فنون الهندسة الإجتماعية

نرتقي لإشر اقة حول معلومات تقنيه مهمة وتوضيحات سريه حول اساليب الخداع من الهاكر

الكتاب إلكتروني فقط ولا يوجد اي نسخة مطبوعه
تم إنشاء الكتاب من قبل أ/عبدالرحمن تهامي
وتم التحقق من صحة المعلومات من مصادرمعروفه

المقدمة

بسم الله الرحمن الرحيم و الصلاة والسلام على رسول الله سيدنا محمد

لا اعلم كم مستفيد من المعلومات ومن سيقرء وكيف سيستغل هذه المعلومات ولذلك، أود ان اقول ان هذه المعلومات بعضها من مصادر معروفه وموثوق منها وبعضها سرية وغير معروفه لإنها يتم استخدامها في اشياء ضد القانون والدين وسوف ابرء نفسي امام الله إذا تم استخدام اي معلومه في ترهيب وإخافة الناس، في هذا الكتاب سوف نتعرف علي اشياء عديده في الانترنت من حيث الحمايه والاستخدام والطرق المستخدمه للخداع وكيفية التفادي من اللصوص الإلكترونية الخ...

ولكن بعضنا سوف يدخل في مواضيع ملخصه من الكتاب ولكن هذه المعلومات متشابكه ومتشابهه في جميع المجالات سواء الحمايه او المعرفه، لذلك يجب ان تعرف ان قراءتك للمعلومه كامله سوف تفهمها اكثر

وحتي لا اطيل عليكم دعونا نبدء في المفيد

ملحوظه : يمكن للكتاب نشره لانه مجاني لكن لديه حقوق نشر من قبل عبدالرحمن تهامي

أهداف الكتاب ومحتوياته

- اساليب الحماية العكسيه والامنة لاجهزتك و حساباتك
- اساليب الخداع التي يستخدمها الهاكر مع المستخدمين
- اساليب حول فن اختراق العقول بدون علم المستهدف
- اساليب وخدع جديده تم اكتشافها للسرقة والتجسس
- كيف يتم التجسس عليك دون علمك
- كيف تستطيع خدمة نفسك دون إحتياج الاخرين

حماية الاجهزة والحسابات

دعونا اولا نعرف كيف تكون الحمايه لحساباتنا واجهزتنا ولكن قبل اي شي يجب ان تعرف بعض المعلومات لكي تساعدك علي الفكر الامن، انا لست المستخدم ولكني سوف اتحدث دائما كمستخدم مثلك تماماً

في بداية الامر نحن من الطبيعي نحمل التطبيقات علي الهو اتف لكن لا نركز في بعض الاشياء وهي

1- ماذا يريد هذا التطبيق

2- ماذا سوف يحصل هذا التطبيق علي اذونات الهاتف

علي سبيل المثال لقد قمت بتحميل تطبيق يعرض لي الاستوديو بشكل أفضل من البرنامج الاساسي واعجبني التطبيق ولكن عند التثبيت لاحظت انه يتطلب اذن الوصول للملفات وهذا امر طبيعي كي يتعرف التطبيق على الصور لكن احيانا في بعض التطبيقات يمكنه طلب منك الوصول الي الموقع او الوصول الي الكاميرا او الوصول الي جهات الاتصال ، هل سيكون هذا امر طبيعي؟، لماذا يطلب التطبيق بالسماح لهذه الاذونات رغم ان التطبيق مجرد فتح الاستوديو؟

الكثير من المستخدمين لا يهمهم ماذا سيحصل التطبيق لكن يهمه هو استخدام التطبيق ، وهذا امر خطير ومنتشر بيننا وعند السماح بهذه الاذونات الخطيره سوف يتعرف التطبيق علي معلوماتك السريه ويحفظها

ولكن يسأل البعض لماذا يفعل التطبيق هذا؟ ، يجب ان تعرف ان كل مستخدم انترنت سواء علي مو اقع التواصل الاجتماعي او متصفح او ايا كان هو مجرد سلعه لا اكثر، نعم انت مجرد سلعه للبيع والشراء يستخدموك في الاعلانات ومدي اهتماماتك وتسمي هذه بتحليل البيانات الضخمه

اذن هل عرفت الان ماذا يستفيد التطبيق منك؟ ، نعم هو بيع معلوماتك لشركات تجارية لإستهدافك في اعلاناتهم علي اي منصه الكترونيه

ولكن هذا في التطبيقات إذن ماذا عن الحسابات وكيف يصل الهاكر لمعلومات جهازي عن طريق البريد او الحساب الخاص بي!

حسنا سوف نوضح هذه الخطوه

يجب ان تعرف اولا انك من ساعدت الهاكر علي هذا وعلي اختر اقك من البدايه.. لنشرح اكثر
منصات التواصل الاجتماعي مثل (فيسبوك ، إنستجرام ، تويتر، سناب شات ، الخ..)
هذه مو اقع عالميه وشبه مستحيل إيجاد ثغرات في هذه المو اقع بمعني اوضح ان اختراق حسابك او بريدك هو مجرد هندسه اجتماعيه وتم جمع معلوماتك من خلال البحث عنك ومعرفة تاريخ ميلادك ورقم هاتفك و اقرب الاقربين وجميعها وتم التجربه علي كل هذا وأعتقد ان معظم القارئين الان يستخدمون تاريخ ميلادهم او ارقام الهو اتف ككلمة سر لحساباتهم
ومعظم الاخر يستخدم منصات البريد الإلكتروني مثل ياهو او هوتميل ك بريد اساسي لحساباتهم ولم يفتحون هذه البريد منذ زمن ولكن معلومه سريعه حول منصات البريد الإلكتروني
يجب ان تعرف ان منصات البريد الإلكتروني يتم حذف البريد الغير مستخدم منذ علي الاقل سنتين من موقعها ويمكن انشاء بريد إلكتروني بنفس اسم البريد المحذوف بكل سهوله ومعني هذا ان يمكن للهاكر استخدام هذه الميزه في سرقة حساباتك
لذلك تأكد دائما ان:-
بريدك الإلكتروني مؤمن وتستطيع استخدامه
ربط بريدك الإلكتروني ببريد اخر لا يعرفه احد سوي انت
تفعيل خطوات تحقق وتشفير الرسائل المهمه
ومن افضل منصات البريد الإلكتروني هي هذه المو اقع

mail.com(ميل دوت كوم)

وهذه منصه امريكيه لا تحذف بريدك ابدا ويمكنك التمتع ب تشفير الرسائل المهمه والمميزه والتي تحتوي علي حسابات بنكيه بكل سهوله اما عيوب هذه المنصه انها لا تدعم اللغه العربية

PROTON Mail (بروتون ميل)

، حيث يتم توليد مفتاح تشفير خاص بين صندوقي البريد على طرفي المراسلة (طبعاً عندما يستخدم الطرفين ذات الخدمة) ، **End To End Encryption** تشفر الرسائل بتقنية
وتمر الرسائل بشكل مشفر تماماً عبر مخدمات الشركة دون إمكانية
فك التشفير كون الشركة لا تملك المفتاح الخاص
كحقوق مستخدم او يمكنك إستخدام بريدك الجامعي افضل من كل هذا وتأكد دائما ان هاتفك لا **gmail** ويوجد العديد من المنصات لكن هذا افضلهم من الناحيه الامنيه وطبعا بعد يعمل مزامنه لملفاتك الا علي بريدك الخاص والذي هو غير مرتبط بأي حساب لك علي اي منصه الكترونيه
بهذه النصائح لا يمكن للهاكر ايجاد ثغره حول وصول الي معلوماتك وحاول دائما إخفاء معلوماتك علي التواصل الاجتماعي مثل :-
(تاريخ ميلادك ، رقم هاتفك ، الاصدقاء ، علاقاتك)

لا تقبل اشخاص لا تعرفهم يمكن ان يكون الحساب زائف ويريد استغلالك
لا تنشر منشورات خاصه عن حالتك الحاليه في العامه لأن اللصوص ليست الكترونيه فقط بل يوجد لصوص علي الو اقع يمكنهم تتبع افعالك من خلال حسابك
تأكد دائما ان بريدك الإلكتروني غير مرتبط ببريد اخر من ناحية الاستيراد و التصدير للرسائل لان اذا قام الهاكر بإختراق بريدك الإلكتروني سوف يفعل هذه الخطوه وهذه يتساعده علي قراءة والوصول الي معلوماتك حتي اذا قمت بتغيير كلمة السر الخاصة بك ويمكنه ايضا الوصول الي صور هاتفك اذا كنت تستخدم مزامنه وهذا يعني اختراق للهاتف ومن الضروري التأكد من هذا!..
والان قد عرفنا كيف يتم حماية جهازك من التجسس وسوف ننتقل الي خطوه يسألها الجميع وهي

هل يتجسس فيسبوك علينا؟

كما ذكرت نحن مجرد سلعه في اي مكان ليس فيسبوك فقط ولكن ببساطهلربما. ولكن لا دليل على ذلك حتى الآن، وكل ما قيل عن أساليب تجسس الفيسبوك وخصوصاً عن طريق المايكروفون يمكن دحضه بسهولة على ضوء المعلومات التي قدمها مدير جهود استهداف الإعلانات السابق في فيسبوك أنطونيو غارسيا مارتينيز. حيث ظهرت مجموعة من الأخبار والشائعات عن استخدام فيسبوك أسلوب تسجيل الصوت لاستخلاص معلومات من المستخدم في سبيل عرض الإعلان المناسب.

فإذا ما فرضنا صحة هذه النظرية فسيكون حجم التسجيل الصوتي ليوم واحد 130 ميغابايت لكل مستخدم، ولدى فيسبوك 150 مليون مستخدم نشط يومياً في الولايات المتحدة وحدها فقط، وهذا يعني الحصول على كم هائل من البيانات يعادل 20 بيتابايت، بينما يبلغ وحدة تخزين بيانات الفيسبوك 300 بيتابايت، كما أن تشغيل المايكروفون سيؤثر استخدام معالج الهاتف، وهذا أمر يسهل كشفه باستخدام بعض البرامج الخدمية، كما سيؤثر أيضاً على استهلاك البطارية بشكل مفضوح.

ثم كيف لفيسبوك معالجة هذا الكم الهائل من التسجيلات الصوتية واستخلاص الكلمات المفتاحية التي تفيد عملاءها؟ ثم إن الحوارات البشرية مليئة بالتورية والمزاح والضحك والسخرية، فكيف للذكاء الصناعي تمييز كل هذا.

وعلى الرغم من أن هناك أجهزة حديثة قد لا يشعر المستخدم فيها ببطء الجهاز، إلا أن هناك كثير من الهو اتف القديمة التي ستتأثر بشكل كبير، وعلى فرض استثناء الأجهزة القديمة من التجسس، فكم ستبلغ نسبة الأجهزة الحديثة؟

إن مصادفتك لأمور قد ذكرتها أو تريد الذهاب إليها أو ما شابه ذلك أثناء تصفحك شبه المستمرّ على موقع فيسبوك لا يعني أنّ فيسبوك يتجسس عليك، ولما سيفعل ذلك، عند ظهور إعلان لقميص محددّ أردت شرائه حيث يتم عرض الإعلانات على صفحتك الرئيسيّة على فيسبوك وفقًا لاهتماماتك ومعلومات ملفك الشخصي التي وفرتها أنت لفيسبوك بمحض إرادتك، وليس وفقًا لما أرسلته لأحد أصدقائك أو قلته له بصوتٍ عال.

لدى فيسبوك العديد من الطرق لمراقبة سلوك مستخدميها، بحيث لا تحتاج للتنصت أو التجسس عليك برغم المصادفات الغريبة التي قد حدثت لك أثناء تصفحك كأن ترى بين اقتراحات الأصدقاء شخصًا قابلته لتوّك منذ بضعة ساعات أو شاهدته في أحد المقاهي، ويمكن تفسير الأخيرة بأنك في حال سجّلت دخولك للمقهى ذاته الذي سجّل ذاك الشخص دخوله إليه فمن المرجح أن تراه بين الأصدقاء المقترحين لكونكما تشاركتما قاسمًا محددّا وهو التردد لهذا المكان وهذا ينطبق على العديد من الأماكن والمتاجر بعض النظر عمّا سبق لا يوجد أي دليل تكنولوجي يدعم فرضيّة تعرّضنا للتجسس من قبل فيسبوك حيث أنّ عمليّات المراقبة في خلفيّة الجهاز ستضعف أدائه ولن يمر الأمر دون ملاحظة خاصةً لتطبيقات رصد التجسس، ولنفترض أنّ أحاديثنا يتم مراقبتها وتحويلها لنسخٍ رقميّة وهو ما سيحتاج تكاليفًا باهظة ووحدات تخزين اكثر من عملاقة؛ هل ستحتوي أحاديثنا على هذا القدر من الأهميّة؟ على الرغم من أنّ معظمها خارج عن السياق العادي أي مليء بالسخرية وازدواج المعاني ومكتوبٌ بلغة عاميّة ولن يقدر الذكاء الصناعي لفيسبوك فهمه أو معرفة ما تعنيه، لذا فارتيابنا لا مبررّ له كمعظم المصادفات الغريبة ليس فقط على فيسبوك.
كثيرما يتم الكلام بين مُستخدمي موقع فيسبوك بأن فيسبوك يقوم بالتجسس عليهم ومعرفة كل شيء عنهم وغيرها من الأمور، فهنالك من يقول بأنه على سبيل المثال يحب مطعم معين ويأكل به بشكل دائم، فيجد الفيسبوك يقوم بعرض الصفحات المُتعلقة به بالإضافة إلى الإعلانات التابعة له، ولكن في حقيقة الأمر شركة فيسبوك طورت قاعدة بياناتها وطورت بناء الأنماط والأفكار حول سلوكيات المستخدمين، وكون هذا الشخص قد سجل دخول في أحد المرات إلى هذا المطعم بواسطة منشور، فمن الطبيعي أن يتم ظهور المواضيع المُتعلقة بهذا المطعم والتي تكون ذات صلة بالطعام.

هنالك نظرية أخرى من قبل الناس عن تجسس فيسبوك عليهم، مثل تساءل الناس فيما إذا كان فيسبوك يقوم بأخذ صورهم أو تسجيل أصواتهم عبر الميكروفون، ولكن وبشكل منطقي ولو وضعنا أنفسنا بمكان مدير منتجات فيسبوك، سنجد أن تسجيل كل شيء يصدر عن هاتفك عندما يكون الهاتف قيد التشغيل، ولنفترض كان قيد التشغيل لمدة 12 ساعة في اليوم الواحد، سيتطلب لتخزين هذا الصوت 130 ميغا لوحدك فقط، فما بالك عن تسجيل أصوات الميكروفون والتجسس على 150 مليون مشترك في فيسبوك نشط وبشكل يومي في الولايات المتحدة فقط، ويمكنك تخيل الأمر على نطاق العالم ككل، ستجد أن الموضوع صعب ويتطلب كمًّا هائلًا من وحدات التخزين وقواعد البيانات والأدوات والتكاليف.

اساليب الاحتيال والخدع علي الانترنت

يستخدم معظمنا الإنترنت ومو اقع التواصل الاجتماعي لتساعدنا في اتخاذ قراراتٍ حول توظيف أموالنا وغيرها من الأمور، وقد تفيد هذه الأدوات المباشرة فعلًا، لكن أيضًا قد تجعلنا أهدافًا للمجرمين وعرضةً لمختلف أنواع الاحتيال على وسائل التواصل اولا سريعو التأقلم مع التقنيات الجديدة، ولا يشكل الإنترنت استثناءً في ذلك، حيث يمثل طريقةً نافعةً في الوصول إلى جماهيرَ عريضةٍ بدون إنفاق الكثير من الوقت والمال. فعبر موقع أو رسالة إلكترونية أو منصة اجتماعية بالإمكان الوصول إلى عددٍ ضخمٍ بأقل جهدٍ.

ومن السهل على المحتالين أن يصمموا رسائلهم بحيث تبدو حقيقيةً وقابلةً للتصديق، ويصعب على الشخص أحيانًا أن يكتشف الفرق بين الحقيقة والاحتيال. فإذا لفت نظرك أي إعلانٍ ترويجيٍّ، ابحث جيدًا حتى قبل تزويده برقم هاتفك وعنوان بريدك الإلكتروني. وإلا ستكون هدفًا للاحتيال.

منصّات مو اقع التواصل الاجتماعي

يعتمد أغلب الأشخاص على مو اقع التواصل الاجتماعي كفيسبوك و أنستغرام ويوتيوب وتويتر ولينكد إن للبقاء على اتصالٍ، ولمتابعة الأخبار، والاستثمار، ولشراء الأشياء حتى.

لكن رغم ذيوع شهرتها، يزداد معها خطر التعرض للاحتيال؛ فميزات هذه المو اقع نفسها تجذب المحتالين والمجرمين الذين يستخدموها لإخفاء نو اياهم، والوصول إلى الكثير من الأشخاص بأقل كلفةً. لذلك على المستخدم أن يكون حذرًا من إغواءات العروض، ويتعرّف أساليب الحماية من الاحتيال على وسائل التواصل الاجتماعي الشهيرة، فأساليب البيع المغرية قد تكون جزءًا من مخططٍ احتياليٍّ.1

حسب دراسة حديثة، فإن 53% من تسجيلات الدخول إلى مو اقع التواصل الاجتماعي ترتبط بحساباتٍ مخادِعةٍ، و25% من الحسابات الجديدة وهمية.

من بين 5 بلدان كأكبر منابع الهجمات الإلكترونية، تعد الفلبين المصدر الأكبر للهجمات البشرية والروبوتية، وتأتي بعدها الولايات المتحدة الأمريكية.

إنّ 50% من الهجمات الإلكترونية التي يقودها بشرٌ مصدرها الصين، وهي أكثر بـ4 مرات من الولايات المتحدة وروسيا والفلبين و أندونيسيا.

تطورت الأهمية الاجتماعية لمو اقع التواصل بقوةٍ، وفي حين تعتبر أدواتٍ عظيمةً للتواصل مع من نحب والاطلاع على أحدث الصيحات، لكن وجدت دراسة حديثة أن قنوات التواصل الاجتماعي اليوم حافلةٌ بالاحتيال.2

أشهر أنواع الاحتيال على وسائل التواصل الاجتماعي

الأصدقاء المزيفون: يجب القول أن عليك الحرص حول من تتواصل معهم على مو اقع التواصل الاجتماعي، فالأشخاص يرسلون طلبات صداقةٍ ثم يطلبون منك المال، وهو شيئ منتشر

ويمكن أن يمضي المحتال لأبعد من ذلك ويدعي أنه أحد أصدقائك أو يرسل إليك رابطَ تصيد يقودك إلى موقعٍ ضارٍ.
تنزيل التطبيقات المجانية: غالبًا ما تطلب منك هذه التطبيقات معلوماتٍ شخصيةً، وأحيانًا يبدو تطبيقٌ ما أنه حقيقيٌّ لكنه فعليًا يقوم بتنزيل فيروسٍ على جهازك. لذلك قبل تحميل تطبيق جديد، تأكد من المصدر، قم بالبحث وتجنب متاجر تطبيقات الطرف الثالث.
المسابقات والاختبارات: تعدك الاستفتاءات المباشرة بإخبارك عن نوع شخصيتك، وتوهمك أنها ستمنحك جائزةً حقيقيةً، لكنها تحمل تهديداتٍ خفيةً. وعادةً ما تتضمن عباراتٍ وشروط . تجنب أي مسابقاتٍ قصيرةٍ IPتسمح بالدخول إلى بياناتك وبيعها لطرفٍ ثالثٍ. كما بمقدور مزود التطبيق أن يحصل على معلوماتٍ عنك من صفحتك الشخصية، وعن أصدقائك وعنوان تعلن عنها مو اقع التواصل الاجتماعي كفيسبوك وتويتر.
العناوين المخفية: احذر من النقر على الرو ابط المختصرة التي تخفي الموقع الكامل لصفحة الويب، وهي منتشرةٌ جدًا على تويتر، وبينما قد توجهك ببساطةٍ إلى الموقع الصحيح فهناك فرصةٌ دائمًا أن تقودك إلى موقعٍ يحمل البرمجيات الخبيثة. لذلك احرص على ما تنقر.3
نصائح من أجل الحماية من الاحتيال على وسائل التواصل
يحتاج الشخص إلى جانب حماية حسابات المو اقع من الاختراق، إلى حمايتها أيضًا من المخادعين الذين يستهدفون مستخدمي المو اقع الاجتماعية، وفيما يلي ثماني طرقٍ لتجنب الخداع على مو اقع التواصل الاجتماعي:

الحذر من الهدايا والمسابقات والبحوث المسحية المخادعة: يقدم المحتالون أحيانًا بطاقات هدايا مجانية أو قسائم حسومات مذهلة تحت مظهر تقديم الأعمال في موقعٍ خاصٍ، أو يوفرون بعض الجو ائز مقابل ملء استبيان. كل هذه مصائد تكون إما للحصول على إذن الدخول إلى معلوماتك على مو اقع التواصل الاجتماعي (مثلًا أن تحتاج إلى السماح لتطبيق فيسبوك بالدخول إلى حسابك لكسب الجائزة) أو لجمع معلوماتٍ شخصيةٍ.
الحذر والتأكد من عدم التواصل مع أشخاص مزيفين: يقوم المجرمون غالبًا بإنشاء حساباتٍ وهميةٍ للتواصل مع أشخاصٍ حقيقيين ثم يستغلون جهات اتصالهم، أو يستخدمون المعلومات في منشورات الضحية الخاصة للاحتيال على أصدقائه أو زملاء العمل. لذلك من الضروري عدم قبول طلبات صداقةٍ من أطرافٍ غير معروفةٍ.
الحذر من طلبات التواصل القادمة من حسابات منتحلي الشخصية: قبل قبول طلب صداقة على فيسبوك، أو طلب تواصل على لينكد إن من أي شخصٍ، تحقق أن الحساب ينتمي فعلًا لذلك الشخص، فأحيانًا يُنشئ المجرمون حساباتٍ مزيفةً ويستخدمون صور الأشخاص المتاحة للعامة. للمساعدة في تحديد ما إذا كان الحساب حقيقيًا، تفقد كم صديقًا أو جهة اتصال مشتركة بينكما، وتمعن إذا كان العدد يبدو منطقيًا، واطلع كم مضى من الوقت على آخر المنشورات في الحساب.
الانتباه إلى المنشورات القادمة من حسابات منتحلي الشخصية: من المعروف أن الاحتيال على وسائل التواصل بأبسط صوره يتجلّى بانتحال الشخصيّة؛ فمثلًا، عندما ينشر أحدهم سؤالًا ما على صفحة الأعمال بفيسبوك قد يقوم المحتال بالإجابة باستخدام حسابٍ ينتحل صفة رجل أعمال أو أحد موظفيه المقربين، وينطبق نفس الأمر على التغريدة.

كن حذرًا بشكل خاصٍ من الرو ابط التي قد تنشرها الحسابات الانتحالية، فأحيانًا يرد المحتالون على أسئلة خدمة زبائن وينصحون المستخدم بزيارة موقع خاص أو تنزيل بعض البرامج، لذلك لا تكن فريسةً لهذا الخداع.

الحماية من البث المباشروعروض الأفلام الاحتيالية: يقدم المحتالون أحيانًا بثًا مباشرًا لأحداثٍ مشهورةٍ أو أفلام، وغالبًا ما تقود رو ابط هذه المنشورات إلى مو اقع تنشر البرمجيات الخبيثة؛ أو تسرق تفاصيل البطاقة الائتمانية أو تطلب معلوماتٍ شخصيةً قد يستخدمها لصٌ أو محتالٌ. لذلك يجب الدخول لرؤية البث المباشر للمناسبات على صفحات هذه المناسبات، ومشاهدة الأفلام حصرًا على المنصّات المصرح لها قانونيًا.

تجنب النقرعلى رو ابط الإعلانات والعناوين المغرية: قد تصلك ادعاءات بتقديم سبقٍ صحفيٍّ عن أخبار بعض المشاهير، أو نشر صور مثيرة عن بعضهم أو بعض المعلومات السرية التي تساعدك في كسب المال بسرعةٍ عبر استثمار بعض الأسهم، فمن المعروف أن المحتالين يبثون رو ابط تلفت الانتباه، الرو ابط طبعًا، غالبًا ما توجه إلى مو اقعَ خبيثةٍ مشابهة لتلك التي تستخدم خدع الهدايا، والمسابقات والمسوح.

تجنب المبالغة بالمشاركات: يبالغ معظم الناس بالمشاركة، لذلك لا تنشر ما لا تثق به؛ فالمشاركة المبالغ بها تمنح المجرمين ما يحتاجونه من معلوماتٍ ليهاجموا حسابك، أو تساعد المجرمين في الإيقاع بأصدقائك أو زملاء العمل كضحايا لمثل هذا الخداع.

تأمين حسابات مو اقع التواصل الاجتماعي: إذا حدث شيءٌ ما بشكلٍ خاطئٍ، عليك التأكد من عدم سيطرة المحتالين بسهولةٍ على حسابات التواصل الاجتماعي، واستخدامها للهجوم على أصدقائك وزملائك؛ لأن اختراق الحساب الاجتماعي الرئيسي سيكون مربكًا على أقل احتمالٍ