سایت اسکم چیست؟

دنیای ارزهای دیجیتال با هدف امنیت بیشتر به وجود آمده است. در این دنیای نوین همچنان روش‌های مختلفی برای کلاه برداری و دزدی از کاربران وجود دارد. سایت اسکم یکی از متداول‌ترین روش‌های کلاهبرداری ارز دیجیتال و دزدی از کاربران است که اکثر کاربران نادانسته در دام آنها می‌افتند.

به دلیل توسعه دنیای بلاک چین و اضافه شدن حوزه‌های مختلف و جدید به این فناوری، در حال حاضر راه‌های جدیدی به وجود آمده‌اند تا هکرها و کلاه برداران سایت‌های اسکم را تاسیس کنند. به همین خاطر سایت‌های اسکم خود به انواع مختلفی تقسیم می‌شوند. در این مطلب از مجموعه کیف پول من قصد داریم تا به **انواع سایت‌های اسکم** پرداخته و راه‌های پرهیز از این پلتفرم‌ها را ذکر کنیم.

سایت اسکم چیست؟

سایت اسکم به سایت‌هایی گفته می‌شود که با هدف **کلاه برداری** و دزدی از کاربران ایجاد شده‌اند. چنین سایت‌هایی می‌توانند به روش‌های مختلف شما را مجبور به انجام برخی کارها کنند تا اطلاعات خود را در اختیار هکرها قرار دهید.

سایت‌هایی که اسکم شناخته می‌شوند، لازم نیست از ابتدا جهت دزدی به وجود بیایند. برخی پلتفرم‌ها وجود دارند که در ابتدا به صورت مطمئن و قانونی فعالیت می‌کنند. چنین پلتفرم‌هایی پس از گذشت مدت خاص و جمع کردن تعدادی کاربر، به دلایل از پیش تعیین شده یا به دلیل ورشکست شدن، از کاربران خود کلاه برداری می‌کنند. به همین دلیل تشخیص برخی سایت‌های اسکم دشوار می‌باشد چرا که برخی از این پلتفرم‌ها در ابتدا توانسته‌اند اعتماد کاربران را جلب کنند.

سایت اسکم در دنیای ارزهای دیجیتال سعی می‌کند تا کاربران را به روش‌های مختلفی، مجبور به پرداخت یک نوع دارایی کند. در چنین سایت‌هایی معمولا هکرها از کاربران ارز دیجیتال دریافت می‌کنند تا قابل ردیابی نباشد.

به همین دلیل اسکم‌ها همیشه موفق هستند و پس از کلاهبرداری از کاربران، نمی‌توان آنها را شناسایی کرد. برای این که کاربران در دام کلاهبرداران بیوفتند، روش‌های مختلفی وجود دارد. این افراد می‌توانند از احساسات شما سو استفاده کرده و به درآمد برسند.

ترساندن یا برانگیختن احساس هیجان یکی از بهترین راه‌های هکرها برای استفاده از سایت اسکم است. برای این که یک سایت اسکم به فعالیت خود ادامه دهد، هکرها سعی می‌کنند تا کاربران را از روش‌های مختلفی جذب پلتفرم خود کنند. برای مثال به شما وعده بیت کوین رایگان را می دهند.

فعالیت در شبکه‌های اجتماعی و تبلیغات یکی از متداول‌ترین راه‌ها برای اسکم از کاربران است. سایت‌های اسکم نیز همانند تله هکرها هستند. زمانی که پای خود را در این سایت‌ها قرار دهید، بسته به نوع اسکم، دارایی خود را به یکی از روش‌های از دست خواهید داد.

انواع سایت اسکم

سایت‌های اسکم در انواع مختلف وجود دارند. یعنی هکرها سعی می‌کنند با امتحان کارهای مختلف به دارایی‌های شما برسند. به همین خاطر تشخیص سایت‌های اسکم سخت‌تر و سخت‌تر می‌شود. بهتر است قبل از استفاده از سایت‌ها و پلتفرم‌های غیرمعتبر آنها را بررسی کنید.

در ابتدا بهتر است با انواع سایت‌های اسکم آشنا شوید تا بدانید با چه نوع پلتفرم‌هایی مواجه خواهید بود. به طور کلی سایت‌های اسکم به چند دسته زیر تقسیم می‌شوند:

- سایت‌های فیشینگ
- سایت‌های طرح پانزی یا هرمی
- صرافی‌های ارز دیجیتال تقلبی
- کیف پول‌های تقلبی
- سایت‌های حاوی بدافزارها
- سایت‌های عرضه اولیه سکه

سایت‌های فیشینگ

سایت‌های فیشینگ که قبل از ارزهای دیجیتال نیز برای کارت‌های بانکی استفاده می‌شدند، حال برای ارزهای دیجیتال استفاده می‌شوند. به همین دلیل اکثر کاربرانی که مدتی در دنیای مجازی فعالیت داشته‌اند، چنین عبارتی آشنا است.

هدف این نوع سایت‌ها دریافت اطلاعات شخصی و مهم شما بوده و از راه‌های مختلفی شما را مجبور به وارد کردن اطلاعات می‌کنند. سایت‌های فیشینگ برای این که معتبر به نظر برسند، ظاهری مشابه و برابر با سایت‌های معتبر دارند. درمورد سایت‌های فیشینگ بانکی، هکرها چنین سایت‌هایی را مشابه درگاه‌های پرداخت بانکی طراحی می‌کردند.

در مورد سایت‌های فیشینگ دنیای ارزهای دیجیتال نیز شاهد همین رویه هستیم. اکثر سایت‌های فیشینگ مشابه سایت‌های معتبر طراحی شده‌اند. برای ایجاد حس اطمینان بیشتر نزد مخاطبین، این سایت‌ها از نظر آدرس و دامنه نیز شبیه سایت اصلی هستند.

به همین خاطر تشخیص چنین سایت‌هایی دشوار است. پس از ورود به سایت، کاربر یک خرید را انجام می‌دهد. برای انجام خرید، لازم است تا شما اطلاعات کارت بانکی یا کیف پول خود را وارد کنید. در برخی از سایت‌های فیشینگ مجبور می‌شوید تا اطلاعات شخصی خود را نیز وارد کنید که بیشتر به ضرر شما خواهند بود. لینک **سایت اسکم** به **روش فیشینگ** به طور معمول در همه جای اینترنت پیدا می‌شود. با کلیک و وارد کردن اطلاعات خود در چنین سایت‌هایی شاهد خالی شدن حساب خود خواهید بود.

سایت طرح پانزی یا هرمی

در **طرح‌های پانزی** به جای این که کلاهبرداران در اولین قدم پول شما را بدزدند، اعتماد شما را جلب می‌کنند. در چنین طرح‌هایی این شما هستید که پول خود را در اختیار پلتفرم‌ها قرار می‌دهید. در طرح پانزی برای این که درآمد بیشتری کسب کنید، باید افراد بیشتری به زیرمجموعه خود اضافه کنید.

حداقل این قولی است که از طرف کلاهبردارن به روش طرح هرمی مطرح می‌شود. به طور معمول افراد می‌توانند در ماه‌های اول و دوم از طرح‌های پانزی کسب درآمد کنند. زمانی که تعداد اعضا و پول‌ها دریافت شده به مقدار کافی رسید یا تیم پانزی نتوانست اعضای بیشتری جذب کند، پول کاربران خود را می‌دزدد.

مطلب پیشنهادی : کلود ماینینگ چیست؟

چنین کارهایی در دنیای ارزهای دیجیتال نیز مشاهده می‌شود. شما در یک سایت ثبت نام کرده و مقداری پول برای سرمایه گذاری واریز می‌کنید. برای این که درآمد شما بیشتر شود، لینک دعوت را به دوستان خود می‌فرستید. آنها نیز مجبورند تا مقداری پول در اختیار چنین سایت‌هایی قرار دهند.

صرافی و کیف پول ارز دیجیتال تقلبی

همان‌طور که معلوم است، چنین سایت‌هایی مانند سایت‌های فیشینگ عمل می‌کنند. کاربران در این پلتفرم‌ها اطلاعات خود را وارد می‌کنند و در نهایت دارایی خود را از دست می‌دهند. در روش دیگر که متداول‌تر است، صرافی ارز دیجیتال یا کیف پول به صورت معتبر به کار خود ادامه می‌دهد. برای مثال شما می خواهید اقدام به خرید بیت کوین کنید، اما از طریق سایتی با URL مشابه صرافی های معتبر انجام می دهید و اطلاعات را در اختیار فرد هکر قرار می دهید.

به جای این که دارایی‌های شما در دست خودتان باشد، نزد صرافی یا کیف پول حفظ می‌شود. آنها می‌توانند برای افزایش سرمایه خود، از کاربران بخواهند تا دارایی‌های خود را درون کیف پول یا صرافی افزایش دهند. با افزایش ارزها، کاربران امتیاز دریافت می‌کنند تا برنده پول زیادی شوند.

زمانی که مقدار سرمایه جذب شده به مقدار مورد نظر صرافی یا کیف پول رسید، حساب شما خالی شده و از شما کلاهبرداری می‌شود. بهتر است قبل از سرمایه گذاری و استفاده از چنین سایت‌ها و پلتفرم‌هایی، پیشینه و اعتبار آنها را بسنجید. سعی کنید در پلتفرم‌هایی که قول سرمایه چند برابر و جایزه‌های گران قیمت را می‌دهند، عضو نشوید.

سایت‌های حاوی بدافزار

بدافزارها نوع نرم افزار کامپیوتری هستند که به صورت خواسته یا ناخواسته وارد دستگاه کاربران می‌شوند. بدافزارهایی که برای اسکم از کاربران در دنیای ارزهای دیجیتال استفاده می‌شود، انواع مختلفی دارد. به همین دلیل بهتر است همیشه مراقب استفاده از سایت‌ها و نرم افزارهای جدید باشید.

اولین نوع این بدافزارها، نرم افزارهایی هستند که وارد سیستم شما شده و در هنگام وارد کردن آدرس کیف پول مقصد، آدرس کیف پول هکر و کلاهبردار را وارد می‌کنید. شما تصور می‌کنید که انتقال پول به حساب فرد مورد نظر انجام می‌شود. در صورتی که آدرس کیف پول قرار داده شده، متعلق به فرد هکر است.

در نوع دیگر، بدافزارها سعی می‌کنند تا از سیستم کامپیوتری شما به عنوان بستری برای استخراج بیت کوین استفاده کنند. این نرم افزارها به صورت مخفی و آشکار می‌توانند کار کنند. بدافزارهای این چنینی نیز انواع مختلفی دارند.

برخی از آنها روی سیستم کامپیوتر یا گوشی موبایل نصب می‌شوند. برخی دیگر نیز تنها با مرورگر کامپیوتر کار می‌کنند. زمانی که کاربر در یک سایت وارد شده یا نرم افزاری را نصب کرد، بدافزار شروع به کار می‌کند. این نرم افزار سعی می‌کنند تا از سخت افزار سیستم شما برای استخراج ارز دیجیتال استفاده کند. بدافزارهای معمول نیز وجود دارند. این بدافزارها که متداول‌ترند، سعی دارند تا اطلاعات شما را بدزدند.

سایت عرضه اولیه سکه

عرضه اولیه سکه یا ICO **روش متداولی برای کلاهبرداری در دنیای ارزهای دیجیتال** است. این اتفاق بارها در دنیای ارزهای دیجیتال مشاهده شده و همچنان نیز کاربران در دام این روش‌ها می‌افتند. عرضه اولیه سکه مکانیزمی برای حمایت از

یک ارز دیجیتال یا پروژه بلاک چینی است. اولین پروژه‌ای که از این مکانیزم استفاده کرد، اتریوم بود. در حقیقت، اتریوم از معدود رمزارزهایی است که عرضه اولیه سکه موفق و معتبر داشته است.

کاربران در این روش سعی می‌کنند تا با خرید توکن و کوین های مربوط به یک پروژه، از آن حمایت کنند. پس از این که مقدار سرمایه جذب شده زیاد شد، تیم توسعه از افراد کلاهبرداری کرده و دارایی‌های کاربران را می‌دزدد.

نحوه شناسایی سایت اسکم

هیچ راه معتبر و مطمئنی نیست که بتوانید با استفاده از آن سایت های اسکم را شناسایی کنید. چرا که برخی از این سایت ها در ابتدا به صورت مطمئن عمل می‌کنند و پس از گذشت مدت زمانی، دارایی شما را از دستتان در می‌آورند.

البته بهتر است برای **افزایش امنیت**، همیشه از سایت‌هایی استفاده کنید که از پروتکل HTTPS به جای HTTP استفاده می‌کنند. اگر یک سایت از پروتکل HTTPS استفاده کند، در کنار نوار آدرس سایت، می‌توانید یک علامت قفل را مشاهده کنید. از طرف دیگر بهتر است اطلاعات کارت بانکی یا کیف پول ارز دیجیتال خود را در اختیار هیچ کسی قرار ندهید.

صرافی‌های ارز دیجیتال و کیف پول ها که تمام دارایی شما در اختیار دارند، خطرناک‌تر از بقیه هستند. به همین خاطر باید همیشه از پلتفرم های معتبر و شناخته شده استفاده کنید. در صورت استفاده از پلتفرم های جایگزین، بهتر است همه سرمایه خود را وارد این پلتفرم ها نکنید.

کلیک بر روی لینک های تبلیغاتی و استفاده از سایت هایی که خدمات گران قیمتی را به صورت رایگان عرضه می‌کنند نیز می‌تواند بسیار خطرناک باشد. چرا که هزینه خدمات را باید با دارایی‌های خود پرداخت کنید.