کلاه برداری بیت کوین به چه صورت است؟

با ایجاد هر فناوری جدید، راه‌های مختلفی برای **کلاه برداری** ایجاد می‌شود. بیت کوین معروف‌ترین ارز دیجیتال و باارزش‌ترین آنها است که می‌تواند روش خوبی برای کلاه برداری باشد. شاید با درک مفهوم بلاک چین و ارزهای دیجیتال به این نتیجه برسید که کلاه برداری و دزدی این نوع از دارایی‌ها امکان پذیر نیست، اما ماهیت غیرمتمرکز بودن رمزارزها باعث شده تا **کلاه برداری از طریق ارزهای دیجیتال** رواج پیدا کند.

چرا که نمی‌توان پیگیری درستی در مواجهه با این اتفاقات انجام داد. امروزه راه‌های مختلفی برای **کلاه برداری بیت کوین** به وجود آمده‌اند که می‌خواهیم در این مطلب از کیف پول من به بررسی آنها بپردازیم تا در آینده در دام این کلاه برداری‌ها نیافتید.

کلاه برداری با بیت کوین، آسان‌تر نیز می‌شود!

فراموش نکنید که بیت کوین و بلاک چین برای این به وجود آمده‌اند تا افراد مالکیت کامل دارایی‌های خود را به دست بگیرند. بدون شخص و سازمان سوم و واسطی شما می‌توانید به معامله با افراد دیگر بپردازید و نیاز نیست تا مدرک یا اطلاعات خاصی را به یک سازمان ارائه دهید.

هرچند معامله، فروش و خرید بیت کوین تسهیل یافته، اما کلاه برداری نیز آسان‌تر شده است. بلاک چین یک ماهیت غیرمتمرکز دارد. با این فناوری، امکان تغییر اطلاعات و دزدی از حساب شما به صفر می‌رسد. البته این در صورتی است که تنها شما اطلاعات امنیتی حساب خود را داشته باشید.

بلاک چین تکنولوژی جدیدی است که هیچ فردی نمی‌تواند اطلاعات شما و دارایی‌های شما را تغییر دهد. هرچند ردگیری و مشاهده تراکنش‌ها برای همه امکان پذیر است. این ویژگی نیز به خاطر شفافیت کامل ارزهای دیجیتال و بلاک چین وجود دارد تا همه بتوانند از معاملات و رد و بدل‌های انجام شده در دنیای ارزهای دیجیتال مطلع شوند.

توجه داشته باشید که در دنیای ارزهای دیجیتال، هر تراکنش تنها یک بار انجام می‌شود. زمانی که انجام یک تراکنش را تایید کنید، دیگر امکان برگشت آن وجود ندارد. چون بلاک چین امکان تغییر در داده‌های ثبت شده را به کاربران نمی‌دهد و انجام این کار نیاز به تایید تمامی افراد حاضر در شبکه دارد. پس زمانی که بیت کوین از حساب شما خارج می‌شود، دیگر نمی‌توان آن را برگشت داد.

از طرف دیگر، افراد در دنیای ارزهای دیجیتال به صورت کاملا ناشناس فعالیت می‌کنند. برای این که در دنیای بلاک چین و حوزه‌های مرتبط به آن فعالیت کنید، هیچ اطلاعات شخصی از شما دریافت نخواهد شد و به طور کامل می‌توانید ناشناس باقی بمانید.

شاید این امر برای اکثر افراد یک مزیت باشد، اما همچنان می‌تواند باعث کاهش امنیت شما شود. چرا که دزدی‌ها و کلاه برداری‌ها نیز در این فضا به صورت ناشناس باقی می‌مانند. نبود یک سازمان واسط و ناظر باعث شده تا همه بتوانند بدون تایید هویت در آن فعالیت کنند.

این تنها بخشی از ایرادات بلاک چین و ارزهای دیجیتال است که باعث کلاه برداری‌های بزرگ و کوچک می‌شود. در این دنیای نوین، متداول‌ترین **روش‌های کلاه برداری** به شرح زیر هستند.

فیشینگ با شبکه‌های اجتماعی

افراد زیادی در دنیای بلاک چین فعالیت می‌کنند که مورد تایید همه هستند. افراد تازه وارد حوزه ارزهای دیجیتال سعی می‌کنند با دنبال کردن افراد معروف و ماهر در شبکه‌های اجتماعی، از علم و تجربه آنها استفاده کنند. به همین خاطر شاید هر حرفی که آن فرد بزند، مورد تایید طرفدارانش باشد. به همین خاطر، فیشینگ با شبکه‌های اجتماعی به وجود آمده است. افراد کلاه بردار در این حالت یک حساب کاربری جعلی در شبکه‌های اجتماعی با هویت غیرواقعی ایجاد می‌کنند.

پس از ایجاد حساب، آنها سعی می‌کنند تا برخی اطلاعات مهم و ترند روز را برای کاربران منتشر نمایند. زمانی که این حساب‌های کاربری به محبوبیت رسیدند و کاربران به آنها اعتماد کردند، به راحتی می‌توانند از آنها برای کلاه برداری استفاده کنند.

پس از این مرحله، افراد کلاه بردار سعی می‌کنند تا برخی صفحات **فیشینگ** را برای کاربران منتشر کنند. در اکثر مواقع، کلاه برداران سعی می‌کنند با وعده سودهای زیاد، دریافت بیت کوین رایگان یا ان اف تی، طرفداران خود را گول بزنند.

کلاه برداری صرافی‌های ارز دیجیتال

صرافی ارز دیجیتال، یکی از پایه‌های دنیای بلاک چین و ارزهای دیجیتال است. برای این که ارز دیجیتالی را خریداری کنید، باید دارایی‌های فیزیکی یا ارزهای فیات خود را به ارز دیجیتال تبدیل نمایید. بهترین و سریع‌ترین روش برای دستیابی به این امر، استفاده از صرافی ارز دیجیتال است.

صرافی ارز دیجیتال می‌تواند واسطی برای تبدیل ارزهای فیات به ارزهای دیجیتال باشد. تعدادی صرافی ارز دیجیتال وجود دارد که مورد تایید همه هستند و اکثر افراد فعال در این حوزه، از آن استفاده می‌کنند.

مانند **کلاه برداری‌های فیشینگ**، امکان این که سایت‌های مشابهی با صرافی‌های ارز دیجیتال به وجود آیند وجود دارد. در صورتی که وارد این نوع از سایت‌های صرافی شده و اطلاعات خود را وارد کنید، افراد کلاه بردار می‌توانند وارد حساب کاربری شما در صرافی‌های معتبر شده و تمامی دارایی شما را بدزدند.

در نظر داشته باشید که در صورت خارج شدن ارزهای دیجیتال از حساب شما، امکان برگشت دادن آنها وجود ندارد. به همین خاطر، بهتر است همیشه آدرس صرافی مورد نظر خود را به خاطر بسپارید و تنها از یک آدرس برای ورود به صرافی استفاده کنید.

از طرف دیگر، صرافی‌های جدید و کلاه بردار به وجود آمده‌اند. این صرافی‌ها با تبلیغات زیاد و فعالیت کوتاه مدت به روی کار می‌آیند و کاربران زیادی را جذب خود می‌کنند. پس از این که تعداد کاربران صرافی‌ها افزایش پیدا کرد، آنها به راحتی می‌توانند از حساب‌های کاربران دزدی کنند.

دنیای ارزهای دیجیتال تا به این جای کار، بارها چنین صرافی‌هایی را به خود دیده و به همین خاطر توصیه می‌شود تنها از صرافی‌های معتبر و مطمئن استفاده کنید. البته توسعه دهندگان بلاک چین برای مقابله با این کلاه برداری‌ها، صرافی‌های غیرمتمرکز را به وجود آورده‌اند.

صرافی غیرمتمرکز مانند خود بلاک چین به صورت غیرمتمرکز عمل می‌کند و افراد می‌توانند در آنها ثبت نام کنند. هیچ فردی نمی‌تواند در این صورت به اطلاعات و دارایی‌های شما دسترسی پیدا کند.

باج گیری با بیت کوین

بیت کوین باارزش‌ترین ارز دیجیتال دنیا است. این رمزارز که ارزش زیادی دارد، می‌تواند مورد سو استفاده نیز قرار بگیرد. در صورتی که اطلاعات شخصی یا مهم شما دست فرد دیگری بیافتد، به راحتی می‌تواند شما را تهدید به افشا اطلاعات کند.

این نوع از **کلاه برداری بیت کوین**، ارتباط زیادی با امنیت دنیای بلاک چین و ارزهای دیجیتال ندارد. هرچند فرد کلاه بردار در صورت دریافت ارزهای دیجیتال مورد نظر، دیگر قابل ردیابی نخواهد بود.

این افراد در ازای افشا نکردن اطلاعات شخصی و خصوصی، ارز دیجیتال درخواست می‌کنند. چرا که هویت صاحب کیف پول دیجیتال مشخص نیست. در این حالت، پلیس نیز به سختی می‌تواند صاحب کیف پول و فرد کلاه بردار را ردگیری کند. به همین خاطر توصیه می‌شود اطلاعات خصوصی و حساس خود را در فضای مجازی انتشار ندهید.

بدافزارها

در دنیای تکنولوژی که برای رفاه مردم به وجود آمده، بعضا شاهد عرضه نرم افزارها و برنامه‌های مخرب هستیم. این برنامه‌ها که در دهه‌های اخیر به تعداد آنها افزوده شده برای کارهای مختلفی استفاده می‌شوند. برخی از این برنامه‌ها می‌توانند اطلاعات شما را به سرقت ببرند یا کامپیوتر و گوشی شما را با مشکل مواجه کنند.

هرچند آنتی ویروس‌های قدرتمند و مختلفی منتشر شده‌اند، اما همچنان برخی باج افزارها و نرم افزارهای مخرب می‌توانند امنیت شما را زیر سوال ببرند. یکی از ساده‌ترین روش‌ها برای **کلاه برداری در دنیای بیت کوین**، باج افزارها هستند. این نرم افزارها زمانی که به کار بیافتند، سیستم شخصی یا گوشی موبایل شما را قفل کرده یا با مشکل مواجه می‌کنند.

برای روشن کردن گوشی یا استفاده از آن، برنامه از کاربر می‌خواهد تا مبلغی را به یک حساب واریز کنید. همان‌طور که حدس می‌زنید، مبلغ واریز شده را باید به صورت بیت کوین به یک کیف پول واریز کنید. ناشناس بودن افراد پشت حساب‌های بیت کوین و ارزش بالای این رمزارز باعث شده تا باج افزارها از بیت کوین برای باج‌گیری استفاده کنند.

درصورتی که مبلغ درخواست شده را پرداخت نکنید، امکان افشا اطلاعات حساب‌های کاربری، اطلاعات خصوصی و شخصی و دیگر داده‌ها وجود دارد. برای جلوگیری از این اتفاق، بهتر است تنها از برنامه‌های معتبر و تایید شده استفاده کنید.

نوع دیگر بدافزارها، نرم افزارهای کپی پیست هستند. این نوع از برنامه‌ها به صورت مخفی در سیستم شما نصب شده و اطلاعات کپی شده در حافظه را به یک فرد دیگر ارسال می‌کنند. زمانی که می‌خواهید وارد حساب

کاربری خود در یک صرافی یا کیف پول ارز دیجیتال شوید، با کپی کردن اطلاعات مربوط به حساب کاربری، این نرم افزارها می‌توانند اطلاعات را مشاهده کرده و برای یک فرد دیگر ارسال کنند.

روش پیشرفته‌تر زمانی است که می‌خواهید مقداری بیت کوین یا ارز دیجیتال به یک فرد دیگر انتقال دهید. در هنگام پیست یا وارد کردن آدرس کیف پول فرد مورد نظر، آدرس کیف پول فرد کلاه بردار وارد خواهد شد. در این شرایط، بیت کوین نیز به حساب کلاه بردار واریز می‌شود.

برای به حداقل رساندن تهدید بدافزارها، بهتر است از آنتی ویروس قدرتمندی برای کامپیوتر یا گوشی خود استفاده نمایید تا از شر باج افزارها در امان باشید. در مرحله بعد، توصیه می‌شود هر چند وقت یک بار، از اطلاعات خود فایل پشتیبان تهیه کنید و روی هر بنر و متنی که در اینترنت مشاهده می‌کنید، کلیک ننمایید.

طرح پانزی در دنیای بیت کوین

کلاه برداری هرمی و **طرح پانزی** نوع رایجی از کلاه برداری است که قبل از بیت کوین نیز وجود داشت. طرح پانزی یک روش کلاه برداری از طریق منابع مالی است. در این روش، افراد با ثبت نام در یک شرکت یا پلتفرم، برای دریافت پول، باید افراد دیگری را عضو سازمان کنند.

به طور معمول، وعده پول‌های هنگفت و چند برابر پرداخت شده به اعضا داده می‌شود. وعده این است که در این سازمان‌ها هر چه فرد بیشتری وارد سازمان کنید، پول بیشتری دریافت می‌کنید.

در دنیای بیت کوین و ارزهای دیجیتال نیز چنین روشی به کار گرفته می‌شود. برخی ارزهای دیجیتال نیز به وجود آمده‌اند تا از طریق طرح پانزی به کلاه برداری بپردازند. رمزارز وان کوین، یکی از معروف‌ترین ارزهای کلاه برداری با روش پانزی است. زمانی که صحبت از دریافت بیت کوین بیشتر با معرفی اعضا جدید را مشاهده کردید، می‌توانید به یاد طرح پانزی بیافتید.

ICO یا عرضه اولیه سکه

عرضه اولیه سکه روشی برای حمایت از پروژه‌ها و پلتفرم‌های نوظهور است. در این روش که ابتدا توسط پلتفرم اتریوم به کار گرفته شد، توسعه دهندگان برای دستیابی به اهداف پروژه، نیاز خود به منابع مالی را اعلام می‌کنند.

مبالغ دریافت شده قرار است تا به افراد توسعه دهنده پرداخت شده و صرف توسعه پروژه شود. اتریوم یکی از مثال‌های موفق عرضه اولیه سکه است. در این روش، پلتفرم‌ها برای دریافت حمایت مالی، کوین‌ها و توکن‌های اولیه را با یک قیمت ثابت به حمایت کنندگان عرضه می‌کنند. افرادی که قصد حمایت از پروژه را دارند، می‌توانند به مقدار دلخواه خود سکه خریداری کنند.

استفاده از عرضه اولیه سکه، امروزه روشی برای کلاه برداری است. چرا که کلاه برداران سعی می‌کنند با ایجاد پروژه‌های تقلبی، سکه‌های فیک خود را به حمایت کنندگان عرضه کنند. آنها در ازای اهداف توکن‌های بی ارزش، از کاربران بیت کوین یا ارزهای دیگر را دریافت می‌کنند. اتریوم یکی از معدود پلتفرم‌هایی است که توانسته با استفاده از روش عرضه اولیه سکه موفق عمل کند.