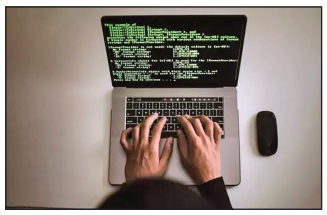
۳ ترفند مقابله با حملات سایبری

حملات سایبری، به‌ویژه حملات مهندسی اجتماعی، همچنان به رشد خود ادامه می‌دهند. با این ۳ راهکار از حملات سایبری جلوگیری کنید: اول ویژگی‌های امنیتی خود را افزایش دهید. سپس نرم‌افزار خود را به‌طور منظم به‌روز کنید و در نهایت فرهنگ آگاهی از امنیت سایبری را ایجاد کنید.

راه‌های محافظت از رمز عبور



محافظت از رمزهای عبور برای حفظ امنیت حساب‌های کاربری آنلاین بسیار اهمیت دارد. استفاده از رمزهای عبور قوی، عدم‌استفاده از یک رمز عبور برای چند حساب، فعال‌سازی احراز هویت دومرحله‌ای، به‌روزرسانی منظم رمزهای عبور، اجتناب از ذخیره رمز عبور در مرورگر و... از مهم‌ترین راه‌های حفاظت از رمز عبور است.

بازخوانی ترفندهای مهمی که کلاهبرداران برای فریب کاربران اینستاگرام استفاده می‌کنند

اینستاگرام روی خط کلاهبرداری

اگر شما تا به حال قربانی کلاهبرداری اینستاگرامی نشده باشید، دست‌کم شنیده‌اید که یکی از دوستان یا آشنایان‌تان در این فضا هدف انواع کلاهبرداری‌ها قرار گرفته است. در این گزارش به بعضی از ترفندهایی که افراد شیاد در اینستاگرام برای کلاهبرداری استفاده می‌کنند می‌پردازیم.

حامی جعلی

اگر خودتان اینفلوئنسر هستید، ممکن است کلاهبردارها با وعده پشتیبانی و حمایت نزدیک‌تان شوند و قرارداد پیشنهادی‌شان هم مشکوک به‌نظر برسد. منظور از این موارد شک برانگیز، درخواست گردش یا اطلاعات حساب بانکی شماست. شاید آنها شماره شبا یا حساب شما را با وعده پرداخت سهم در سود یا هدیه طلب کنند. شاید در ابتدا متوجه جدی‌بودن قضیه نشوید اما کلاهبرداری از اینفلوئنسرها یکی از رایج‌ترین انواع شیادی در حال حاضر شمرده می‌شود.

دعوت به مشاغل جعلی

وقتی بیکار هستید، ممکن است به اشتغال در هر کاری رضایت دهید؛ اما وقتی استخدام‌کننده از شما اطلاعات بانکی و کد ملی درخواست می‌کند دیگر باید به او شک کنید. کلاهبرداری اینستاگرامی در این روش، معمولا بدون درخواست مصاحبه انجام می‌شود. هرگاه استخدام‌کننده پیشنهاد حقوقی بالاتر از حد متعارف بازار کار را برای انجام وظایف کمتر ارائه داد، به واقعی‌بودنش مشکوک شوید.

فروش محصول جعلی

برخی از افراد شیاد مدعی فروش محصولات لاکچری با تخفیف چشمگیر هستند. شما به‌عنوان خریدار می‌توانید برای آنها پول واریز کنید، اما اگر محصولی هم به دست‌تان رسید مطمئن باشید که اصلی نخواهد بود. در برخی موارد از این نوع کلاهبرداری اینستاگرامی، فروشنده ادعا کرده صاحب همان برندی است که محصولاتش را می‌فروشد. ساده‌ترین نکته در این‌باره چیست؟ اینکه وقتی قیمت یک محصول بیش از حد پایین اعلام شده، باید به اصالت آن مشکوک شوید.

سرمایه‌گذاری

این نوع شیادی به کاربران رویای سودآوری به کمک یک سرمایه‌گذاری اولیه را می‌دهد. منظور از این نوع سرمایه‌گذاری می‌تواند چیزی شبیه خرید رمز ارز باشد. کلاهبردار پس از دریافت پول تحت عنوان سرمایه‌گذاری اولیه، راه‌های ارتباطی را می‌بندد و غیب می‌شود. حتی اگر غیب نشود هم شما دیگر نمی‌توانید پول خود را برگردانید. شاید برجسته‌ترین نشانه این نوع کلاهبرداری هم تأکید بر موفقیت در صفحه اینستاگرام کلاهبردار باشد.

کلاهبرداری به سبک کریپتو

برخی مردم توانسته‌اند در سال‌های اخیر با فعالیت در بازار رمز ارزها ثروتمند شوند. از طرفی هم فرصت سوءاستفاده برای رویافروشان به‌وجود آمده تا به کاربران بقبولانند هر کسی می‌تواند با کمترین تلاش و سرمایه به سرعت خودروی فراری خودش را خریداری کند. با تقریب بالایی می‌توانیم بگوییم هر شخصی ضمانت کرد از خرید و فروش رمز ارزها ثروتمند می‌شوید، حتماً به‌دنبال پول درآوردن از خود شماست.

اینفلوئنسرهای قلابی

این دسته‌بندی وسیع است و می‌تواند با موارد دیگری هم از این فهرست (مثلاً مورد بعدی) همپوشانی داشته باشد. گاهی ممکن است شخصی پیام دهد تا درباره سرمایه‌گذاری یا بهبود دیده‌شدن در اینستاگرام به شما مشاوره دهد. توضیحات آنها مختصر به‌نظر می‌رسد و همه تلاش خود را به‌کار می‌گیرند تا شما را به کلیک کردن روی لینک ارسالی وادار کنند. در این موارد از باز کردن لینک خودداری کنید، چون این لینک احتمالاً بدافزار یا ابزار فیشینگ است. تصویر پروفایل آنها معمولاً جذاب انتخاب شده تا نظر شما را جلب کند.

وسوسه جایزه

انواع قرعه‌کشی‌های کاملاً واقعی و معتبر هر روزه در اینستاگرام انجام می‌شود. کلاهبرداران هم معمولاً یک حساب کاربری جعلی با هویت فرد یا کمپانی دیگری راه‌اندازی کرده و تصاویر و ویدئوهای صاحبان اصلی را در صفحه خودشان بازنشر می‌کنند. آنها به این روش برای خودشان تأیید مخاطب دریافت می‌کنند و سپس برنامه قرعه‌کشی را به اجرا درمی‌آورند. در همین روند است که شیادان، شروع به درخواست اطلاعات هویتی و بانکی بیشتر و برخی جزئیات غیرضروری دیگر می‌کنند.

کلاهبرداری عاطفی

برخی از کاربران مرد اینستاگرام پیام‌هایی از کاربران ظاهراً زن دریافت می‌کنند. اگر واقع‌بینانه به این پیام‌ها بنگرید، متوجه رویکرد شیادانه آنها می‌شوید. معمولا لینک‌های مشکوک در پروفایل این افراد وجود دارد. اما بدترین نوع این کلاهبرداری، فریبکاری رمانتیک بلندمدت است. برخی کلاهبردارها به شما نزدیک می‌شوند و توهم رابطه عاطفی واقعی را برایتان ایجاد می‌کنند. آنها به انتظار می‌نشینند سپس موردی اضطراری به ناگهان در زندگی‌شان به‌وجود می‌آید که به پول زیادی نیاز پیدا می‌کنند.

فیشینگ یا ماهیگیری

منظور از حمله فیشینگ (Phishing) در واقع استفاده از صفحات وب جعلی است تا کاربران را به منظور اشتراک اطلاعات شخصی مانند داده‌های بانکی یا رمز عبور اینستاگرام گول بزنند. کلاهبرداران اینستاگرامی با روش فیشینگ می‌توانند حساب بانکی شما را به سرعت خالی کنند یا کنترل حساب اینستاگرامتان را به سرعت به‌دست بگیرند. علاوه بر این، کلاهبردارها شما را در معرض خطر اخاذی، جعل هویت یا استفاده از فراداده برای ورود به سایر خدمات اینترنتی قرار خواهند داد. خوشبختانه وقتی با سازوکار فیشینگ آشنا می‌شوید، دیگر قادر خواهید بود از احتمال وقوع آن جلوگیری کنید. مثلا یا اینستاگرام هرگز شما را به تعلیق حساب کاربری تهدید نمی‌کند؛ مگر اینکه نتوانید هویت خود را به‌عنوان صاحب حساب تأیید کنید. برای مثال، باز کردن ای‌میل، واتساپ یا لینک ارسال شده پیامکی می‌تواند هویت شما را برای ورود به اینستاگرام تأیید کند. آدرس‌های اینترنتی فیشینگ با آدرس‌های متعلق به شرکت‌های واقعی تفاوت دارند. بدین ترتیب وقتی یک URL با عبارتی مانند Instagram. com آغاز نشود، احتمالاً نشان‌دهنده زنگ خطر برای کاربر خواهد بود. وقتی از اینستاگرام یک لینک را باز می‌کنید، همیشه به آدرس دامنه توجه کنید.

نکات کلیدی در امنیت تلفن همراه

تلفن همراه به‌عنوان یک ابزار ضروری و همه‌گیر، نقش محوری در زندگی روزمره افراد ایفا می‌کند. با توجه به حجم بالای داده‌های شخصی و اطلاعات حساس ذخیره‌شده در این دستگاه‌ها، حفظ امنیت آنها از اهمیت بالایی برخوردار است. در این مقاله، نکاتی کلیدی برای ارتقای امنیت تلفن همراه ارائه شده است.

۱.انتخاب رمز عبور قوی و منحصر به فرد

برای انتخاب رمز عبور قوی از ترکیب حروف بزرگ و کوچک، اعداد و نمادها استفاده کنید.

۲.فعال‌سازی قفل‌های بیومتریک

استفاده از قفل‌های بیومتریک مانند اثر انگشت یا تشخیص چهره، لایه امنیتی اضافی را به تلفن همراه شما اضافه می‌کند.

۳.دانلود اپلیکیشن‌ها از منابع معتبر

همیشه اپلیکیشن‌ها را از فروشگاه‌های رسمی مانند گوگل پلی و اپ‌استور، کافه بازار، مایکت و چارخونه دانلود کنید.

۴.به‌روزرسانی سیستم‌عامل و اپلیکیشن‌ها

به‌روزرسانی‌های سیستم‌عامل و اپلیکیشن‌ها اغلب شامل وصله‌های امنیتی هستند که آسیب‌پذیری‌های موجود را برطرف می‌کنند.

۵.محدود کردن دسترسی اپلیکیشن‌ها

به هر اپلیکیشنی اجازه ندهید به همه اطلاعات تلفن همراه شما دسترسی پیدا کند.

۶.احتیاط در استفاده از شبکه‌های وای‌فای عمومی

از اتصال به شبکه‌های وای‌فای عمومی برای انجام تراکنش‌های مالی یا دسترسی به اطلاعات حساس خودداری کنید.

۷.استفاده از نرم‌افزارهای امنیتی

نصب یک نرم‌افزار امنیتی معتبر می‌تواند به شما در شناسایی و حذف ویروس‌ها، بدافزارها و سایر تهدیدات کمک کند.

۸.هوشیاری در برابر پیام‌های فیشینگ

به پیام‌هایی که از شما می‌خواهند اطلاعات شخصی یا مالی خود را وارد کنید، اعتماد نکنید. این پیام‌ها ممکن است توسط کلاهبرداران برای سرقت اطلاعات شما ارسال شده باشند.

۹.قفل کردن تلفن در صورت سرقت

اکثر سیستم‌عامل‌های تلفن همراه امکان قفل کردن از راه دور و پاک کردن داده‌های تلفن را در صورت گم‌شدن یا سرقت فراهم می‌کنند. این قابلیت برای اکثر گوشی‌های اندرویدی و آیفون‌ها وجود دارد تنها کافی است نحوه فعال کردن آن را جست‌وجو کنید.