امنیت در شبکه های اجتماعی

خب وقتی حرف از امنیت میاد همه فکرشون به سمت هکر ها میره . امروزم قصد داریم برای شما توضیح بدیم آیا شبکه های اجتماعی همچون تلگرام یا اینستاگرام یا سایر شبکه ها قابل هک هستند؟ اگر هستند چه اقداماتی انجام بدین ؟ چگونه با هکر ها مقابله کنیم؟

در ابتدا چند سوال در ذهن ما بوجود میاد

آیا شبکه های اجتماعی هک میشوند؟

آیا سرویس جیمیل نا امن است ؟

آیا شبکه اجتماعی فیسبوک و یا توییتر امنیت ندارد ؟

آیا شبکه اجتماعی تلگرام امنیت زیادی دارد؟

اگر هر یک از شبکه‌های اجتماعی بزرگ و یا سرویس‌دهندگان بزرگ ایمیل دچار مشکل نرم افزار و وب سایتی بودند تا به حال هزاران هکر تمام حساب‌های کاربری را هک کرده و این شرکت‌ها زودتر از آن چیزی که تصور می‌کنید ورشکسته شده بودند و این نکته هم در مورد امنیت بگم که هیچ شرکت یا شخصی نمیتواند ادعا کند که امنیتش 100% است.

اما حال ببینیم مشکل کجاست ؟

مشکل اصلی هک شدن برخی از حساب‌های کاربری در شبکه‌های اجتماعی ، ایمیل و... خود کاربران هستند.

بله ؛ خود کاربران.

کاربران با نداشتن علم کافی ممکن است کارهایی انجام دهند که دقیقاً یک هکر برای دسترسی نیاز داشته باشد.

حال به شما چندین روش برای امنیت بیشتر در فضای مجازی را توضیح میدهیم

در زیر چند نکته جهت حفظ امنیت در شبکه های اجتماعی اشاره می‌کنیم:

1. قبول کنید شما هم می‌توانید قربانی هکرها شوید.
2. مجبور نیستید به سوالهایی که از شما در مورد خودتان پرسیده می‌شود به صورت عمومی جواب بدهید و سریع شخصیت‌تان را آشکار کنید. هیچ چیز بدتر این نیست که خیلی ها شخصیت شما را بدانند و بتوانند خیلی سریع شما را شناسایی کنند.
3. از امنیت نرم افزارهایی که به اطلاعات شما روی کامپیوتر یا گوشی‌تان دسترسی دارند مطمئن شوید.
4. روی لینک‌های کوتاهی که نمی‌دانید مقصدشان کجا هستند کلیک نکنید.
5. در مورد پست‌هایی که عنوان‌هایی مانند « این ویدئو را از دست ندهید » دارند محتاط باشید، معمولا بعد از اینکه روی این لینکها کلیک می‌کنید پیغامی به شما می‌دهد که ویدئو پلیر شما به روز نیست و لینکی می‌دهد که از این سایت به روز کنید، هنگامی که روی لینک کلیک می‌کنید در حقیقت یک نرم افزار مخرب را دانلود می‌کنید.
6. از تنظیمات امنیتی سایت‌های شبکه اجتماعی آگاه باشید. امن‌ترین تنظیمات را اعمال کنید، و به صورت منظم تنظیمات امنیتی و حریم شخصی را بررسی کنید تا در صورت به روز رسانی، از امکانات جدید آن مطلع شوید و تنظیمات خود را به روز کنید.
7. نرم افزارها و ویژگی های جغرافیایی برخی اپلیکیشن‌ها، مکان شما را منتشر می‌کنند و این باعث می‌شود مجرمان بدانند شما کجا هستید. مراقب باشید مکان‌تان توسط این نرم افزارها آشکار نشود.
8. برای هر حساب کاربری خود، نام کاربری و رمزعبور جداگانه‌ای تعریف کنید. به خصوص در مورد رمز عبور، از رمز عبورهای پیچیده و منحصر به فرد برای هر حساب تان استفاده کنید.
9. وقتی از سایتی بازدید می‌کنید، دامنه آن را بررسی کنید تا گرفتار حملات فیشینگ نشوید. برای مثال وقتی وارد فیسبوک می‌شوید مطمئن باشید دامنه بدین صورت است «https://www.facebook.com» ممکن است مجرمان سایتی مشابه فیسبوک با آدرس «http://www.facbook.com» برای سرقت اطلاعات ورود فسبوک شما، آماده کرده باشند.
10. مطمئن باشید کامپیوتر یا گوشی و تبلت شما حتما آنتی ویروس به روز و فایروال دارند.
11. هیچ وقت به طور ۱۰۰ درصد مطمئن نباشید که امنیت‌تان تضمین شده است

چگونه تلگرام را امن کنیم؟

آیا اصلا تلگرام قابل هک هست؟

در بالا توضیح دادم و دوباره میگم در واقع این کاربر ها هستند که هک میشوند .

به فرض مثال یک حساب کاربری به چه صورت هک میشود؟

خب در جواب باید بگم روش های زیادی وجودی داره که چند مورد رو براتون توضیح میدم

در اصل هک کردن تلگرام همون دریافت کد 5 رقمی برای ورود که از ما میخواد هست . شما کافیه اون کد 5 رقمی رو بدست بیارید انگار تلگرام شخصی رو هک کردید.

خب حالا این کد 5 رقمی رو چگونه میتوانند بگیرند؟

ساده ترین روش اینه که شخصی در کنار شما نشسته هست و گوشی شما دستشون هست و در همین هنگام شماره شما را در تلگرام دیگه ای وارد میکند و وقتی کد 5 رقمی به گوشی شما ارسال شد سریع بر میدارد و وارد تلگرام میکند و به همین راحتی میتواند وارد حساب شما شود

یا بفرض مثال شخصی از طریق نرم افزار های جاسوسی که برای شما ارسال کرده بود و یا روی گوشی شما نصب کرده بود از طریق اون میتواند به کلیه اسمس های دریافتی و ارسالی شما دسترسی داشته باشد وقتی هم کد 5 رقمی براتون اسمس شود براحتی به ان دسترسی دارد. نرم افزار های جاسوسی یک مبحث جداست که در آموزش های آینده ایشالله توضیح خواهد داد

چگونه امنیت تلگرام را بالا ببریم و آن را ضد هک کنیم؟

قدم اول

با این روش حتي اگر کد 5 رقمي شما در اختيار کسي نفوذگر قرار بگيره باز هم نميتونه به تلگرامتون وارد بشه:

1. به Setting برید و روي Privacy and Security كليك كنيد.
2. بر روي Two-Step Verification كليك كنيد.
3. يك رمز امن وارد كنيد و ايميل خودتون رو وارد كنيد.

نكته: حتما ايميلتون رو صحيح وارد كنيد ، در صورتي كه پسورد دوم تون يادتون رفت بتونيد از طريق ايميل بازيابي كنيد.

قدم دوم

همیشه نسخه رسمی تلگرام را نصب کنید زیرا در سایر نسخه های تلگرام امکان دارد ابزار های جاسوسی که موجب هک شدن شما میشود قرار بدهند.همچنین رعایت این نکته که تلگرام را فقط از سایت رسمیش دانلود کنید

قدم سوم

با استفاده از این روش میتوانید دستگاه هايي که به اکانت شما وصل هستند را ببینید:

1. به Setting بروید و روي Privacy And Security كليك كنيد و روي گزينه Active Sessions کلیک کنید.
2. میبینید که دستگاه هاي متصل شده به اکانت شما را نشان مي دهد.

حالا میتونید اگر دستگاهی هست که برای شما نیست ولی تو اینجا نشونش میده رو حذف کنید.

- نكته: با اين روش مي توانيد ببينيد كه آيا هك شديد يا نه!
-

قدم چهارم

برنامه هايي که به اسم هك تلگرام و شبکه هاي اجتماعي در کانال ها میفروشن را به هیچ عنوان روي دستگاه خودتون نصب نکنید (تمامي اين برنامه ها فيك هستند).اگر قرار بود تلگرام با يك برنامه هك بشه مطمئن باشید هیچوقت نه بوجود مي اومد نه امن ترین پیام رسان شناخته مي شد. پس هیچکدوم از این نرم افزار ها صحت ندارد و صرفا جهت دسترسي گرفتن از گوشي شما ساخته شده.به هیچ عنوان اینچنین نرم افزار ها را روي گوشي خودتون نصب نکنید

قدم پنجم

برای امنیت بیشتر هنگام مکالمات در تلگرام میتوانید از امکان secret chat استفاده کنید . در این بخش امکاناتی برای شما فراهم میشود که از گفتگو هایتان محافظت خواهد کرد . حتی شخصی که دارد با شما چت میکند امکان اسکرین شات گرفتن از پیام ها را هم ندارد.

یک هکر به چند روش میتواند حساب کاربری مارا هک کند؟

امروز میخوایم ببینیم یک هکر چجوری حساب ما توی شبکه های اجتماعی رو هک میکنه و ما چه کارهایی باید بکنیم که این اتفاق نیفته.بحث ما شبکه های اجتماعی ای هست که شما توسط یک Browser به اونا وصل میشید نه چیزی مثل تلگرام یا واتس آپ، البته شاید در یکسری از انواع حملات یکی باشن ولی بعضی از حملات هم متفاوت هست.قبلا درباره امنیت در شبکه های اجتماعی مانند تلگرام در یک مقاله پرداختیم و الان هم میخوایم درباره حساب هایی مثل فیسبوک صحبت کنیم.

حالا با چه روشی هایی ما هک میشیم؟

اولین مورد هک شدن با روشی به نام Phishing هست.خب هکر در این روش چیکار میکنه؟ در این روش یک هکر یا با استفاده طراحی و کد نویسی سایتی مانند فیس بوک ، یعنی بصورتی است که شما سایت رو ببینید باور میکنید که این سایت فیس بوک میباشد . از نظر ظاهر هیچ تفاوتی با سایت اصلی فیس بوک ندارد . در اینجا شما فکر میکنید واقعا سایت فیس بوک هست و نام کاربری و رمز عبور خود را وارد میکنید . در این قسمت طبق کد نویسی هایی که توسط هکر انجام شده بود نام کاربری و رمز عبور وارد شده شما به هکر ارسال میشود و به همین راحتی شما هک شده اید

حالا به چه صورت آدرس قلابی را برایتان ارسال میکند؟

یه ایمیل فیک میسازه به شما یک ایمیل میده به انگلیسی که آقا یا خانم عزیز شما مشکل امنیتی داری بدو بیا رمزت رو عوض کن و یه لینک هم میده که لینک اون صفحه ساختگی هست. شما وارد میشی و میبینی بله سایت فیسبوک اومد بالا و میگه حالا یوزر و پست رو بزن و شما هم میزنی، حالا چی میشه؟ شما میری به صفحه اصلی فیسبوک با همون قابلیت redirect ای که هکرمون گذاشته بوده و پیش خودت فکر میکنی که خب صفحه یک بار reload شده و دوباره یوزر پس رو تو سایت اصلی میزنی و وارد میشی و اصلا متوجه نمیشی که شما یوزر و پست رو به راحتی دادی به هکرمون(:

خب حالا راهکار چیه؟

اولا که گول هیچگونه ایمیل و پیامی رو نخورید. اگر فیسبوک بخواد خبری به شما بده حتما تو اکانت خودتون ذکر میکنه نه با ایمیلتون و راه دوم هم یک نگاه ساده به url ای هست که دارید توش رمزتون رو میزنید. شکل غیر عادی ای از url رو دیدید شک کنید، تاکید میکنم هر شکلی رو چون راهکارهای عجیبی هست که واقعا url رو شبیه چیزی میکن که شما گول بخورید پس وقتی میخواید وارد فیسبوک بشید فقط url خود فیسبوک رو بزنید و اگر اسمی شبیه بود شک کنید.حالا بریم سراغ راه دوم که پسورد های ذخیره شده تو مرورگر ماست

این یکی از خطرناک ترین راه ها هست. شاید هرکسی نتونه استفاده بکنه از این راه چون باید به دستگاه شما دسترسی داشته باشه ولی مشکل از جایی شروع میشه که حتی دوستان و آشنایان ما برای شوخی هم که شده میخوان این کار رو بکنن و حتی اگر دوست و آشنا نباشه کافیه یک مقدار با مهندسی اجتماعی بیاد جلو.چند بار در روز دوستانتون یا اطرافیانتون توی محل کار یا دانشگاه میگن که فلانی یک لحظه لپ تاپت رو بده تا یچیزی بریزم رو فلشم یا اطلاعات فلش رو بریزم رو هاردم یا خیلی چیزای دیگه؟ خب شما یا نباید لپ تاپتون رو به کسی بدید که نمیشه :) یا اینکه اطلاعاتتون میره رو هوا.

چجوری؟

خب یکسری برنامه هست که روی فلش نصب میشود و بعد از وصل کردن فلش به لبتاب یا کامپیوتر پس از وارد کردن چند مرحله دستور یا حتی اجرا یک نرم افزار میتواند براحتی کلیه اطلاعات اون سیستم را بگیرد و در درون فلش خود ذخیره کند

حالا چیکار کنیم که این اتفاق نیفته؟

یک مقدار به خودمون سختی میدیم و هر حساب کاربری ای که باهاش وارد میشیم رو نمیدیم مرورگر ذخیره کنه و لحظه ای که میپرسه ذخیره کنم شما میگی زحمت نکش خودم هروقت خواستم بیام تو حسابم یوزر و پس رو میزنم(:

روش های زیادی وجود دارد که ما سعی کردیم مهم ترین آنها را برای شما توضیح دهیم

اما بریم سراغ امنیت در اینستاگرام

۸ قدم برای حفظ امنیت حساب اینستاگرام اشاره می‌کنیم.

۱ -حساب کاربری‌تان را Private کنید.

یکی از نکته‌های مهم حفظ امنیت حساب اینستاگرام محدود کردن آن به دوستانی است که آنها را می‌شناسید. فقط به دوستان مورد اعتمادتان اجازه دهید عکس‌های شما و خانواده و یا هر عکس دیگری که منتشر می‌کنید ببینند. برای این کار باید حساب کاربری اینستاگرام‌تان Private باشد:

- وارد Profile حساب کاربری‌تان شوید
- روی گزینه EDIT YOUR PROFILE کلیک کنید
- در پایین پنجره باز شده روی گزینه Posts are Private کلیک کنید
- مطمئن شود رنگ دکمه Posts are Private آبی شده است به معنی در حالت فعال بودن می‌باشد.

حالا می‌توانید مطمئن شوید فقط افرادی که شما را Follow می‌کنند، می‌توانند عکس‌های شما را ببینند.

۲ -افراد ناشناسی که شما را Follow می‌کنند را Block کنید

بسیار خوب در مرحله قبل شما حساب‌تان را Private کردید اما همچنان افرادی که شما ا Follow می‌کنند قادر هستند عکس‌ها و همچنین موقعیت مکانی آن‌ها یعنی موقعیت شما را ببینند. در پست‌های قبلی در مورد شبکه‌های اجتماعی نوشته بودیم که با کسانی در ارتباط باشید که آن‌ها را می‌شناسید، پس نگاهی بهFollower های خود بیندازید و ببینید ا افرادی هستند که هویت آن‌ها برای شما مشخص نیست ؟ آنها را Block کنید. به این ترتیب فقط افرادی را در قسمتFollower های خود خواهید داشت که می‌شناسید و به آن‌ها اعتماد دارید.

- لیست Followers خود را بررسی کنید
- روی آیکن منو در گوشه سمت راست تپ کنید
- در پنجره باز شده روی گزینه **Block User** کلیک کنید

۳ -اطلاعات حساب کاربری اینستاگرام‌تان را Private نگاه دارید

در قسمت معرفی خودتان اطلاعات بیش اندازه ننویسید و سعی کنید با منتشر نکردن اطلاعات مهم در باره خودتان، حریم شخصی‌تان را حفظ کنید. وارد قسمت EDIT PROFILE حساب کاربری‌تان شوید و اطلاعات بیش از اندازه و مهم‌تان را حذف کنید. این قسمت به خود شما بستگی دارد، ممکن است حتی نوشتن اسم فرزندتان حریم شخصی‌تان را به خطر بیندازد.

۴ -موقعیت خود را منتشر نکنید

یکی دیگر از اقدامات امنیتی اینستاگرام برای حفظ اطلاعات شناسایی شما و همچنین جلوگیری از خطرات دنیای دیجیتال و واقعی، مخفی نگاه داشتن موقعیت‌تان است. مطمئن شوید که سرویس location یا همان موقعیت مکانی شما در حساب کاربری اینستاگرام‌تان خاموش یا غیر فعال است. فراموش نکنید در قدم اول خودتان در عنوان‌های عکس‌هایی که منتشر می‌کنید موقعیت‌تان را ننویسید.

- وارد Profile حساب کاربری‌تان شوید
- وارد قسمت Photo Map شوید
- روی آیکن منو در گوشه سمت راست کلیک کنید
- تغییرات لازم در جهت پاک کردن موقعیت‌تان را انجام دهید.

۵ -گزینه تگ کردن را به حالت تائید دستی تغییر دهید

تصور کنید فردی برای خصومت و یا هر دلیلی حساب اینستاگرام شما را در عکس نامناسبی تگ (Tagging) بکند. و یا شما عکسی را با دوست‌تان انداخته‌اید که نمی‌خواستید منتشر کنید ولی دوست شما این عکس را در اینستاگرام منتشر می‌کند و شما را تگ می‌کند یعنی نام شما و حساب کاربری اینستاگرام‌تان به آن عکس اضافه می‌شود!

برای اینکار باید گزینه تگ کردن را به حالت دستی تغییر دهید به این معنی که شما تشخیص بدهید کدام عکس به شما تعلق دارد یا نه.

- وارد Profile حساب کاربری اینستاگرام‌تان شوید
- وارد قسمت Photos of You شوید
- روی آیکن منو در گوشه سمت راست کلیک کنید
- روی گزینه add photos manually کلیک کنید

۶ -احراز هویت دو عامله را فعال کنید

یکی از نکته‌های مهم **حفظ امنیت حساب اینستاگرام** فعال کردن احراز هویت دو عامله است. احراز هویت دو عامله در واقع یک لایه امنیتی دیگری برای حفاظت از حساب آنلاین شما اضافه می‌کند. در مواقعی که مجرمان سایبری از هر طریقی به رمزعبور شما دسترسی داتشه باشند، با فعال بودن احراز هویت دو عامله نمی‌توانند وارد حساب آنلاین شما شوند زیرا به کد دوم دسترسی ندارند .

این کد دوم منحصر بفرد و تاریخ دار را از طریق اپلیکیشن Duo Mobile یا Google Authenticator دریافت می‌کنید .

چگونه احراز هویت دو عامله اینستاگرام را فعال کنید:

۱ -اپلیکیشن اینستاگرام را باز کنید

۲ -وارد پروفایل کاربری‌تان شوید

۳ -منوی تنظیمات را باز کنیدSettings .

۴ -روی گزینه Two-Factor Authentication تپ کنید

۵ -سپس گزینه Authentication App را فعال کنید .

مطمئن باشید که اپلیکیشن Duo Mobile یا Google Authenticator را نصب کرده باشید.

علاوه بر این در همین مسیر بالا می‌توانید کدهای Backup را هم دریافت کنید، تا در مواقعی که به موبایل خود برای دریافت کد دوم دسترسی نداشتید از این کدها برای ورود به حسابتان استفاده کنید.

۷ -دسترسی اپلیکیشن‌های دیگر به حساب اینستاگرامتان را قطع کنید

احتمالا با حساب اینستاگرام خود در سرویس‌های دیگر حساب کاربری ایجاد کرده‌اید. اگر اینچنین است باید این دسترسی‌ها را کنترل کنید و فقط به اپلیکیشن‌های مطمئن و قابل اعتماد امکان دسترسی بدهید.

بررسی دسترسی اپلیکیشن‌ها به حساب اینستاگرام:

۱ -روی لپ‌تاپ یا کامپیوترتان وارد حساب کاربری اینستاگرام شوید

۲ -روی عکس پروفایلتان کلیک کنید و Edit Profile را انتخاب کنید

۳ -از منوی باز شده Manage Applicationsرا انتخاب کنید. در این صفحه می‌توانید دسترسی اپلیکیشن‌های غیر ضروری یا غیر قابل اعتماد را قطع کنید.

۸ -درخواست تائید حساب کاربری اینستاگرام

این ویژگی برای شفافیت و صحت اعتبار حساب‌های برخی کاربران اینستاگرام است.

ارسال درخواست تائید حساب کاربری به این معنی نیست که حساب شما حتما تائید خواهد شد. برای ارسال درخواست تائید مسیر زیر را دنبال کنید :

از منویSettings ، و بخش Account روی گزینه Request Verification کلیک کنید. سپس نام خود را بنویسید و کپی کارت رسمی هویت که عکس، نام و تاریخ تولد شما مشخص باشد را ارسال کنید.

راهنمایی‌های کلی قبل از ارسال هر پستی در اینستاگرام

- مطمئن شوید عکسی که منتشر می‌کنید اطلاعات مهم شما را نشان نمی‌دهد.
- موقعیت خودتان را مخفی نگاه دارید
- مطمئن شوید عکس‌هایی که منتشر می‌کنید موقعیت شما را لو نمی‌دهند.
- از هشتگ‌هایی که ممکن است اطلاعات شخصی شما را فاش کند استفاده نکنید.
- عکس‌های خشونت آمیز یا تحریک آمیز را منتشر نکنید
- بدون اجازه افراد عکس‌های آن‌ها را منتشر نکنید
- درگیر زورگیری‌های آنلاین نشوید.

در اینستاگرام بر خلاف سایر شبکه های اجتماعی گزینه‌های امنیتی و حریم شخصی زیادی وجود ندارد، و این خود ما هستیم که باید بیشتر احتیاط کنیم.

افراد خلاف کار اینترنتی و یا سارقین واقعی اطلاعات زیادی از ما را از طریق شبکه های اجتماعی، عکس‌ها، ویدئوها و متن‌هایی که منتشر می‌کنیم بدست می‌آورند. پس محتاط باشیم.