یکی از روش‌های آسان برای کلاهبرداری در بازار رمزارزها متقاعد کردن افراد به سرمایه‌گذاری روی رمزارزهای جدید بی‌ارزش است. ساده‌ترین روش جلوگیری از این روش کلاهبرداری، بررسی درصد کوین‌ها یا توکن‌های توسعه‌دهندگان و مالکان پروژه است



رایج‌ترین شگردهای کلاهبرداری در رمزارزها و روش‌های جلوگیری از آنها

کلاهت را محکم بچسب



رضا کریمی
خبرنگار فناوری

بازار رمزارزها بازار نوپایی است و بسیاری از علاقه‌مندان به سرمایه‌گذاری، دانش و آگاهی کمی از آن دارند. این امر باعث شده کلاهبرداران این بازار را فرصتی مناسب ببینند و به روش‌های مختلف، اقدام به کلاهبرداری از سرمایه‌گذاران کنند. از طرفی، نبود نظارت نهادهای دولتی بر رمزارزها نیز باعث شده مالباختگان به‌سختی بتوانند سرمایه دزدیده‌شده خود را برگردانند. این مساله اهمیت بالای شناخت روش‌های رایج کلاهبرداری در رمزارزها و راه‌های جلوگیری از آن را نشان می‌دهد. روش‌های کلاهبرداری در بازار رمزارزها بسیار متنوع هستند. در این روش‌ها که به آنها «اسکم، Scam» می‌گویند، کلاهبردار اشخاص مختلف را فریب می‌دهد تا اطلاعات مختلف یا سرمایه خود را اختیارش بگذارند. تقریبا در بیشتر مواقع نیز پول دزدیده‌شده قابل بازپس‌گیری نخواهد بود. اگر قصد دارید در دام کلاهبرداران بازار رمزارزها نیفتید، تا پایان همراه ما باشید.

فیشینگ (Phishing)

فیشینگ یکی از رایج‌ترین روش‌های کلاهبرداری اینترنتی در سراسر دنیاست و از آنجایی که بازار رمزارزها، بازاری دیجیتالی است، فیشینگ نیز در آن بسیار مرسوم است. در این روش کلاهبردار به روش‌های مختلف (مثلا ارسال یک ایمیل حاوی یک لینک) به شما صفحاتی نشان می‌دهد که تصور می‌کنید صفحه صرافی یا کیف پول شما است. به بیان بهتر، این صفحه از نظر ظاهری کاملا شبیه به صفحه صرافی یا کیف پول شما است. بسیاری از سرمایه‌گذاران که آگاهی کمی دارند، اطلاعات خود را برای ورود در این صفحات وارد می‌کنند و اسکمرها (یا همان کلاهبرداران دنیای رمزارز) اطلاعات واردشده را ذخیره می‌کنند. به این ترتیب کنترل حساب صرافی یا ولت شما به طور کامل در اختیار کلاهبرداران قرار گرفته و آنها می‌توانند به‌راحتی رمزارزهای شما را برداشت کنند.

روش جلوگیری از فیشینگ

ساده‌ترین روش جلوگیری از فیشینگ، این است که به آدرس سایتی که از شما اطلاعات شما را می‌خواهد دقت کنید. از آنجا که صفحات فیشینگ کاملا از نظر ظاهری شبیه به نمونه‌های واقعی خود هستند، تنها راه تمایز آنها نشانی این صفحات است. علاوه‌بر این، صفحات فیشینگ معمولا پیشوند https ندارند. به طور کلی باز کردن لینک‌های ارسال‌شده از طرف افراد ناشناس به هر شکلی خطرناک است و سعی کنید تا جای ممکن چنین لینک‌هایی را باز نکنید.

راگ پول (Rug pull)

یکی از روش‌های آسان برای کلاهبرداری در بازار رمزارزها، متقاعد کردن افراد به سرمایه‌گذاری روی رمزارزهای جدید بی‌ارزش است. از آنجایی که ساختن یک رمزارز هزینه چندانی ندارد؛ کلاهبرداران به‌راحتی می‌توانند با تبلیغات فراوان افراد زیادی را متقاعد به خرید رمزارز خود کنند. در این روش کلاهبرداران مبلغ قابل‌توجهی از کوین‌ها یا توکن‌های یک رمزارز را در اختیار دارند. این افراد می‌توانند رمزارزهای خود را به‌راحتی بفروشند و پروژه را رها کنند. ارزش رمزارزهای خریداری‌شده قربانیان در این حالت سریعا سقوط می‌کند و تقریبا بی‌ارزش می‌شود. به این روش بسیار مرسوم کلاهبرداری در دنیای رمزارزها راگ پول می‌گویند. افرادی که در دام کلاهبرداران این روش می‌افتند، تقریبا به هیچ روشی نمی‌توانند سرمایه خود را برگردانند.

روش جلوگیری از راگ پول

ساده‌ترین روش جلوگیری از این روش کلاهبرداری، بررسی درصد کوین‌ها یا توکن‌های توسعه‌دهندگان و مالکان پروژه است. امروزه بسیاری از رمزارزهایی که روی بستر پروژه‌های بزرگ‌تر مانند اتریوم یا بایننس راه‌اندازی شده‌اند، به طور دقیق سهم هر سرمایه‌گذار از تعداد کوین‌ها یا توکن‌های پروژه را نشان می‌دهد. هر چقدر درصد مالکیت توسعه‌دهندگان رمزارز بر کوین‌ها و توکن‌های آن کمتر و تعداد آدرس‌های ولت‌های آن بیشتر باشد، احتمال رخ دادن راگ پول کمتر است. همچنین پیش از خریداری رمزارزهای جدید، سوابق تیم و اهداف آن را به‌دقت بررسی کنید.

پانزی (Rug pull)

طرح پانزی یک روش قدیمی کلاهبرداری است که در بازار رمزارزها نیز مرسوم است. در این روش معمولا کلاهبرداران افراد دیگر را ترغیب می‌کنند تا سرمایه‌گذاران جدیدی را برای‌شان پیدا کنند و در ازای آن سود (معمولا توکن یا کوین بیشتر) بگیرند. در این روش سودها از طریق پول‌های سرمایه‌گذاران جدید تامین می‌شود و به سرمایه‌گذاران قدیمی داده می‌شود اما درواقع ارزش جدیدی تولید نشده است. این فرآیند تا زمانی ادامه پیدا می‌کند که سرمایه‌گذار جدیدی وارد این هرم نشود یا سرمایه‌گذاران قبلی سود خود را درخواست کنند. در این حالت، ارزش کوین یا توکن‌های خریداری‌شده سرمایه‌گذاران صفر خواهد شد.

روش جلوگیری از طرح پانزی

طرح پانزی معمولا در رمزارزهای نوپا رخ می‌دهد و تقریبا روش خاصی جز مطالعه و بررسی دقیق پروژه برای جلوگیری از آن وجود ندارد. با این حال، تقریبا در همه کلاهبرداری‌های پانزی ویژگی‌های مشخصی وجود دارد. وعده سود فراوان و پایدار، زیرمجموعه‌گیری، معرفی و همچنین گیج کردن سرمایه‌گذاران با استراتژی‌های پیچیده از جمله این ویژگی‌ها هستند.

طرح پانزی معمولا در رمزارزهای نوپا رخ می‌دهد و تقریبا روش خاصی جز مطالعه و بررسی دقیق پروژه برای جلوگیری از آن وجود ندارد



روش‌های کلاهبرداری در بازار رمزارزها بسیار متنوع هستند. به این روش‌های کلاهبرداری که به آن Scam می‌گویند، کلاهبردار اشخاص مختلف را فریب می‌دهد تا اطلاعات مختلف یا سرمایه خود را اختیارش بگذارند

صرافی‌های قلابی

در این روش کلاهبرداران، مالکان صرافی‌های رمزارز هستند. سرمایه‌گذاران به این صرافی‌ها پول واریز می‌کنند اما امکان برداشت از آنها وجود ندارد.

روش جلوگیری از کلاهبرداری از طریق صرافی قلابی

ساده‌ترین روش بررسی حجم معاملات صرافی‌ها و تعداد کاربران آن است. صرافی‌های نامعتبر حجم معاملات کمی دارند، سفارشات خرید و فروش آنها با تاخیر زیاد اجرا می‌شود و پشتیبانی ندارند.

توکن عرضه اولیه (ICO)

هنگامی که یک رمزارز جدید کار خود را آغاز می‌کند، کوین‌ها و توکن‌های اولیه آن با قیمت بسیار پایینی عرضه می‌شوند. این امر برای تشویق افراد به خرید بیشتر و نوعی تبلیغات برای پروژه‌های نوپاست. به این عرضه اولیه رمزارز ICO می‌گویند. عرضه اولیه توکن یا کوین به خودی خود کلاهبرداری نیست اما بسیاری از کلاهبرداران از آن به عنوان ابزاری برای کلاهبرداری استفاده می‌کنند. بسیاری از اسکمرها در واقع پروژه‌ای را تبلیغ می‌کنند که اصلا وجود ندارد! سرمایه‌گذاران ناآگاه پول خود را به روش‌های مختلف به این افراد پرداخت می‌کنند، ولی در ازای آن چیزی دریافت نمی‌کنند.

روش جلوگیری از کلاهبرداری از طریق ICO

رمزارزهای معتبر، ویژگی‌های خاصی دارند که اگر آنها را بررسی کنید، هرگز در دام این روش کلاهبرداری نخواهید افتاد. وایت پیپر واضح، برنامه‌ها و تقویم مشخص، توسعه‌دهندگان باتجربه و نامدار، جامعه هواداران بزرگ در شبکه‌هایی مانند ردیت و دیسکورد، وبسایت و شبکه‌های اجتماعی فعال و همچنین درصد و روش پخش شدن کوین‌های پروژه (توکنومیکس) از جمله این ویژگی‌هاست.

ایردراپ (Airdrop)

بسیاری از کلاهبرداران از ایردراپ به عنوان ساده‌ترین روش برای تخلیه کیف پول‌های افراد استفاده می‌کنند. ایردراپ به معنای هدیه یک یا چندین توکن یا کوین رمزارز به صورت رایگان به افراد مختلف است. ایردراپ از سوی مالکان پروژه برای تبلیغ بیشتر اجرا می‌شود. این کار کلاهبرداری نیست اما کلاهبرداران می‌توانند از این طریق به اطلاعات کیف پول شما دسترسی پیدا کنند.

روش جلوگیری از کلاهبرداری از طریق ایردراپ

سعی کنید به هیچ عنوان در ایردراپ‌های پروژه‌های جدید و نامعتبر شرکت نکنید و اطلاعات کیف پول خود را در اختیار هیچ‌کس قرار ندهید.