان الأمان، لذا لا تغلقها

يمكن كذلك الذهاب إلى صفحة "الأجهزة المستخدمة حديثاً - Recently used devices"، والتي تمدك بقائمةٍ تحتوي على جميع أجهزة الكمبيوتر، والهواتف المحمولة، والأجهزة اللوحية المستخدمة في آخر 28 يوماً دخلت فيه إلى حسابك، وبالمثل سيكون من السهل عليك تمييز أي نشاطٍ لا يخصك

إعدادات التحقق المزدوج - Double Check Settings

هناك طرق بسيطة لقراءة الرسائل في حساب شخص ما دون ترك دلائل واضحة، ويمكن التحكم فيها من إعدادات Gmail، وتستطيع الوصول إليها بالضغط على علامة الترس في أعلى اليمين

في صفحة الإعدادات، اضغط على "حسابات وواردات - Accounts and Import"، واذهب إلى الخانة قبل الأخيرة: "احصل على طريقة للوصول إلى حسابك - Grant access to your account". يمكن لأحدهم أن يضغط على إضافة حساب جديد، ثم يدخل حساب جيميل آخر، وهذا سُمِّحته من الدخول إلى بريدك الإلكتروني من الحساب الذي أضفاه، وقراءة رسائلك دون أن يتركها "مقروءة".

بعدها، اضغط على "الصادرات و بروتوكول مكتب البريد/ بروتوكول الوصول إلى رسائل الإنترنت - Forwarding and POP/IMAP"، وافحص الجانب العلوي من صادرات البريد

تتيح خدمات البريد الإلكتروني للمستخدمين أن يعيد بريدهم الإلكتروني توجيه الرسائل الواردة إلى بريدٍ إلكتروني آخرٍ أعتقد أنه يجب على

كل شخص أن يُفعل هذه الخاصية وبشكل شخصي، ضبطت إعدادات Gmail ليعيد إرسال كل الرسائل الواردة إلى حساب بريدي الإلكتروني على موقع أوتلوك، وبهذا أستطيع قراءة الرسائل الواردة والرد عليها، حتى لو لم تستطع الدخول إلى Gmail. والأهم، أنه حتى لو منعك Gmail من دخول حسابك الشخصي، فسيكون بحوزتك رسائل تعود إلى أبريل 2004 مثلاً

لذا، إذا كان باستطاعتك الدخول إلى صندوق بريد شخص ما، يمكنك إعداد نظام إعادة الإرسال ليُرسل نسخة من كل رسالة تصل إلى هذا البريد الإلكتروني إليك، وغالباً لن يلاحظ أحد الأمر! تأكد فقط أن هذا لا يحدث معك

فلو كنت تستخدم حساب Gmail الخاص بك فقط عبر المتصفح، يمكنك كذلك تعطيل خاصيتي بروتوكول مكتب البريد، وبروتوكول الوصول إلى الرسائل عبر الإنترنت! سيوفر هذا بعضاً من الحماية، لكنني لا ينصح بهذا على كل حال

توجد العديد من المزايا في استخدام برامج البريد الإلكتروني على الكمبيوتر الشخصي، مثل ميكروسوفت Outlook، أو Thunderbird، أو Im client لتجميع رسائل Gmail عبر بروتوكول الوصول إلى الرسائل عبر الإنترنت ولدى هذه البرامج خصائص أكثر من نسخة المتصفح العادي لـ Gmail، فيمكنها مثلاً تخزين الرسائل على جهازك لتستطيع الدخول إليها حتى لو لم تكن متصلاً بالإنترنت

ويترك بروتوكول الوصول إلى الرسائل عبر الإنترنت البريد الإلكتروني متصلاً بالإنترنت، ما يعني أنه يمكنك تصفحه باستخدام أجهزة أخرى، حيث يمكنك تحميل تطبيق جيميل أوفلاين من خلال تبويب عدم الاتصال بشبكة الإنترنت - (Offline tab).

تأمين كلمة المرور

بمجرد التأكد من أن حسابك لم يتعرّض للاختراق، قم بتغيير كلمة المرور لمزيد من الأمان

في Gmail، عد مرة أخرى إلى حسابات وواردات - Accounts and Import، واضغط على تغيير كلمة المرور - Change password.

اختر كلمة أو عبارة مرور قوية، تتضمن أرقاماً وأحرفاً كبيرة يجب أن تتألف كلمة المرور من 8 أحرف على الأقل، لكن حاول أن تكون كلمتك ما بين 12 و16 حرفاً، أو حتى أكثر من ذلك، فكلما طالت الكلمة كان ذلك أفضل لا يجب أن تكون الكلمة عشوائية، إلا لو كنت تستخدم برنامجاً لتوليد كلمات المرور! تجنّب استخدام أسماء أفراد العائلة، أو الحيوانات الأليفة، أو تواريخ الميلاد، وكذلك الفرق الرياضية المفضّلة، أو أي عنصر واضح آخر

يمكن أن يحفظ المتصفح الخاص بك، أو برنامج توليد كلمة المرور، كلمة مرورك! لو سمحت بهذا، فسيرتبط أمان بريدك الإلكتروني بأمان جهاز الكمبيوتر الشخصي، وبالتالي سيُتاح لأي شخص يستطيع استخدام جهازك الدخول إلى بريدك الإلكتروني

لكن أسهل طريقة لاختراق البريد الإلكتروني هذه الأيام هي باستخدام روابط مُخدّعة في هذه الحالة، يفتح الضغط على الرابط تبويماً في المتصفح الخاص بك، وستطلب منك صفحة تدّعي أنها غوغل أن تُسجّل دخولك بكتابة بريدك الإلكتروني وكلمة المرور، وسُترسل هذه البيانات إلى المُخترق مباشرة

لو تركت جهازك الشخصي دون حماية، أو ضغطت على أحد هذه الروابط المُخدّعة، لن يهتم مدى قوة كلمة مرورك على أي حال

فعل خاصية التحقق على خطوتين - Two-step verification

إذا استطاع شخص الدخول إلى الحساب الخاص بك، سيكون بإمكانه تغيير كلمة السر وحرمانك من الدخول! لكن على أي حال، يمكنك منع هذا عن طريق خاصية التحقق على خطوتين

في جيميل، يعني هذا غالباً أن جوجل سترسل كوداً إلى هاتفك المحمول! عيب هذه الخاصية الوحيد هو حالات انقطاع الشبكة، أو فقدان الهاتف! وفي هذه الحالة، سيطلب Gmail رقماً هاتفياً احتياطياً (يمكنك تلقي رسالة صوتية عبر الخطوط الأرضية). ويتيح لك Gmail أيضاً فرصة طباعة مجموعة من أرقام التأكيد، والتي يمكنك التحرك بها في أثناء السفر

يوفر جوجل بديلاً عن الرسائل النصية القصيرة، في صورة جوجل أوثينتيكيتور - Google authenticator، وهو تطبيق خاص بأجهزة أندرويد وآبل

ويمكنك تبسيط عملية التحقق على خطوتين، باستخدام كلمات مرور مُخصّصة للتطبيقات! على سبيل المثال، لو ولجت إلى جيميل عن طريق تطبيق خاص بالهواتف الذكية، أو عميل بريد إلكتروني لا يستطيع التعامل مع التحقق على خطوتين، يُمكن أن تطلب كلمة سر منفصلة لكل برنامج بريد إلكتروني على كل جهاز! يجب إدخال هذه الكلمة مرة واحدة فقط

لاستخدام خصائص الحماية الإضافية في Gmail، اذهب إلى "حسابات وواردات"، اضغط على "إعدادات حساب جوجل الأخرى - Other Google Account settings"، وبعدها "تسجيل الدخول والأمان - Sign-in & security". سيتيح لك هذا الاطلاع على أي تغييرات طرأت على كلمة المرور، والتحقق على خطوتين، وخيارات استعادة الحساب

ماذا لو أنك تُدخِل كلمة السر الخاصة بك ولكنك لا تستطيع الدخول إلى حسابك على Gmail؟

عادةً تكون أولى الخطوات في عملية استعادة الحساب، هي طرح بعض الأسئلة الشخصية، مثل اسم عائلة الأم □ سَمَحَ هذا للعديد من الأشخاص باختراق حسابات البريد الإلكتروني باستخدام معلومة متاحة على الشبكات الاجتماعية □ تستطيع منع هذا، عن طريق استخدام حروف عشوائية، أو كلمات ليس لها معنى، مثال: اسم عائلة الأم: Quetzalocatl. لكن احرص على تذكّر الإجابات □

تتضمّن عملية استعادة الحساب في جوجل رقم الهاتف، وبيداً إلكترونياً آخر، وسؤالاً سريعاً □

سُئِلَ كذلك عن تاريخ إنشاء هذا الحساب، وآخر مرة استخدمته فيها □

يمكنك معرفة تاريخ إنشاء الحساب عن طريق البحث قبل تاريخ 15/4/2004 (كما في حالتي)، أو أي تاريخ مكتوب بصيغة اليوم/الشهر/السنة □ لن تفلح هذه الطريقة لو كنت قد أزلت رسالة الترحيب، لكن على أي حال حاول التنويع في التواريخ حتى تصل إلى أقدم رسالة □

عملية استعادة الحساب هي الطريقة الوحيدة لاستعادة حساب بريدك الإلكتروني مرة أخرى، وذلك في حال نسيانك لكلمة المرور، أو إذا غَيَّرَهَا مُخْتَرِقٌ هاجَمَ حسابك □ لكنها لا تصلح دائماً، وقد يخبرك Gmail في النهاية بأنّ: "لا يمكن تسجيل دخولك، لأن غوغل لم تستطع التأكد من أن الحساب الفلاني يخصك".

ثم بعدها، ينتهي بك الأمر في "دوامٍ من محاولات استعادة الحساب المُتكرِّرة، دون خدمة عملاء، ولا محادثة فورية، ولا تفاصيل عن قائمة الأشخاص". ولا يبقى في يدك إلا أن تفتح حساباً جديداً، وتغيّر كلمات مرورك كلها وعناوين بريدك الإلكتروني، وتأمّل ألا يستغل أحدهم حسابك في ارتكاب جريمةٍ ما □