در این مقاله به راه های فیشینگ و اسکمینگ در بازار ارز دیجیتال می پردازیم. این روش های کلاهبرداری باعث سرقت دارایی های دیجیتال افراد زیادی در سراسر دنیا شده است. این مقاله را تا انتها بخوانید تا قربانی این نوع کلاهبرداری ها نشوید. ما در آموزش خصوصی صفر تا صد بازار ارز دیجیتال به صورت مفصل راجع به این اتفاق ها صحبت کرده ایم. بسیاری از افراد اما بخاطر استرس معاملاتی که دارند ممکن است برخی از این جزئیات را از قلم بندازند و قربانی این نوع از کلاهبرداری ها بشوند.در قلمرو ارزهای دیجیتال که به سرعت در حال تکامل هستند، هم سرمایه گذاران باتجربه و هم تازه واردان با تهدید کلاهبرداری های فیشینگ کریپتو با هدف سوء استفاده از اعتماد آنها برای سرقت اطلاعات حساس یا دارایی های رمزنگاری شده روبرو هستند. با افزایش محبوبیت ارزهای دیجیتال، کلاهبرداران تکنیک های فیشینگ خود را تقویت می کنند، صرافی ها و کیف پول ارز دیجیتال قانونی را جعل می کنند و از مهندسی اجتماعی برای دسترسی غیرمجاز به دارایی های دیجیتال استفاده می کنند.

فیشینگ در بازار ارز دیجیتال به روش های زیر صورت می گیرد

کلاهبرداری از طریق پست و پیام

یکی از روش‌های رایج مورد استفاده در کلاهبرداری‌های فیشینگ رمزنگاری جعل هویت نهادهای قابل اعتماد، مانند صرافی‌های ارز دیجیتال یا ارائه‌دهندگان کیف پول است. کلاهبرداران ایمیل ها یا پیام هایی را ارسال می کنند که به نظر می رسد از طرف این سازمان های قانونی باشد، با استفاده از مارک، آرم ها و آدرس های ایمیل مشابه. هدف آنها فریب گیرندگان به این باور است که ارتباط از یک منبع قابل اعتماد است.

برای رسیدن به این هدف، کلاهبرداران ممکن است از تکنیک هایی مانند جعل ایمیل استفاده کنند، جایی که آدرس ایمیل فرستنده را جعل می کنند تا به نظر برسد که گویی از یک سازمان قانونی است. آنها همچنین ممکن است از تاکتیک‌های مهندسی اجتماعی برای شخصی‌سازی پیام‌ها و واقعی‌تر جلوه دادن آنها استفاده کنند. کلاهبرداران با جعل هویت نهادهای مورد

اعتماد، از اعتماد و اعتبار مرتبط با این سازمان ها سوء استفاده می کنند تا کاربران را فریب دهند تا اقداماتی را انجام دهند که امنیت آنها را به خطر می اندازد.

درخواست های پشتیبانی جعلی

کلاهبرداران فیشینگ ارزهای دیجیتال اغلب به عنوان نمایندگان پشتیبانی مشتری صرافی های قانونی ارزهای دیجیتال یا ارائه دهندگان کیف پول ظاهر می شوند. آنها ایمیل یا پیام هایی را برای کاربران ناآگاه ارسال می کنند و ادعا می کنند که مشکلی در حساب کاربری آنها وجود دارد یا یک تراکنش معلق که نیاز به توجه فوری دارد.

کلاهبرداران یک روش تماس یا پیوندی به یک وب‌سایت پشتیبانی جعلی ارائه می‌کنند که در آن از کاربران خواسته می‌شود اعتبار ورود به سیستم یا سایر اطلاعات حساس خود را وارد کنند.

عمری لاهاو، مدیر عامل و یکی از بنیانگذاران Blockfence - یک افزونه مرورگر امنیت رمزنگاری - به کوین تلگراف گفت: «به یاد داشته باشید که اگر شخصی پیام یا ایمیلی ناخواسته برای شما ارسال کند، احتمالاً چیزی از شما می خواهد. این پیوندها و پیوست‌ها می‌توانند حاوی بدافزارهایی باشند که برای سرقت کلیدهای شما یا دسترسی به سیستم‌های شما طراحی شده‌اند.»

علاوه بر این، آنها می توانند شما را به وب سایت های فیشینگ هدایت کنند. برای اطمینان از ایمنی، همیشه هویت فرستنده و مشروعیت ایمیل را تأیید کنید. از کلیک مستقیم روی پیوندها خودداری کنید. URL را کپی کرده و در مرورگر خود جایگذاری کنید و هرگونه اختلاف املایی در نام دامنه را به دقت بررسی کنید.

کلاهبرداران با جعل هویت پرسنل پشتیبانی، از اعتماد کاربران به کانال های پشتیبانی مشتری قانونی سوء استفاده می کنند. علاوه بر این، آنها تمایل به حل و فصل سریع مسائل را به دام می اندازند و باعث می شود که کاربران با میل اطلاعات خصوصی خود را فاش کنند، که کلاهبرداران می توانند بعداً از آنها برای اهداف مخرب استفاده کنند.

وب سایت های جعلی و پلتفرم های شبیه سازی شده

بازیگران مخرب همچنین می‌توانند وب‌سایت‌ها و پلتفرم‌های جعلی بسازند تا کاربران ناآگاه را جذب کنند.

جعل نام دامنه تکنیکی است که در آن کلاهبرداران نام های دامنه ای را ثبت می کنند که شباهت زیادی به نام صرافی های قانونی ارزهای دیجیتال یا ارائه دهندگان کیف پول دارند. به عنوان مثال، آنها ممکن است دامنه ای مانند "exchnage.com" را به جای "exchange.com" یا "myethwallet" به جای "myetherwallet" ثبت کنند. متأسفانه، این تغییرات جزئی می تواند توسط کاربران ناآگاه به راحتی نادیده گرفته شود.

نرم افزارهای مخرب و برنامه های موبایل

هکرها همچنین می توانند از نرم افزارهای مخرب برای هدف قرار دادن کاربران استفاده کنند. کی لاگرها و ربودن کلیپ بورد تکنیک هایی هستند که کلاهبرداران فیشینگ رمزنگاری برای سرقت اطلاعات حساس از دستگاه های کاربران استفاده می کنند.

کی لاگرها برنامه‌های نرم‌افزاری مخربی هستند که هر ضربه‌ای که کاربر روی دستگاه خود انجام می‌دهد را ضبط می‌کند. هنگامی که کاربران اعتبار ورود یا کلیدهای خصوصی خود را وارد می کنند، کی لاگر این اطلاعات را می گیرد و آن را به کلاهبرداران می فرستد. ربودن کلیپ بورد شامل رهگیری محتوای کپی شده در کلیپ بورد دستگاه است.

ایمنی در برابر کلاهبرداری فیشینگ

برای محافظت در برابر فیشینگ، کاربران باید احراز هویت دو مرحله‌ای (FA۲) را فعال کنند، احراز هویت مبتنی بر سخت‌افزار یا نرم‌افزار را به آن‌هایی که مبتنی بر پیامک هستند ترجیح دهند، URLهای وب‌سایت را به‌صورت دستی وارد کنند، روی پیوندها برای تأیید مقصد حرکت کنند، پیوست‌های ایمیل را با نرم‌افزار آنتی‌ویروس اسکن کنند، نرم‌افزار را نگه دارند. به روز شده و از نرم افزارهای امنیتی معتبر استفاده کنید. علاوه بر این، آموزش خود در مورد آخرین تکنیک‌های فیشینگ و دنبال کردن منابع مورد اعتماد در جامعه ارزهای دیجیتال برای به‌روزرسانی‌های امنیتی، می‌تواند از کلاهبرداری‌های فیشینگ بیشتر محافظت کند.

روش های مقابله با فیشینگ و اسکمینگ ارز دیجیتال

اریک پارکر، مدیر عامل Giddy، توصیه می کند که نسبت به ارتباطات ناخواسته یا پیشنهادهایی که برای درست بودن بیش از حد خوب به نظر می رسند، تردید داشته باشید، زیرا اغلب نشان دهنده کلاهبرداری هستند. تاکتیک‌های رایج فیشینگ عبارتند از جعل هویت اشخاص مورد اعتماد از طریق ایمیل یا پیام، تظاهر به عنوان پشتیبانی مشتری برای درخواست اطلاعات حساس و ایجاد وب‌سایت‌های جعلی یا پلتفرم‌های شبیه‌سازی شده با تغییرات جزئی در نام دامنه برای فریب کاربران.

Omri Lahav، مدیر عامل Blockfence، بر تأیید هویت فرستنده و URLهای وب سایت و اجتناب از کلیک مستقیم روی لینک از ایمیل ها یا پیام ها تأکید دارد. کلاهبرداران همچنین از نرم افزارهای مخربی مانند کی لاگرها و سرقت کلیپ بورد برای سرقت اطلاعات از دستگاه های کاربران استفاده می کنند.

اسکمینگ در بازار ارز دیجیتال

کلاهبرداری های ارزهای دیجیتال با استفاده از تاکتیک های مختلف برای کلاهبرداری افراد توسط کلاهبرداران در حال افزایش است. در اینجا برخی از کلاهبرداری های رایج ارزهای دیجیتال و نحوه محافظت از خود آورده شده است:

طرح های سرمایه گذاری بیت کوین

کلاهبرداران به عنوان مدیران سرمایه‌گذاری ظاهر می‌شوند و وعده بازدهی بالایی می‌دهند، اما در عوض هزینه‌های اولیه و اطلاعات شخصی را می‌دزدند.تأییدیه های جعلی افراد مشهور برای جذب قربانیان به سرمایه گذاری های تقلبی استفاده می شود.

کلاهبرداری راگ پول

کلاهبرداران یک پروژه یا کوین جدید را تبلیغ می کنند، وجوه جمع آوری می کنند، سپس ناپدید می شوند و سرمایه گذاران را با دارایی های بی ارزش می گذارند.

مثال قابل توجه: کلاهبرداری با سکه مرکب، که حدود ۳ میلیون دلار از سرمایه گذاران کلاهبرداری کرد.

کلاهبرداری های عاشقانه

افراد فریب می‌خورند تا در روابط عاشقانه آنلاین، ارز دیجیتال را بخرند یا بدهند، فقط برای اینکه کلاهبردار بعداً ناپدید شود.

حملات Man-in-the-Middle

کلاهبرداران اطلاعات کلیدی ارسال شده از طریق شبکه های عمومی را رهگیری می کنند.استفاده از VPN می تواند به رمزگذاری داده ها و جلوگیری از چنین حملاتی کمک کند.

کلاهبرداری های هدیه ارز دیجیتال در رسانه های اجتماعی

پست های تقلبی وعده هدایای بیت کوین را می دهند که اغلب از تاییدیه های جعلی افراد مشهور برای جذب قربانیان به سایت های مخرب استفاده می کنند.

طرح های پانزی

سرمایه‌گذاران جدید با وعده‌های بازدهی بالا جذب می‌شوند، اما وجوه سرمایه‌گذاران جدید برای پرداخت به سرمایه‌گذاران قدیمی‌تر استفاده می‌شود.

پیشنهادهای استخدامی و کارمندان متقلب

کلاهبرداران جعل هویت استخدام‌کنندگان یا جویندگان کار برای دسترسی به حساب‌های ارزهای دیجیتال یا هدف قرار دادن شرکت‌ها برای حملات سایبری هستند.

مثال قابل توجه: کلاهبرداری "نیروی کار سایه" کره شمالی که منجر به سرقت ۶۰۰ میلیون دلاری شد.

حملات وام فلش

مهاجمان برای دستکاری در قیمت گذاری در پلتفرم های DeFi وجوه قرض می گیرند و از اختلاف قیمت سود می برند.

مثال قابل توجه: Platypus Finance 8.5 میلیون دلار در یک حمله وام فوری در فوریه ۲۰۲۳ از دست داد.

اقدامات حفاظتی

مراقب وعده هایی که با سودهای بزرگ همراه است باشید، فقط ارز دیجیتال را به عنوان پرداخت، تعهدات قراردادی و تاییدیه های جعلی بپذیرید.

استانداردهای امنیتی دیجیتال مانند رمزهای عبور قوی، استفاده از اتصالات ایمن یا VPN و انتخاب فضای ذخیره سازی امن برای ارز دیجیتال خود را رعایت کنید.هرگز کلیدهای کیف پول یا کدهای دسترسی را با کسی به اشتراک نگذارید.

به بازارهای شناخته شده مبادلات ارز دیجیتال پایبند باشید و قبل از انجام معاملات یا سرمایه گذاری در ارزهای دیجیتال، تحقیقات کاملی انجام دهید.با اطلاع و رعایت احتیاط، افراد می توانند بهتر از خود در برابر این کلاهبرداری ها و سایر کلاهبرداری های ارزهای دیجیتال محافظت کنند.