

إختراق حسابات الفيسبوك حقيقة أم خيال ؟



تعرف على طرق إختراق حسابات
الفيسبوك وعش بأمان في الفيسبوك

تأليف

سرور نور

@Soroor_Noor

المقدمة

بسم الله الرحمن الرحيم الصلاة والسلام على أشرف الأنبياء والمرسلين سيدنا محمد وعلى آله وصحبه أجمعين اللهم علمنا ما ينفعنا وأنفعنا بما علمتنا إنك أنت العليم الحكيم أما بعد : في الفترة الأخيرة إنتشرت في موقع الفيسبوك منشورات وهمية مثل :

فتح كاميرا أي شخص في الفيسبوك ، ضع علامة الوثوق في حسابك في الفيسبوك الخ .. كل هذه المنشورات وهمية ويضع في المنشور رابط يوتيوب لشرح وضع كود في (console) في المتصفح وبمجرد وضع الكود والضغط على Enter يتم النشر نفس المنشور (أو أي منشور يحددها صاحب الكود) في جميع المجموعات المشتركة بها أنت ويتم تسجيل إعجابات لصفحات لاتعرفها وأشياء كثيرة يمكن معرفتها من خلال زيارة سجل النشاطات لحسابك من خلال الضغط على سهم الموجود بجانب علامة القفل الموجود في أعلى الصفحة الرئيسية للفيسبوك وقم بإختيار سجل النشاطات

فإذا وقعت في هذا الخدع فأنصحك بتغيير كلمة السر لحسابك فوراً .
وثق تماما أن لا يوجد برنامج أو ثغرة لمعرفة الكلمة السرية لحسابات الفيسبوك في الانترنت حتى وإن وجدت ثغرة فمكتشف الثغرة ليس غيبا أن ينشر الثغرة في المنتديات أوفي اليوتيوب أو في أي موقع آخر في الإنترنت .

فإذاً كل البرامج الموجودة في المنتديات والمدونات واليوتيوب الخ.. ملغومة
وكم من فيديو فيها إعجابات ومشاهدات كثيرة ولكنها للأسف يضع رابطاً أو
برنامجاً ملغوماً في الوصف وأنت تظنظ على الرابط أو ملف تحملها وتشغلها في
جهازك وتصبح أنت الضحية .

ويستطيع صاحب البرنامج الملغوم بالتحكم في جهازك وجلب الإيميلات والكلمات
السرية المحفوظة من المتصفحات
الموجودة في جهازك وتشغيل الكاميرا والميكروفون ومعرفة كل ماتكتبه بلوحة
المفاتيح وتصوير سطح المكتب الخ ..

وإن تسألني لماذا لا يوجد برنامج أو ثغرة للحصول على الكلمة السرية ؟

لأن شركة الفيسبوك تدفع الملايين لحماية أجهزتها وخصوصية مستخدميها من
السرقه

وهذا لا يعني أن لا يوجد ثغرة للحصول على الكلمة السرية نهائياً ولكنه صعب

الطرق اللذي يستخدمها الهاكرز الغير أخلاقيون لإختراق حسابات الفيسبوك

إختراق حسابات الفيسبوك عشوائياً سهل أما استهداف شخص معين هذا ليس سهل
أوصعب فهذا يعتمد على ذكاء الشخص وهو (الضحية)

ملاحظة مهمة : هناك فرق بين الطرق والثغرات والتي أذكرها هي طرق وليس ثغرات

موقع الفيسبوك

١-الصفحات المزورة

من الطريقة الشائعة والسهلة هي الصفحات المزورة في اختراق حسابات الفيسبوك
أوأي موقع من مواقع التواصل الإجتماعي والبريد الإلكتروني وهذه الطريقة غالبا
مايستخدمها هم أطفال الهاكرز لا أقصد بأطفال الهاكرز صغار السن أقصد بصغار
العقول

ماهي الصفحات المزورة ؟ هي صفحات شبيه بالأصلية ولكن عندما تقوم بتعبئة
بياناتك

في هذه الصفحة سترسل هذه البيانات الى صانع الصفحة وتتم سرقتها بكل سهولة
وهذه الطريقة إما يكون عشوائيا أو استهداف

وإذا وقعت في هذه الخدع فهي تدل على غبائك عليك أن تتأكد من رابط الموقع جيدا
وإن ذهبت الى الصفحة المزورة من حسابك على الفيسبوك فكيف يمكن أن تسجل
الدخول مرة أخرى من نفس المتصفح وأنت مسجل الدخول أليس هذا غباء وقم بتغيير
كلمة السر لحسابك وإذا تم سرقة قام بإسترجاعها (طرق إسترجاع حساب الفيسبوك
موجود في آخر الكتاب)

٢-الهندسة الإجتماعية

هي تجميع أكبر عدد من المعلومات عن الضحية ثم تجريبها على حسابه
مثل معرفة سؤال الأمان للضحية بخداعه وغيرها من المعلومات المهمة

والهاكر الغير أخلاقي يقوم بإنشاء موقع بإسم جذاب مثلا : اربح المال من خلال تعبئة هذه البيانات ويطلب من الضحية معلومات مهمة مثل : سؤال أمان أو كلمة السر فإحتمال كبير أن الضحية يضع نفس سؤال أمان والجواب أو نفس كلمة السر مثل ما وضعت في الفيسبوك وهكذا بكل سهولة يتم سرقة حسابه ولتجنب من هذه الخداع نصيحتي لاتستخدم كلمة سر أو سؤال أمان واحدة لعدة حسابات لاتعطي معلوماتك المهمة لأي شخص وهذه الطريقة استهداف

٥-التخمين

التخمين تعني جلب كلمة المرور عن طريق التفكير وتجميع أفكار والاحتمالات في مفكرة نصية ثم تجربتها دفعة واحدة بإستخدام نظام كالي لينكس أو ويندوز ببرامج مخصصة لها ولاكن الأفضل كالي لينكس وهذه الطريقة إستهداف

للتعرف أكثر عن هذه الطريقة قم بتحميل كتاب التخمين في العالم العربي

كتاب جميل جدا من عباقره من الهاكرز

رابط تحميل الكتاب

<http://goo.gl/vT3RZO>



٣-الكيوليجر(رصد لوحة المفاتيح)

إرسال جميع المعلومات التي يكتبها الضحية باستعمال لوحة المفاتيح إلى صانع السيرفر (server)

وهذه الطريقة سهلة ويتم ذلك عن طريق تكوين سيرفر (server)

السيرفر في إختراق الأجهزة هو : **ملف خبيث يربط بين الضحية وصانع السيرفر عبر منفذ معين**

ويتم إنشائه ببرامج مخصصة لها ومن أشهرها برنامج **Keylogger**

ويستطيع صانع السيرفر تشفيرها من برامج الحماية ودمجها بصورة أوفديو أو مع أي برنامج آخر وعندما يتم تشفير السيرفر لا يستطيع برنامج الحماية كشفها ولا يستطيع الضحية حذفها بشكل عادي لأنها يشتغل في الخلفية فيحتاج إلى برامج مخصصة لحذف السيرفرات ومنها البرنامج الشهير **procexp**

هذه الطريقة إما يكون استهداف أو عشوائيا

٤-إختراق جهاز صاحب الحساب

إختراق جهاز صاحب الحساب وسحب الكلمات السرية المحفوظة في المتصفحات و رصد لوحة المفاتيح (الكيولجر)..

وهذه الطريقة أخطر من الطرق اللذي ذكرتها في الأعلى لأنها إنتشرت بكثرة

لدى أطفال الهاكرز (njRAT) 

وأيضاً لأنها يمكن التحكم بجهاز الضحية وسحب الكلمات السرية من المتصفحات وتشغيل الكاميرا وتصويرها والتصنت على المايكروفون والتحكم بملفاتها وتصوير سطح المكتب وإيقاف تشغيل الجهاز وإخراج القرص من محرك الأقراص وغيرها الكثير من الأشياء ..

ويتم ذلك عن طريق تكوين باتش أو سيرفر باستعمال برنامج الشهير **njRAT** أو أي برنامج آخر يعمل بنفس الوظيفة

السيرفر في إختراق الأجهزة هو : ملف خبيث يربط بين الضحية وصانع السيرفر عبر منفذ معين

للإختراق بهذه الطريقة لايتطلب إلى ذكاء عالية فهي طريقة سهلة جداً ويستعمل هذه الطريقة بكثرة لدى أطفال الهاكرز لا أقصد بأطفال الهاكرز صغار السن أقصد بصغار العقول ويستطيع صانع السيرفر بتمويه السيرفر بدمجها بصورة أو فيديو أو بأي برنامج آخر

وتشغيلها من أي برنامج حماية لكي لايستطيع برنامج الحماية كشفها

وبعدها ارسال السيرفر إلى الضحية وفتح منفذ لإرسال والإستقبال ويصل التبليغ الى صانع السيرفر فور الضغط على السيرفر وهكذا يتم إختراق الجهاز والتحكم بها بكل سهولة

أو عن طريق إرسال رابط للضحية وبمجرد الضغط على الرابط يتم إختراق جهازه بواسطة أداة أرميتاج

أو عن طريق معرفة عنوان الأيبي الخاص بالضحية وإختراقها بواسطة ميتاسبلوبت

٥-بفتح بريد الكتروني متشابه

إنشاء بريد الكتروني متشابه ببريد الكتروني الضحية

هذه الطريقة ينجح إذ فتح الضحية حساب بإستخدام بريد الكتروني وهمي مثل: **yopmail, mohmal** أو فتح حساب لتأكيد الهوية ولم يراجع البريد لمدة طويلة جدا فيحذف عنوان بريده الإلكتروني من قاعدة بيانات الشركة الذي أنشأه حساب البريد الكتروني مثل: **hotmail** فيصبح هذا العنوان متاح لأي شخص وهنا يأتي دور الهاكر وبكل سهولة يقوم بفتح حساب بنفس العنوان وأخذ الحساب عن طريق إسترجاع كلمة السر للحساب وهذه الطريقة غالبا يكون عشوائياً

٦-التجسس على رسائلك دون معرفة كلمة السر

عندما تقوم تقوم بإشتراك في تطبيقات أو ألعاب في الفيسبوك يطلب منك الموافقة على بعض الصلاحيات فإنك توافق على بعض الصلاحيات المهمة مثل: النشر في بروفايلك ومعرفة البريد الإلكتروني .. ومعلومات مهمة جدا

ولكن للأسف المشكلة لا حد يقرأ ما هو مكتوب فلدينا ثقافة الضغط على **Next** حتى النهاية

والهاكر يقوم بإنشاء تطبيق مزيف بأسماء جذابة مثل : معرفة من يزور بروفايلك ، زيادة عدد المتابعين الخ ..

فصاحب التطبيق يعرف الأكسس توكن الخاص بك بمجرد الإشتراك في التطبيق

ويستخدم الهاكر الأكسس توكن (Access Token) الخاص بك للتجسس على رسائلك والنشر في بروفايلك الخ.. بدون معرفة كلمة السر لحسابك الذي أنت تعرفه وهذا الأكسس توكن يعتبر الباسورد الثاني لحسابك فأنصحك بالإبتعاد عن تطبيقات أو ألعاب غير موثوقة و قراءة صلاحياتها قبل الموافقة عليها وهذه الطريقة إما يكون عشوائيا أو استهداف وللحماية منها قم بتغيير كمة السر الخاص بحسابك وإزالة التطبيقات الغير الموثوقة من حسابك عبر الرابط التالي

<https://www.facebook.com/settings?tab=applications>

طرق لإستعادة حسابك تعرض للإختراق أونسيت كلمة السر

أضبط نسيت كلمة المرور من الصفحة الرئيسة للفيسبوك وأبحث عن حسابك بكتابة اسم حسابك أو البريد الإلكتروني أو رقم الجوال أو رقم الأيدي (اسم المستخدم) الخاص بحسابك في الفيسبوك وأختار الطريقة اللذي تريده في إسترجاع حسابك

١- بالبريد الإلكتروني

٢- برقم الجوال

٢- بالحصول على كود الإسترجاع لحسابك عن طريق تطبيق الفيسبوك الخاص بالجوال

٤- بتسجيل الدخول في البريد الإلكتروني المرتبط بحسابك

٥- بالإجابة على سؤال الأمان

٦- بمساعدة الأصدقاء

٦- لا تستخدم هذه الطريقة فوراً لأنه أصعب من الطرق المذكورة في الأعلى فإذا
لاستطيع إسترجاع حسابك بالطرق المذكورة في الأعلى اختر سؤال الأمان وإذا لا يوجد
سؤال الأمان في حسابك إتبع هذه الطريقة

وهي كالتالي:

اضغط على نسييت كلمة المرور وابحث عن حسابك وقم بالضغط على لم يعد لدي الوصول إلى هذه
وإختر استعد حسابك بمساعدة الأصدقاء

الخطوة الأولى : اختر ٣ من الأصدقاء الموثوق بهم

الخطوة الثانية : اتصل بأصدقاءك

الخطوة الثالثة : استعد حسابك

أفضل النصائح لحماية حسابك وجهازك من الإختراق

- أنشئ كلمة سر قوية واستخدمها في فيس بوك فقط
- قم بتغيير كلمة السر كل بعد فترة معينة
- قم بإضافة إعدادات أمان متقدمة لحماية حسابك مثل : منع تسجيل الدخول إلى حسابك إلا بعد إرسال رسالة إلى هاتفك فيها كود التأكيد لتسجيل الدخول إلى حسابك
- انتبه من الصفحات المزورة وتأكد من الرابط في كل مرة تسجل الدخول إلى حسابك
- قم بتسجيل الخروج من فيس بوك بعد استخدام كمبيوتر شخص آخر وتأكد من عدم حفظ كلمة المرور في المتصفح الخاص به
- احذر من المنشورات المزيفة الذي تنشر من أي شخص حتى أصدقائك اللذين تثق بهم فربما صديقك وقع في خدعة لصق كود في المتصفح ونشرت منشورات وهو لايعلم أو تم إختراق حساب صديقك ونشر روابط مزيفة وأنت لاتعلم
- تجنب الضغط على روابط غير معروفة
- تجنب تحميل الملفات أو البرامج من مصادر غير موثوقة
- لا تضيف أشخاص لاتعرفهم
- إحذر من التطبيقات الغير موثوقة مثل : زيادة عدد متابعين ،إعرف من زار بروفايلك ، حتى تطبيقات ذكر الله لأن للأسف في هذا الزمن القليل من الناس يخافون الله وحتى وصل لدرجة الحلف كذبا لكسب عدد المشاهدات في اليوتيوب ..و الربح منه
- حافظ على تحديث برنامج مكافحة الفيروسات
- شغل إضافة الجافا في المتصفح عندما تحتاجها فقط

وأخيراً أحب أن أقول لك إختراق الفيسبوك ليس شيئاً مستحيلاً ولكنه شبه مستحيل

أتمنى أن وصلت فكرة إختراق الحسابات وأتمنى وأتمنى من صميم القلب أن
تنشرو هذا الكتاب حتى يستفيد الجميع وإن شاء الله أضع شروحات في
اليوتيوب لجميع الطرق اللتي ذكرتها في الأعلى ليس الهدف من وضع
الشروحات تعلم الإختراق

وإنما لكي تعرف كيف يخترق الهاكرز الغير أخلاقيون حسابك وتحمي نفسك
(للحماية)

وأنا أبرئ ذمتي أمام الله من أي إستخدام خاطئ لمحتوى هذا الكتاب
قناتي على اليوتيوب: إشتراك في القناة حتى يصلك الفيديوهات أولاً بأول

<http://www.youtube.com/user/soroor3noor>

للتواصل معي ولأي استفسار :

البريد الإلكتروني:

rore0770@gmail.com

فيسبوك:

<https://www.facebook.com/soroornoor>

تويتر: @Soroor_Noor

https://twitter.com/Soroor_Noor

تم اصدار الكتاب بتاريخ ١٠/٧/١٤٣٥