خطوات هامة يجب الحذر منها لحماية حساب "فيس بوك" من السرقة!

ويقدم موقع "ميك يوز أوف" التقني المتخصص الطرق المثالية، لمعرفة أن حسابك على فيسبوك تم اختراقه أو سرقته، وكيفية مواجهة تلك المشكلة واستعادة حسابك المسروق أو المخترق.

ويستهدف دوما المخترقون أو الهاكرز بصورة كبيرة الحسابات الفردية على فيسبوك، لأنها أسهل في الاختراق.

كيف يتم سرقة حسابات فيسبوك؟

يحدد الخبراء عدد من الطرق والحيل، التي يستخدمها الهاكرز أو القراصنة، لاختراق وسرقة حسابات فيسبوك، والتي جاءت على النحو التالي:

1- انتحال صفة صديق.

تشير بيانات الشفافية الخاصة في فيسبوك إلى أن هناك نحو 120 مليون حسابك مزيف على فيسبوك، بحلول

نهاية عام 2020، علاوة على أن المنصة قيدت نحو 234.5 مليون محتوى غير مرغوب فيه.

ينتحل معظم قراصنة الملفات الشخصية على فيسبوك صفة ضحاياهم ويخدعون أصدقاءهم ومتابعيهم بعد اختراق حساباتهم، لذلك، غالبًا ما تكون اتصالات الضحية هي الأهداف، وليس أصحاب الحسابات أنفسهم، بل يستهدفون دوما أصدقائهم المقربين الذين يتحدثون معهم دوما لتكن عملية الاختراق سهلة.

2- التصيد والهندسة الاجتماعية.

إذا تركت رقم هاتفك أو عنوان بريدك الإلكتروني علنيًا في ملفك الشخصي على فيسبوك، فأنت أكثر عرضة لهجمات التصيد الاحتيالي، وغالبًا ما تصاحب الهندسة الاجتماعية هذا النوع من الهجوم، حيث يحدث التصيد الاحتيالي عندما يرسل المهاجم رابطًا وهميًا للضحية.

على سبيل المثال، يمكنهم إرسال رسالة تخبر الضحية بتسجيل الدخول إلى حساب فيسبوك الخاص بهم عبر الرابط المحدد لأغراض أمنية أو لاسترداد رسالة، وبمجرد النقر على الرابط وإدخال اسم المستخدم وكلمة المرور على فيسبوك، يستحوذ المهاجم على هذه المعلومات.

وإذا فشلت الضحية في إدراك التسريب بالوقت المناسب، يمكن للمهاجم تسجيل الدخول إلى حسابه، ثم يغير المخترق معلومات تسجيل دخول المستخدم المتأثر ويسيطر ملفه الشخصي، كما يمكن للمهاجم أيضًا طلب كلمة مرور جديدة نيابة عنك.

لسوء الحظ، يقع العديد من مستخدمي فيسبوك ضحية لهذا الفخ، وغالبًا ما يكون قد فات الأوان قبل أن يدركوا أنهم فقدوا الوصول إلى حساباتهم على فيسبوك، لأن المخترق يغير معلوماتهم الشخصية.

ويمكن أن يكون إخفاء معلومات الاتصال الشخصية مثل أرقام الهواتف وعناوين البريد الإلكتروني من الجمهور إجراء وقائيا فعالا، وإن لم يكن عمليا دائما.

لذلك، كن حذرً من نوع الرسائل، والرسائل القصيرة ورسائل البريد الإلكتروني والمكالمات، التي ترد عليها، بغض النظر عن شكلها الرسمي، ولا تنقر فوق الروابط المشبوهة التي تبدو غريبة أو ضارة، حتى لو كنت على دراية بها، فاحرص على عدم مشاركة معلومات تسجيل الدخول الخاصة بك مع تطبيقات أو مواقع الطرف الثالث.

3- هجمات القوة الغاشمة.

يستخدم قراصنة القوة الغاشمة كلاً من الأساليب اليدوية والآلية لتركيبات كلمات مرور الجهاز، لمساعدتهم، ويستخدم المهاجمون العديد من تطبيقات إنشاء السلاسل لتخمين كلمات المرور، والمثير للدهشة أن الناس الآن يجعلون هذه العملية سهلة للقراصنة، حيث أصدرت مؤسسة "نورد باس" مؤخرًا أسهل 200 كلمة مرور في عام 2020، ومن السهل جدا تخمين 73 بالمائة منها.

كلما كانت كلمة المرور أقل تعقيدا، كلما كانت أكثر عرضة لهجوم القوة الغاشمة، ولمنع هجوم القوة الغاشمة، تأكد من استخدام كلمات مرور قوية يصعب تخمينها، بحيث تكون مزيج من الأحرف الخاصة مع الأحرف الكبيرة والصغيرة.
ثم استخدم المصادقة الثنائية على فيسبوك، بذلك، حتى إذا خمن المهاجم كلمة مرورك بشكل صحيح، فلن يتمكن من الوصول إلى حسابك دون إذنك.

وأدخل فيسبوك بعض القيود للمساعدة في أمنك، بما في ذلك قيود على طلب كلمات مرور جديدة، ومع ذلك، يمكن أن تتسبب هجمات القوة الغاشمة في حدوث صداع بدون المصادقة ذات العاملين.

4- الروابط الخاطئة وبرامج التجسس.

تطلب بعض التطبيقات الإذن للوصول إلى بيانات اعتماد فيسبوك الخاصة بك، وبعض هذه التطبيقات تتجسس عليك، وفي أسوأ الحالات، يمكنهم الاستيلاء على حسابك لإرسال رسائل غير مرغوب فيها إلى أصدقائك، ويمكن للقراصنة أيضًا استخدام روابط وتطبيقات تجسس مخصصة، لتثبيت برامج التجسس على جهاز الكمبيوتر الخاص بك.

ويمكن لبرامج التجسس هذه الوصول إلى حساب فيسبوك الخاص بك لأداء الإجراءات دون علمك، ويمكن للروابط والتطبيقات المصابة تنفيذ التعليمات التي ينظمها المتسللون، لكن منع هذا الهجوم سهل، فإن رفض وصول التطبيقات غير الموثوق بها لقراءة بيانات فيسبوك الخاصة بك يقطع شوطًا طويلاً لمساعدتك في إيقافه.

ولا تنقر أبدًا على رابط مريب، وتجنب التطبيقات غير الموثوق بها، لأنها يمكن أن تقدم برامج ضارة

إلى جهاز الكمبيوتر الخاص بك وتؤثر على فيسبوك.

5- تسريب كلمة المرور واسم المستخدم.

إذا كان هاتفك أو متصفحك يخزن معلومات تسجيل الدخول، فأنت في خطر التعرض للاختراق، ويمكن أن يؤدي تسجيل الدخول إلى حسابك على فيسبوك عبر شبكة عامة أو كمبيوتر مشترك إلى ترك حسابك في خطر.

وعند استخدام أجهزة كمبيوتر مشتركة، قد تنسى تسجيل الخروج، هذه فرصة للمتسللين لانتزاع حسابك على فيسبوك، حيث يمكنهم الحصول على معلومات شخصية عنك من حسابك الذي قمت بتسجيل الدخول إليه، ويمكن للمهاجم أيضًا استخدام ملفات تعريف الارتباط للجلسة للتجسس عليك عبر شبكة "واي فاي" العامة.

ومع ذلك، عند حفظ معلومات تسجيل الدخول، يمكن للأشخاص الآخرين الذين يستخدمون جهاز الكمبيوتر الخاص بك تسجيل الدخول إلى حسابك دون إذنك، لذلك، تذكر، أنه لا يمكنك الوثوق بأي شخص.