بررسی روش های کلاهبرداری از طریق ارزهای دیجیتال و بیت کوین Bitcoin

نویسنده: امید فدوی

شیوه های کلاهبرداری از طریق بیت کوین Bitcoinو ارزهای دیجیتال به چه صورت هست؟

در این مقاله به طور جامع می خواهیم به بررسی روش های کلاهبرداری از طریق ارزهای دیجیتال و بیت کوین بپردازیم و شما را با تمامی راه و روش های شناخته شده آشنا کرده و بگوییم چطور از این نوع کلاهبرداری ها در امان بمانید.

اگر بخواهیم خیلی کوتاه تفاوت کلاهبرداری در ارزهای دیجیتال و ارز های سنتی مانند دلار و ریال را برای شما بیان کنیم. باید بگوییم که در ارزهای سنتی شما امکان پیگیری دارید. یعنی شما می توانید به بانک خود و یا سازمان های مربوطه مراجعه کرده و اعلام برداشت غیرمجاز و کلاهبرداری کرده و در مراحل بعدی می توانید شکایت کنید. در این حالت امکان پیگیری و اینکه مبدا و مقصد پول کجا و به نام چه کسانی بوده است مشخص می شود. در بحث ارز های دیجیتال اما اوضاع کمی متفاوت است. نه سازمان مرکزی وجود دارد که شما بخواهید به آن شکایت کنید و نه اصلا نام و مشخصات واقعی وحود دارد که بخواهید به دنبال آن باشید.

درواقع یکی از بزرگترین و بهترین ویژگی ارزهای دیجیتال که ناشناس بودن است در همچین مواقعی می تواند به ضرر برخی کاربران، مخصوصا افراد تازه کار باشد. پس مهم است که پیش از ورود به این بازار پر رونق و پر سود، کمی با شیوه های کلاهبرداری آن نیز آشنایی داشته باشید.

فهرست مطالب

فهرست مطالب

اهمیت داشتن امنیت

همان طور که می دانید در بحث ارز های دیجیتال از آن جا که این ارز ها ارزش زیادی دارند و مبالغ زیادی در این صنعت سرمایه گذاری شده، امنیت عامل بسیار مهمی است. در ادامه ی مقاله قصد داریم شما را با یک راهنمای کامل درباره ی کلاهبرداری با استفاده از ارز های دیجیتال همراهی کنیم.

در این مقاله شما را با انواع کلاهبرداری ها، بدافزار ها و سایر مسایل مهم در زمینه ی امنیت آشنا می کنیم. با این که روز به روز مردم آگاه تر شده و با روش های کلاهبرداری بیشتر آشنا شده و خود را از آن ها دور می کنند اما در این میان کلاهبردار ها هم بیکار ننشسته و همواره روش ها جدید و خلاقانه (!) ای را برای کلاهبرداری اختراع می کنند.

در این مقاله ما این کلاهبرداری ها را به ۱۴ روش کلی دسته بندی کرده ایم و در ادامه هر کدام از آن ها را برای شما توضیح خواهیم داد. با ما همراه باشید.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از ICOها

ICOها درواقع همان عرضه عمومی توکن ها هستند. در مطالعه ای که به تازگی منتشر شده است، مشخص شده حدود ۸۰ درصد از این ICOهای انجام شده در سال ۲۰۱۷ درواقع کلاهبرداری بوده و به عنوان اسکم شناحته شده است.

کلاهبرداری Confido

یکی از مشهور ترین کلاهبرداری های ICO در سال ۲۰۱۷ مربوط به Confido است. Confido موفق شد در نوامبر ۲۰۱۷ با استفاده از برگزاری یک عرضه عمومی توکن، مبلغی معادل ۳۷۵ هزار دلار سرمایه جمع کند و ناگهان ناپدید شود.

پس از این که اخبار مربوط به کلاهبرداری این توکن منتشر شد، ارزش آن در بازار سقوط کرد. قیمت این توکن در بازار در عرض دو ساعت از ۰.۶۰ دلار به ۰.۱۰ دلار رسید. پس از آن هم تنها چند ساعت بعد و در دومین مرحله از سقوط، ارزش آن به زیر یک سنت رسید.

کلاهبرداری Centra

اگر فکر می کنید کلاهبرداری Confido خیلی بزرگ بوده باید بگوییم که اصلا این طور نیست! کلاهبرداری بعدی که می خواهیم درباره ی آن به شما بگوییم بسیار بزرگ تر است.

کلاهبرداری Centra بسیار بزرگ تر بود. در این کلاهبرداری مبلغ ۳۲ میلیون دلار جمع آوری شد. این پروژه آنقدر توانست برای خود تبلیغ کند که حتی افراد مشهوری مانند Floyd Mayweather و DJ Khaled هم از حامیان آن بودند.

البته این کلاهبرداری برای موسسان آن پایان خوشی نداشت. هر دو موسس این توکن در آپریل ۲۰۱۸ دستگیر شدند. مانند سایر کلاهبرداری های دیگر، این توکن هم بعد از اخبار منتشر شده ارزش خود را در بازار از دست داد و تقریبا به کلی نابود شد.

پروفایل های تقلبی

در ارتباط با کلاهبرداری از طریق ICOها یک روش دیگر هم وجود دارد. این روش ایجاد پروفایل ها ساختگی و تقلبی برای یک پروژه ی ساختگی است. کلاهبرداران در این روش با استفاده از عکس های تصادفی و یا عکس افراد مشهور که به راحتی و در حالت های مختلف در اینترنت قابل دسترسی است، آن ها را به عنوان تیم پروژه و پشتیبان کننده ی ارز معرفی کرده و با فریب دادن افراد از آن ها پول دریافت کرده و پس از آن ناپدید می شوند.

تصاویر تیم ICOها را می توان در گوگل ردیابی کرد. می توانید تصویر تیم را در قسمت تصاویر گوگل آپلود کنید و منتظر نتایج بمانید. اگر عکسی که آپلود کردید را در جستجوی گوگل و با عنوانی متفاوت پیدا کردید احتمالا باید نگران شوید! زیرا به احتمال زیاد در پروژه کلاهبردار ها می خواهید شرکت کنید.

تحقیق کردن

البته همه ی ICOها اینطور نیستند و با کمی سرچ در اینترنت و عضویت در انجمن های گفت و گو می توانید با افرادی که اطلاع بیشتری دارند صحبت کرده و از معتبر بودن ICOاطمینان حاصل کنید.

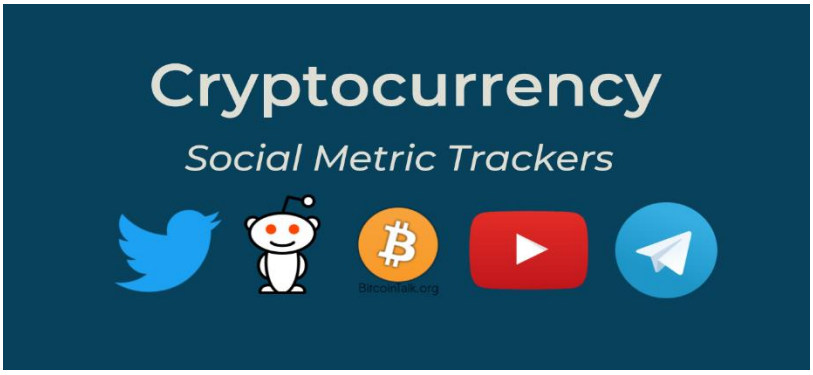
البته در این میان مشاوران ارز دیجیتال را هم فراموش نکنید. اگر در زمینه ی ارز های دیجیتال حرفه ای نیستید بهترین راه مشاوره گرفتن از اشخاصی هست که در این زمینه حرفه ای هستند.

مقاله ی زیر را در ارتباط با مشاوان ارز دیجیتال مطالعه کنید:

مشاور ارز دیجیتال کیست و چگونه میتوان از مشاوره نتایج مثبت کسب کرد

همچنین می توانید از ***مشاوره ارزدیجیتال*** آکادمی امید فدوی نیز استفاده کرده و فعالیت خود را در زمینه ارز های دیجیتال با آگاهی کامل آغاز کنید.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از شبکه های اجتماعی



این مورد یکی از رایج ترین روش های کلاهبرداری است. در واقع این روش آن قدر متداول هست که ارز دیجیتال تنها قسمتی کوچک از کلاهبرداری در فضای مجازی و شبکه های اجتماعی است.

اگر اخبار را دنبال کرده باشید حتما با خبر های مربوط به کلاهبرداری در شبکه های اجتماعی مانند فیسبوک، توییتر، تلگرام، اینستاگرام و سایر شبکه های اجتماعی برخورد کرده اید.

کلاهبردار ها در بسیاری از مواقع با استفاده کردن از هویت و تصویر افراد مشهور مانند Vitalik Buterin و Elon Musk و یا حتی افرادی که خیلی هم شناخته شده نیستند اقدام به ایجاد مسابقه های جعلی کرده و یا با تهیه کردن یک ایده ی جذاب و وعده ی پرداخت جایزه و پاداش های خوب، مردم را به شرکت در آن وسوسه می کنند.

آن ها معمولا برای ثبت نام در این برنامه ها به شما لینک هایی می دهند و از شما می خواهند با کلیک کردن بر روی آن و پر کردن فرم نام خود را در لیست قرعه کشی قرار دهید. در برخی مواقع برای شرکت در این برنامه ها باید پول هم پرداخت کنید.

جایزه بزرگ!

اجازه دهید این مورد را با یک مثال در دنیای ارز های دیجیتال به شما توضیح دهیم.

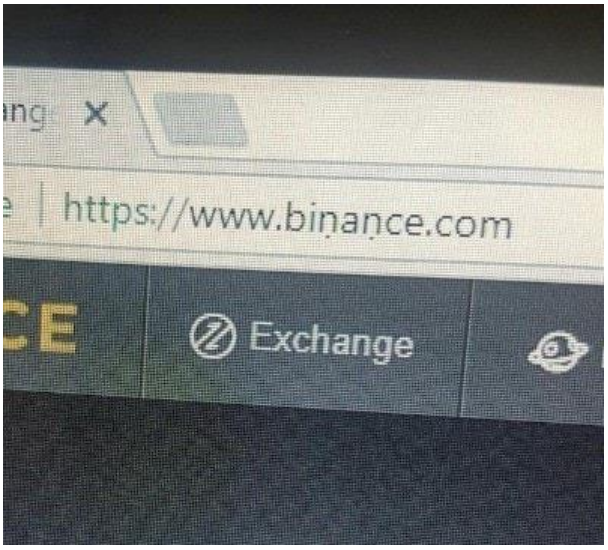
برخی اسکمر ها از مردم می خواهند یک اتریوم به یک آدرس مشخص ارسال کنند و در ازای آن شانس دریافت جایزه ی ۱۰ یا ۱۰۰ برابری را خواهند داشت. حال فرض کنید این ترفند با استفاده پروفایلی انجام شود که عکس و مشخصات یک فرد مشهور مانند ایلان ماسک را دارد.

افرادی که در دنیای مجازی حرفه ای نیستند و از راه های تشخیص پروفایل فیک از اصلی خبر ندارند ممکن است به راحتی فریب خورده و پول خود را از دست بدهند.

این نکته را فراموش نکنید که ارز های دیجیتال هم مانند پول های کاغذی با ارزش هستند و هیچ کس بی دلیل به کسی پول مجانی نمی دهد!

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از سایت های تقلبی

برخی از کلاهبردار ها از نام سایت های مشهور کپی برداری کرده و با ایجاد یک سایت مشابه سایت اصلی و قرار دادن پروژه های مشابه در سایت اقدام به کلاهبرداری می کنند.



در این روش آن ها یک سایت با طراحی کاملا مشابه سایت اصلی و شاید به اختلاف های بسیار کوچک و جزئی درست می کنند که شاید تشخیص آن در نگاه اول اصلا ممکن نباشد.

آدرس اینترنتی این سایت ها هم مشابه سایت های اصلی و با یک اختلاف کوچک، برای مثال یک حرف کم یا بیشتر و یا پسوند متفاوت درست می شود که اگر دقت نکنید ممکن است متوجه این تغییر هم نشوید.

این کار معمولا برای سایت های معروف و ICOهای پر طرفدار انجام می شود.

روش فریب دادن

در این روش فرد و یا افراد قربانی وارد سایت شده و از آن جا که عنوان سایت و طراحی آن مشابه سایت اصلی هست متوجه تقلبی بودن سایت نمی شوند. آن ها در این سایت مشخصات خود را وارد می کنند و این اطلاعات مستقیما به دست هکر ها می رسد.

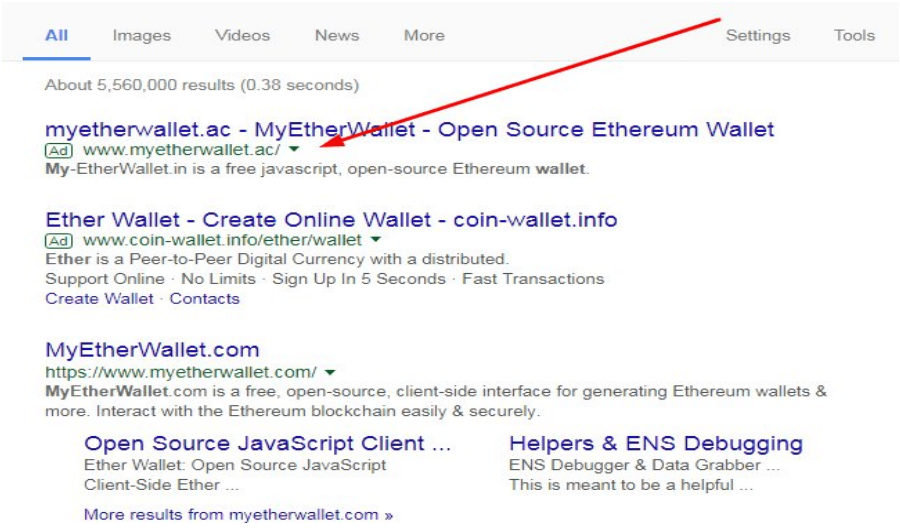
از آن جا که برای مثال این کلاهبردار ها سایت یک صرافی را شبیه سازی کرده اند، فرد مشخصات حساب خود را که در این صرافی دارد وارد می کند. سپس کلاهبردار می تواند با استفاده از این مشخصات در سایت اصلی به حساب قربانی وارد شود و آن را خالی کند.

در یک روش دیگر، باز هم یک سایت مشابه ساخته می شود اما این بار به جای کیف پول اصلی، کیف پول کلاهبردار به جای کیف پول مقصد وارد شده است و افراد با دست خودشان پول را به حساب جعلی وارد می کنند.

برای این که از اصل بودن سابت مطمئن شوید، همیشه آدرس سایت مورد نظر را بوک مارک کنید و از صحیح بودن آن مطمئن شوید.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از تبلیغات اسکم گوگل

شاید باورش سخت باشد اما شما به راحتی و با استفاده از یک سایت در صفحه ی اصلی و اول گوگل می توانید فریب بخورید. بسیاری از اسکمر ها یک سایت جعلی ساخته و آن را در بخش تبلیغات گوگل قرار می دهند. از آن جا که این تبلیغ ها معمولا در صفحه ی اول سرچ و در بالای صفحه قرار می گیرد افراد زیادی ممکن است فریب بخورند.



این سایت ها که با عنوان فیشینگ شناخته می شوند با این هدف ساخته می شوند که افراد با سرچ کردن عنوان مورد نظر آن ها در گوگل، سایتشان را در بالای صفحه ببینند و به آن وارد شوند و سپس با وارد کردن مشخصات، اطلاعات لازم را به دست هکر ها برسانند.

برای جلوگیری از ورود به این گونه از سایت ها می توانید در گوگل کروم از افزونه ی Metamask.io استفاده کنید. این افزونه سایت های فیشینگ را شناسایی کرده و به شما هشدار می دهد.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از هک کردن DNS

در این بخش می توانیم دو وبسایت را برای شما مثال بزنیم. یکی از این سایت ها یک اکسچنج غیر معتبر به نام Etherdelta است. سایت بعدی که می خواهیم به شما معرفی کنیم یک کیف پول آنلاین به نام MyEtherWalletاست. هر دوی این سایت ها از قربانیان هک شدن DNSهستند.

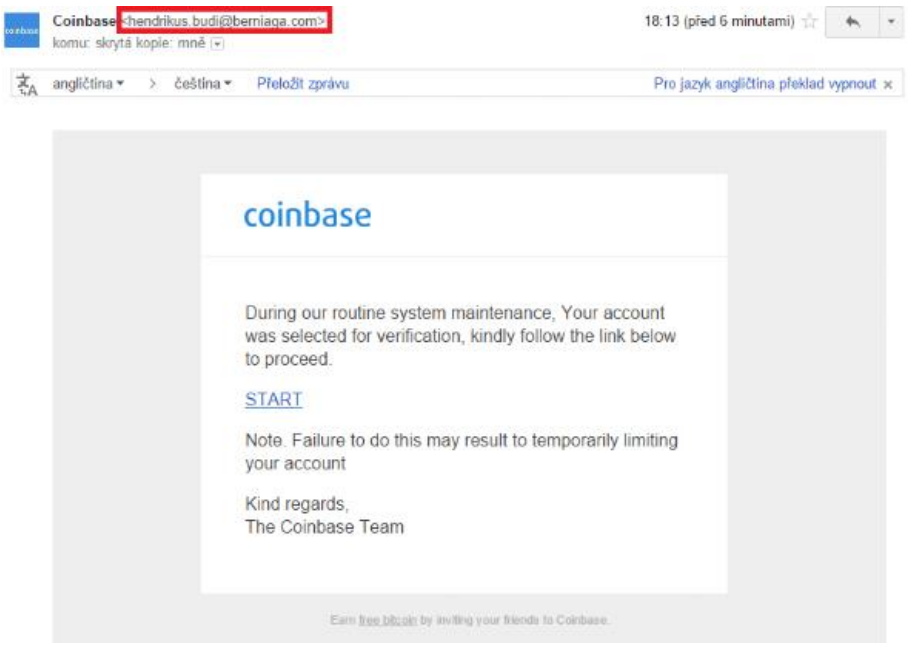
نحوه هک شدن

نحوه انجام این نوع کلاهبرداری به این صورت است که با استفاده از هک کردن و تغییر DNS، ترافیک و بازدید از سایت اصلی به وبسات مورد نظر کلاهبردار ها منتقل می شود.

در این روش آدرس سایت به درستی وارد شده و شخص به یک وب سایت دقیقا مانند سایت اصلی وارد می شود اما در واقع این سایت جعلی بوده و اطلاعات کاربران را سرقت می کند.

این شیوه یکی از بدترین روش ها برای کاربران است. زیرا در این روش شما کاملا سایت را درست وارد کرده اید و عملا نباید چیزی غلط از آب در بیاید اما با این حال شما به سایت جعلی وارد شده اید.

در این حالت شما تنها یک راه برای با خبر شدن از اعتبار سایت دارید و آن هم چک کردن اعتبار گواهینامه SSLاست. این گواهینامه را می توانید در بخش نوار آدرس مرورگر خود ملاحظه کنید.



در این روش این گونه به مخاطب القا می شود که این ایمیل از یک مرجع معتبر ارسال شده است. اما نه تنها سایت ارسال کننده اصلی و معتبر نیست، بلکه اطلاعات درون آن هم جعلی است. در لینک هایی که در این گونه ایمیل ها قرار دارد شما به سایت های جعلی وارد می شوید و با وارد کردن اطلاعات شخصی خودتان، آن ها را در اختیار افراد کلاهبردار قرار می دهید.

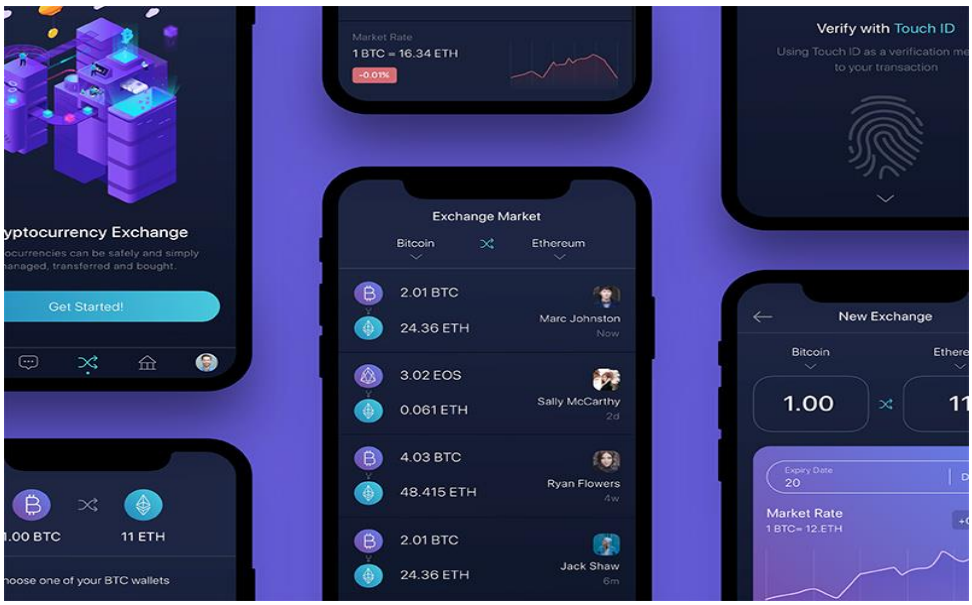
جمع آوری این گونه ایمیل ها معمولا از طریق ICOهای جعلی انجام می پذیرد. در این روش از دیتابیس ایمیل ها و سایر اطلاعات شخصی موجود، برای فریب دادن افراد استفاده می شود.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از تیم پشتیبانی کننده ی اسکم

نوع دیگری از کلاهبرداری فیشینگ، گروه و یا افرادی هستند که ادعا می کنند تیم پشتیبانی یک پروژه هستند. آن ها با این روش از شما اطلاعات شخصی، واریز کردن مبلغ و یا آدرس کلید خصوصی را طلب می کنند.

این افراد راه های مختلفی را برای برقراری ارتباط با افراد مورد نظرشان انتخاب می کنند و نمی توان گفت چه روشی مطمئن است و چه روشی خطرناک.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از اپلیکیشن های تقلبی و ساختگی



باید به این نکته توجه کنید که هنگامی که قصد خرید و فروش و تبدیل ارز های متفاوت را دارید باید حتما به صرافی های معتبر و آدرس های معتبر آن ها مراجعه کنید. برخی از این پلتفرم ها مانند LocalBitcoins و بایننس و KuCoin از دسته ی صرافی های معتبر هستند.

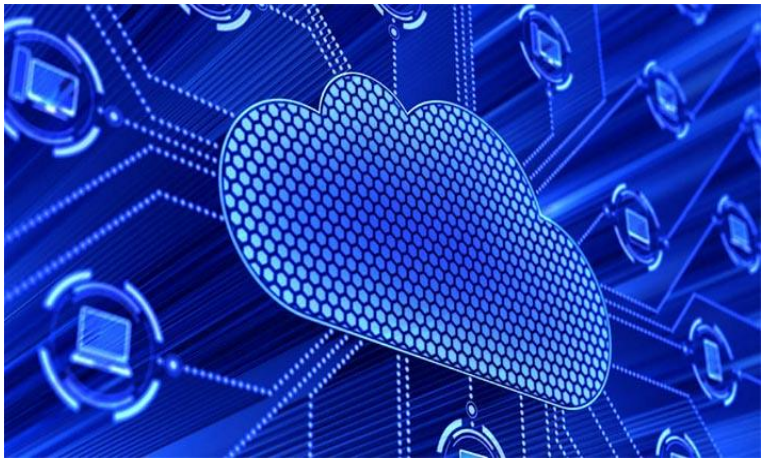
در چند سال گذشته صرافی های زیادی برای انجام خدمات و تراکنش های ارز های دیجیتال تاسیس شده اند. اما همه ی این صرافی ها امن و قابل اعتماد نیستند. این احتمال همیشه وجود دارد که افراد سودجو و کلاهبردار با ایجاد یک صرافی و یا ساختن اپلیکیشن های موبایلی قصد داسته باشند دارایی کاربران را سرقت کنند.

این مطلب هم میتونه براتون مفید باشه: چرا به آموزش تریدینگ ارزهای دیجیتال نیاز دارید؟

نمونه ی یکی از این صرافی ها BitKRX بود. این صرافی در سال ۲۰۱۷ و توسط دولت کره جنوبی تعطیل و توقیف شد.

همیشه از اپلیکیشن هایی که بر روی تلفن همراه خود نصب می کنید مطمئن شوید. همیشه از نسخه اصلی استفاده کنید و به برنامه هایی که ادعا می کنند همان نسخه اصلی به همراه قابلیت های ویژه و اضافه تر هستند اعتماد نکنید.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از استخراج به صورت ابری



از آن جا که روز به روز هزینه برق و تهیه ی دستگاه های ماینر زیاد می شود، بسیاری به سمت استخراج ابری می روند. همین امر باعث شده کلاهبردار ها به این روش استخراج هم وارد شده و فعالیت های خودشان را گسترش دهند!

یکی از نمونه های این گونه کلاهبرداری سایت MiningMax است. این سایت به کاربران خود وعده داده بود که در ازای سرمایه گذاری ۳۲۰۰ دلاری می تواند سرمایه آن ها را در طول دو سال به همراه پورسانت ۲۰۰ دلاری برگرداند. این سایت در نهایت مبلغی در حدود ۲۵۰ میلیون دلار از پول سرمایه گذاران را برداشته و محو شد.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از ترفند های پونزی و چند سطحی

در ابتدا اجازه دهید ترفند پونزی را برای شما توضیح دهیم. در این روش کلاهبردار ها سرمایه افراد و اعضای جدید را دریافت کرده و با استفاده از آن ها سود افراد قدیمی تر را پرداخت می کنند.

این کار آن قدر ادامه پیدا می کند تا سرانجام به نقطه ای می رسد که برای ادامه ی کار نیاز به مبلغ بسیار زیادی است و دیگر امکان پرداخت با کمک پول اعضا جدید ممکن نیست. در این لحظه است که مدیران کلاهبردار سایت، تمام پول ها را جمع کرده و پا به فرار می گذارند.

ترفند پونزی در دنیای واقعی

شناخته شده ترین کلاهبرداری با استفاده از این ترفند مربوط به پروژه ی Bitconnect است. این سایت موفق شد در کمال تعجب حدود یک سال به فعالیت خود ادامه دهد. البته در نهایت بزرگ ترین کلاهبرداری پونزی را به نام خود ثبت کردند.

در همان زمان هایی که کلاهبرداری این سیستم مشخص شد و اخبار آن پخش شد، ارزش کل بازار پروژه ی Bitconnect به حدود دو میلیارد دلار می رسید. قیمت هر کدام از ارز های آن ها هم حدود ۳۲۰ دلار قیمت داشت. پس از بخش شدن خبر و مشخص شدن کلاهبرداری این گروه ارزش سکه های آن در عرض ۲۴ ساعت به ۶ دلار رسید.

BitConnect Coin Lending Profits Interest

Lending Amount	Interest (Accrued Daily)	Capital Back
$100 - $1000	Volatility Software Interest (up to 40 % Per Month)	After 299 Days
$1010 - $5000	Volatility Software Interest + 0.10% Daily (up to 40 % Per Month)	After 239 Days
$5010 - $10000	Volatility Software Interest + 0.20% Daily (up to 40 % Per Month)	After 179 Days
$10010 - $100000	Volatility Software Interest + 0.25% Daily (up to 40 % Per Month)	After 120 Days

افراد زیادی از پروژه Bitconnect حمایت می کردند و این ارز دنبال کننده ی زیادی داشت. بازاریابی انجام شده برای این پروژه بسیار بزرگ و موفق بود و توانسته بود افراد زیادی را به سمت خود جذب کند.

اما در نهایت این نکته را فراموش نکنید که اگر یک پیشنهاد خیلی خوب است و پیشنهادی را به شما می دهد که در هیچ کجای دیگر نمی توان آن را یافت، شاید بهتر است قبل از این که در آن سرمایه گذاری کنید کمی بیشتر فکر و پرس و جو کنید.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از ایجاد بدافزار های استخراج ارز دیجیتال

به طور کلی در زمینه ی ارز های دیجیتال دو نوع بد افزار وجود دارد که در ادامه آن ها را به شما معرفی می کنیم.

نوع اول)

نرم افزار های مخربی که بدون اجازه و اطلاع کاربر بر روی سیستم مورد استفاده مانند کامپیوتر و موبایل نصب می شوند. هدف از این گونه بد افزار ها دسترسی به اطلاعات خصوصی کاربر، موجودی ارز و دسترسی به کلید خصوصی است.

نوع دوم)

نوع بعدی از این گونه بد افزار ها، نرم افزار های استخراج هستند که به طور مخفیانه و بدون اطلاع کاربر از منابع سیستم آلوده شده استفاده کرده و با آن ها به استخراج ارز های دیجیتال مانند مونرو می پردازند.

یکی از راه های تشخیص این که سیستم شما به بر افزار نوع دوم آلوده شده است افزایش استفاده از CPUو GPUدستگاه است. علاوه بر آن داغ شدن بیش از اندازه سیستم و افزایش صدای فن ها هم یکی دیگر از این نشانه ها است.

برای جلوگیری از آلوده شدن به هرگونه بد افزاری، مطمئن شوید که نرم افزار هایی که اقدام به نصب آن ها می کنید معتبر بوده و از سایت ها و یا منابع معتبری تهیه شده باشند.

اگر از مرورگر گوگل کروم استفاده می کنید همیشه به افزونه هایی که بر روی آن نصب کرده اید توجه کنید.

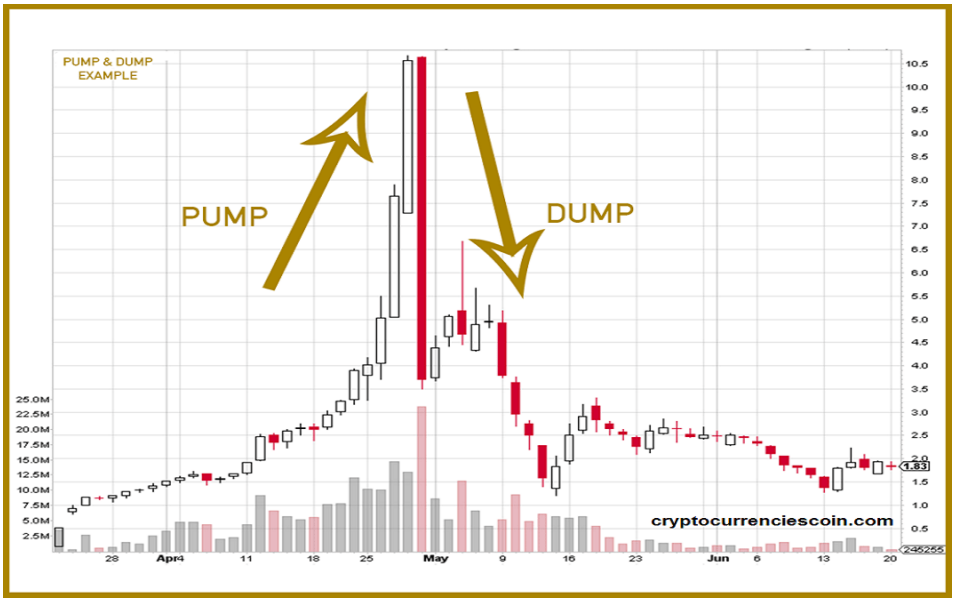
کلاهبرداری از طریق ارزهای دیجیتال با استفاده از گروه های سرمایه گذاری اسکم

این گروه های سرمایه گذاری معمولا در دو پیام رسان تلگرام و دیسکورد تشکیل می شوند. در این گروه ها برای سرمایه گذاری در ICOها پیشنهاد های جذابی ارائه می شود. این افراد از مردم می خواهند برای شرکت در این گروه ها و سرمایه گذاری ها برای آنان ارز ارسال کنند. در ازای دریافت وجه به مردم گفته می شود توکن خریداری شده ی آن ها بعدا به حساب آن ها ریخته خواهد شد.

البته تمام این گروه ها کلاهبردار نیستند و گروه های سالم و معتبر هم در بین آن ها یافت می شود. اما در این میان همیشه باید به کلاهبردار ها توجه ویژه ای کرد.

فراموش نکنید که در دنیای ارز های کاغذی شما شاید بتوانید نام صاحب حساب و مشخصاتی از آن را پیدا کنید اما این گزینه در مورد ارز های دیجیتال در دسترس نیست. به دلیل این که ارز های دیجیتال ذاتا ناشناس هستند، در صورتی که ارزی را برای کلاهبردار ها ارسال کنید از هیچ طریقی امکان پیگیری و بازگشت وجه را ندارید.

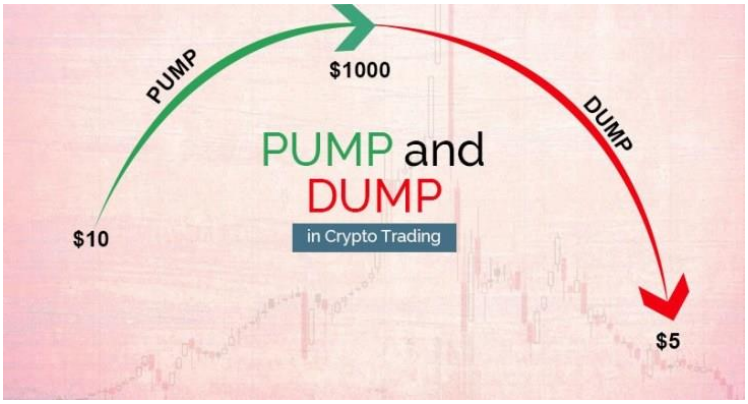
کلاهبرداری از طریق ارزهای دیجیتال با استفاده از پامپ و دامپ کردن



گروه هایی که در زمینه ی پامپ و دامپ کردن فعال هستند کارشان به این صورت هست که در قیمت و ارزش ارز ها دست کاری می کنند. آن ها این کار را با دستکاری در حجم و تعداد معاملات انجام می دهند. این کار معمولا بر روی ارز هایی با ارزش و قیمت پایین انجام می شود.

نحوه انجام این کار هم به این صورت است که این افراد به صورت هماهنگ شروع به خرید یک ارز مشخص می کنند. پس از این که خرید ها انجام شد قیمت برای مدتی بالا می رود. نتیجه ی بالا رفتن قیمت حجوم افراد عادی برای خرید آن ارز است. در این بخش است که کلاهبردار ها ارز های خودشان را با قیمت بالا می فروشند. پس از این که ارز ها با قیمت بالا به فروش رسید، از حجم معاملات کاسته شده و قیمت افت می کند.

البته باید بدانید که این گروه ها در دسته ها و سطوح مختلفی مشغول به کار هستند. در ابتدا گروه های رده بالا اقدام به خرید ارز می کنند و پس از آن که قیمت بالا رفت و پامپ شد به گروه های پایین تر اطلاع می دهند.



توضیحات یک جوان ۲۰ ساله روسی درباره ی روش دستکاری در قیمت توکن ها

یک جوان ۲۰ ساله ی روسی درباره ی روش کارش در زمینه ی دست کاری قیمت ارز های دیجیتل توضیحات جالبی داده است.

او میگوید دو سال پیش و زمانی که ۱۸ سال سن داشت بدون این که اطلاع زیادی از ارز های دیجیتال داشته باشد به یک استارت آپ که در زمینه ی کریپتو فعالیت می کرد پیوست. کار این استارت آپ کمک کردن به توکن ها و سکه های جدید برای لیست شدن در صرافی ها معتبر مانند کوین کپ بود.

فراموش نکنید که در حال حاضر تعداد ارز های دیجیتال قدیمی و معتبر که ارزش آن ها ثابت شده زیاد است و اگر ارز جدیدی پدید آمد که بدون دلیل مشخص و منطقی رشد معاملات زیادی داشت شاید بهتر است برای سرمایه گذاری در آن کمی بیشتر دقت کنید.

اگر یک جوان ۲۰ ساله می تواند با یک گروه همکاری کرده و تراکنش های ساختگی صد هزار دلاری ایجاد کند، پس افراد دیگری هم هستند که این کار را با رقم های بیشتر و به شکل گسترده تر انجام دهند.

بررسی قوانین صرافی

صرافی کوین کپ فقط سکه هایی را لیست می کند که حجم معاملات آن ها بیشتر از روزی ۱۰۰ هزار دلار باشد. بیشتر توکن هایی که این جوان روسی به نام الکسی بر روی آن ها کار می کرد، سکه های جدید و بی ارزشی بودند که حتی به مرز صد هزار دلار نزدیک هم نبودند. حتی بعضی از این سکه ها کلاهبرداری بودند.

الکسی و همکارانش به این نتیجه رسیدند که با انجام یکسری خرید و فروش های ساختگی می توانند ارزش ارز ها را بالا ببرند. آن ها یک ربات ساختند که بدون این که پولی رد و بدل شود درخواست های خرید و فروش درست می کرد و ارزش توکن را بالا می برد.

آن ها موفق شدند ارزش ۲۸ توکن را به صورت ساختگی بالا ببرند.

کلاهبرداری از طریق ارزهای دیجیتال با استفاده از هک کردن شماره موبایل

برخی از افراد گزارش داده اند که دارایی و ارز های آن ها با حملاتی که به شماره تلفن همراهشان شده به سرقت رفته است.

روش کار در این روش به این صورت است که کلاهبردار ها به شرکت ارائه دهنده ی سیم کارت زنگ زده و ادعا می کنند که صاحب خط هستند. در بخش بعد اگر موفق شدند شرکت را قانع کنند که صاحب خط هستند، از آن ها می خواهند که شما ره را به یک خط جدید انتقال دهند.

در نتیجه ی این انتقال، هکر به ایمیل، ورود دو مرحله ای و سایر ابزار های لازم برای ورود به کیف پول و به سرقت بردن ارز ها دست پیدا می کند.

نشانه هایی برای تشخیص کلاهبرداری ارزهای دیجیتال

در این قسمت می خواهیم به شما پنج روش را بگوییم که در آن احتمال وجود کلاهبرداری بسیار زیاد است. اگر با هر کدام از موارد زیر برخورد کردید بهتر است کمی فکر کنید، شاید شما در یک قدمی قربانی شدن باشید!

وعده دادن سود های بسیار بالا و فضایی

همیشه باید به این نکته توجه داشته باشید که وعده ی سود های بسیار عجیب و فضایی معمولا هیچ کدام به حقیقت نمی پیوندند. البته تمام این پروژه ها هم دروغین نیستند، اما اگر با پروژه ای برخورد داشتید که وعده ی سود فضایی می داد بهتر است بیشتر تحقیق کنید.

دعوت کردن از سایر افراد

اگر در جایی مانند شرکت در یک سرمایه گذاری از شما خواسته شد که برای ورود ابتدا باید از سایر افراد دعوت کنید که به آن سرمایه گذاری بپیوندند، احتمالا شما با یک سیستم و روش چند سطحی و یا ترفند پونزی برخورد کرده اید.

البته باید بدانید که سیستم همکاری در فروش و برنامه های دعوت از دوستان وجود دارد و هیچ مشکلی هم ندارد. بسیاری از پروژه های معتبر هستند که شما در ازای دعوت از دوستان و آشنایان می توانید پورسانت دریافت کنید.

اما اگر احساس کردید پروژه ای که قصد شرکت در آن را دارید بیش از اندازه روی دعوت از سایرین اصرار دارد شاید بهتر باشد که به تحقیقات خودتان ادامه دهید.

درخواست کلید خصوصی

هیچ گاه و تحت هیچ شرایطی رمز عبور، کلید خصوص و یا عبارت بازیابی رمز کیف پول را برای هیچ کس فاش نکنید. در این مورد دیگر اما و اگر وجود ندارد. هر شخص، پروژه و یا ICOای که از شما رمز خصوصی را بخواهد بدون شک کلاهبردار است.

کلاهبردار های پیشین

باید بدانید که خیلی کم پیش می آید آدم ها واقعا تغییر کنند. یک کلاهبردار همیشه کلاهبردار است و آن حس را در خود دارد. اگر با پروژه ای برخورد کردید که افرادی در آن شرکت دارند که به کلاهبرداری متهم شده و یا محکوم شده اند شاید بهتر باشد که سرمایه خود را برداشته و در جای دیگری سرمایه گذاری کنید.

تیم پروژه

هرگز به مقالات و صحبت های گفته شده در یک سایت اعتماد نکنید. شما باید اکانت لینکدین شخص و پروژه را پیدا کنید و همچنین در گوگل هم به جستجو بپردازید. سعی کنید اکانت های معتبر فیسبوک، توییتر و سایر شبکه ها و سایت های مرتبط با آن شخص را پیدا کرده و از معتبر بودن آن ها اطمینان حاصل کنید.

روش های بررسی یک ICO

در این بخش می خواهیم به شما روش هایی را معرفی کنیم که با کمک آن ها می توانید از معتبر بودن یک ICO مطمئن شوید.

عمومیت

- آیا اسامی و چهره های مرتبط با این پروژه وجود دارد؟
- آیا قرارداد همکاری با سایر شرکت ها منعقد شده است؟
- آیا پروژه نقشه راه دارد؟
- آیا پروژه محصول فعال دارد یا تنها در حد یک ایده است؟

فعالیت

باید بدانید که اگر یک پروژه توسط سازندگانش رها شده باشد پس شایسته سرمایه گذاری و وقت گذاشتن را ندارد.

- افراد در شبکه های اجتماعی چه صحبت هایی درباره ی این سکه می کنند؟
- واکنش افراد در برابر سوال درباره ی پروژه چگونه است؟
- آیا جامعه ی فعالی برای پروژه وجود دارد؟

تکنولوژی

بلاک چین همه چیز نیست و هنوز هم موارد دیگری برای بروز بودن وجود دارد.

- آیا تکنولوژی ارائه شده توسط این پروژه در واقع برای حل یک مشکل آمده است؟
- ارز دیگری هم وجود دارد که همین مشکل را حل کند؟

تاریخچه

سوابق همیشه اهمیت دارند.

- آیا هدف مورد نظر پروژه، هدف درستی است؟
- آیا تیم پروژه موفق شده به این اهداف دست پیدا کند؟
- آیا در طول انجام این پروژه با مشکلی برخورد کرده اند؟
- آیا این سکه قبلا پامپ و دامپ شده است؟
- آیا تغییرات جدیدی در ساختار تیم پروژه ایجاد شده است؟

این ها همگی مواردی بودند که باید برای مطمئن شدن از اعتبار یک ICOپاسخشان را پیدا کنید.

پیشنهاد می کنیم پس از مطالعه این مقاله حتما از ***کلاهبرداری ارزدیجیتال*** دیدن فرمایید. این آموزش ویدیویی موقتا به طور کاملا رایگان در سایت قرار داده شده است و کامل کننده این مقاله می باشد.

ارز دیجیتال e2c

پیش از آن که به بررسی این ارز و کلاهبرداری آن بپردازیم، ابتدا کمی آن را برای شما معرفی می کنیم.

ارز دیجیتال e2cبا هدف پیشرفت و ارتقای انرژی سبز و سوخت های فسیلی ایجاد شده است. این ارز چندی پیش اقدام به جمع آوری سرمایه کرد و افراد بسیار زیادی در آن شرکت کردند.

در پشت این ارز دیجیتال، شرکت WorldWide energy قرار دارد. این شرکت ادعا کرده فعالیت های خود را در زمینه ی معاملات و مبادلات بازار انرژی و تحقیقات و ایجاد پیشرفت در زمینه ی انرژی سبز دنبال می کند.

کلاهبرداری e2c

همیشه و با پیدایش صنایع جدید، خیلی سریع پای کلاهبردار ها هم به آن صنعت باز می شود. افراد کلاهبردار همیشه در کناری منتظر یک فرصت جدید هستند تا با استفاده از آن کلاهبرداری کرده و سرمایه مردم را به سرقت ببرند.

کلاهبرداری از ارز های دیجیتال مخصوصا به این دلیل که امکان پیگیری و ردیابی ارز های دیجیتال وجود ندارد به شکل گسترده ای در حال انجام است و اصلا نمی توان به راحتی این افراد سودجو و کلاهبردار را تشخیص داد و پیدا کرد.

اگر می خواهید بدانید منظور ما از «گسترده» بودن کلاهبرداری در ارز های دیجیتال چیست به این آمار توجه کنید:

حدود ۸۰ درصد از ICOهای برگذار شده کلاهبرداری (اسکم) هستند.

اگر این آمار را باور ندارید باید بگوییم که این آمار توسط سازمان ها و سایت های بسیار معتبر منتشر شده و اصلا دروغ نیست. حتی بسیاری بر این باور هستند که این درصد بسیار بالاتر از چیزی است که اعلام شده!

کلاهبرداری ارزهای دیجیتال

در این میان اما افرادی هستند که با ساده ترین روش های کلاهبرداری فریب می خورند. برخی از این روش ها آن قدر مشخص هستند که اگر فقط یک سرچ ساده در سطح اینترنت انجام می شد، جعلی بودن آن مشخص می شد.

یکی از این کلاهبرداری ارزهای دیجیتال مربوط به ارز دیجیتال e2cاست. ارز دیجیتال e2cادعا کرده است که توانسته پلتفرمی برای انجام معاملات انرژی راه اندازی کند. اگر این پروژه را با ICOسایر پروژه های معتبر مقایسه کنید، به راحتی متوجه کلاهبرداری e2cخواهید شد. با بررسی این دلایل به راحتی می توان به غیر معتبر بودن ارز دیجیتال e2cپی برد.

این مطلب هم میتونه براتون مفید باشه: Cryptofriends چیست و آیا کلاهبرداری پانزی است؟

در ادامه می خواهیم به شما دلایلی که به کلاهبرداری e2cاشاره دارند را معرفی و بررسی کنیم.

دلایل کلاهبرداری e2c

در این قسمت می خواهیم ۸ دلیل برای شما بیاوریم و با بررسی آن ها به شما کلاهبرداری e2cرا ثابت کنیم.

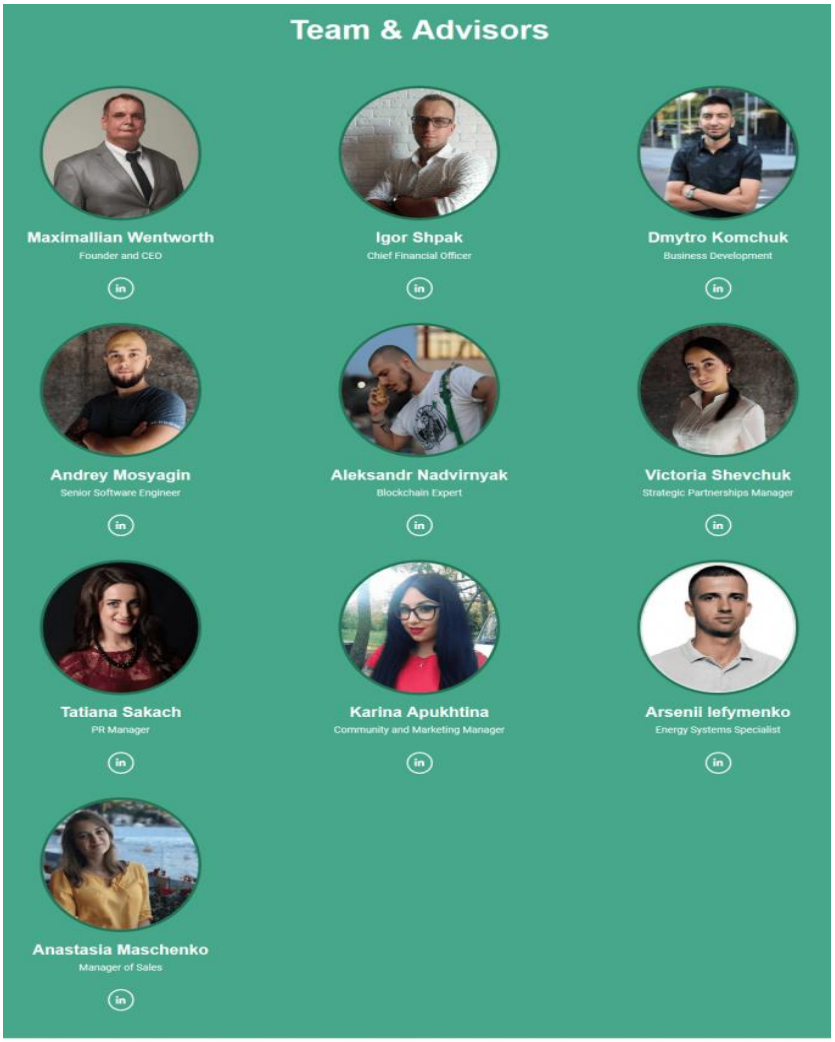
در ابتدا این هشت دلیل را به صورت عنوان به شما معرفی کرده و در ادامه هر کدام را به طور کامل بررسی می کنیم.

- نبودن جزئیات دقیق و شفاف درباره ی تیم پروژه
- عدم وجود هرگونه مشاور
- لیست نشدن پروژه در دایرکتوری ها و سایت های معتبر
- وجود موارد مشکوک در سایت
- وجود نشانه هایی مبنی بر سابقه ی کلاهبرداری
- مسدود شدن حساب ها در سایت medium.com
- عدم وجود هیچ ویدیویی از این پروژه
- وجود نداشتن یک محل آزاد برای تبادل نظر درباره ی پروژه

حال در ادامه ی مقاله هر کدام از دلایل بالا را به طور کامل برای شما معرفی می کنیم.

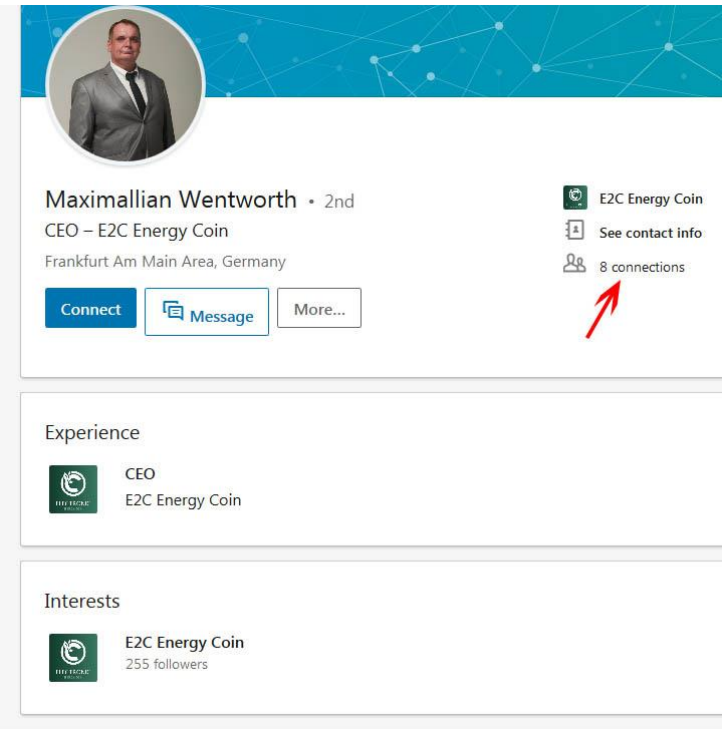
نبودن جزئیات دقیق و شفاف درباره ی تیم پروژه

یکی از فاکتور های بسیار مهم و شاید اصلی ترین فاکتور جهت بررسی یک پروژه، تیم آن پروژه است.



با مشاهده ی اصلاعاتی که از تیم پروژه ی این ارز در سایت آن ها درج شده و بررسی آن، هیچ نشانه ای از وجود یک تیم واقعی پیدا نشده است. تنها اطلاعاتی که درباره ی این تیم منتشر شده چند عکس و اطلاعات ضد و نقیض است. البته به همراه چند حساب نا مربوط از لینکدین.

برای مثال اگر حساب کاربری Maximallian Wentworth که به عنوان موسس و مدیر اجرایی این پروژه معرفی شده را در لینکدین مشاهده کنیم، هیچ اطلاعاتی درباره ی او وجود ندارد. در حساب او اصلا صحبتی از میزان تحصیلات، سوابق کاری و حرفه ای او به چشم نمی خورد. این حساب تنها دارای هشت کانکشن است.



لینکدین

اگر با سایت لینکدین آشنا باشید حتما می دانید که یک شخص حرفه ای و واقعی در آن هویت مشخصی دارد و اطلاعات پروفایل او حتما کامل است. افراد حرفه ای در پروفایل خود از تجربیات و سوابق کاری و تحصیلی خود صحبت کرده و آن ها را اعلام می کنند. علاوه بر آن تعداد ارتباطات آن ها بسیار بیشتر از هشت عدد است.

البته این پروفایل ناقص تنها مربوط به موسس این تیم نبود. با مشاهده ی پروفایل سایر اعضا باز هم به همین مشکلات برخورد کردیم. البته بعضی از آن ها پروفایل کامل تری دارند اما تفاوت خیلی زیادی با هم ندارند.

ما برای آن که مطمئن شویم به یکی از این پروفایل ها پیام دادیم. پیام ارسال شده برای پروفایل Aleksandr Nadvirnyak که به عنوان متخصص بلاک چین در این پروژه معرفی شده فرستاده شد. این پروفایل با وجود این که پیام ما را مشاهده کرد اما هیچ پاسخی به آن داده نشد.

نکته عجیب تر اما در پروفایل این شخص هیچ صحبت و نشانه ای از این پروژه وجود ندارد. هیچ اشاره ای به تخصص بلاک چین نشده است. درواقع نکته جالب اینجاست که عنوان شغلی او متخصص دیجیتال مارکتینگ اعلام شده است.

در سایر پروفایل ها هم همین مشکلات و نا هماهنگی ها به چشم می خورد.

عدم وجود هرگونه مشاور

هنگامی که یک پروژه بلاک چین قصد دارد با استفاده از ICO سرمایه جذب کند، باید حتما از وجود یک مشاور بهره ببرد. اهمیت این موضوع و وجود مشاور را در تمام پروژه های ICO معتبر می توان مشاهده کرد.

وظیفه این مشاور ها آن است که پروژه را در زمینه های مختلف مانند مالی، فنی، بازاریابی و موارد مشابه راهنمایی کنند و به رشد آن کمک کنند.

اما در این پروژه با مشاهده ی اطلاعات درج شده در سایت electronicenergycoin.com هیچ مشاوری برای ارز دیجیتال e2c معرفی نشده است.

مشاوران بلاک چین به طور معمول افراد شناخته شده و مشخصی هستند که سوابق کاری مرتبط با پروژه ها را دارند. به همین دلیل است که نمی توان یک پروفایل جعلی برای مشاور پروژه ساخت. احتمالا دلیل معرفی نشدن یک مشاور تقلبی برای این پروژه هم همین سختی در درست کردن یک مشاور جعلی است.

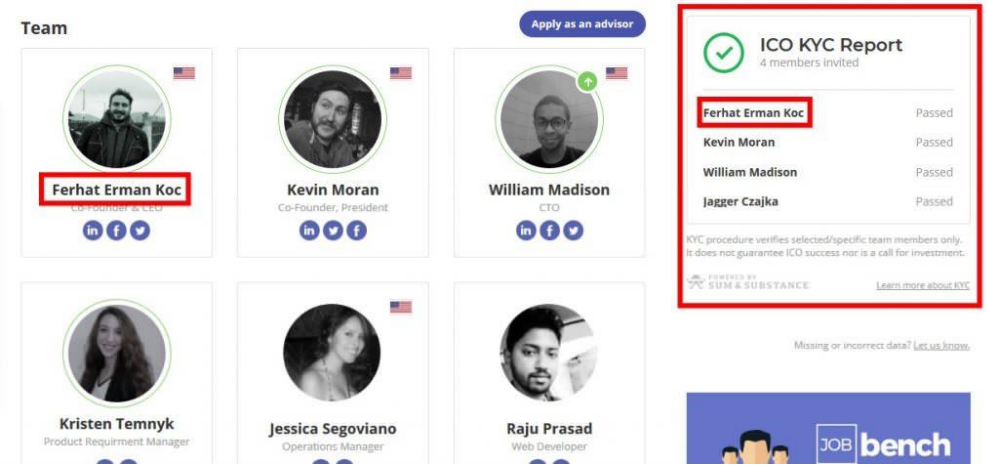
لیست نشدن پروژه در دایرکتوری ها و سایت های معتبر

دایرکتوری های زیادی مانند icobench.com وجود دارند که تمرکزشان بر روی کار ICOها است.

اگر یک ICO به اندازه کافی معتبر باشد، تقریبا می توان گفت حتما در این سایت های دایرکتوری لیست شده و نامشان در آن ها ثبت خواهد شد. اما برای این پروژه هیچ نامی پیدا نشد.

سایت icobench.com یک مزیت بسیار بزرگ دارد، این مزیت احراز هویت تیم اصلی پروژه است. با این قابلیت پروژه هایی که افراد واقعی و معتبر پشت آن ها هستند مشخص می شوند.

برای مثال در عکس زیر صفحه یک ICO را می توانید مشاهده کنید که در آن افراد در سایت هویتشان تایید شده است



حال اگر صرفا سایت icobench.com را در نظر نگیریم و باقی سایت ها را هم سرچ کنیم تنها در دو سایت به نام E2C برخورد می کنیم.

پروژه ارز دیجیتال e2cتنها در دو سایت icoholder.com و investfuture.ru لیست شده و غیر از این دو سایت در هیچ کجای دیگر نامی از این پروژه وجود ندارد.

باید این نکته را بدانید که تنها ICOهایی با تیم معتبر می توانند در این سایت ها لیست شوند.

وجود موارد مشکوک در سایت

هنگامی که به سایت معرفی شده برای پروژه ارز دیجیتال e2cوارد می شوید، در صورتی که به دنبال اطلاعات تماس و راه ارتباطی با اعضای این پروژه بگردید، هیچ چیزی پیدا نخواهید کرد. نه اطلاعات تماس و نه حتی یک آدرس بسیار ساده ی ایمیل!

نکته بعدی که در این سایت به چشم می خورد وجود نداشتن هرگونه لینک عضویت است. تنها لینک هایی که در این سایت وجود دارد لینک های مربوط به زیر مجموعه گیری است.

هنگامی که شما می خواهید به طور مستقیم به صفحه ی ثبت نام در این سایت وارد شوید تنها اتفاقی که می افتد این است که مجدد صفحه ی اصلی سایت برایتان به نمایش در می آید. درواقع هیچ صفحه ی ثبت نامی در این سایت وجود ندارد.

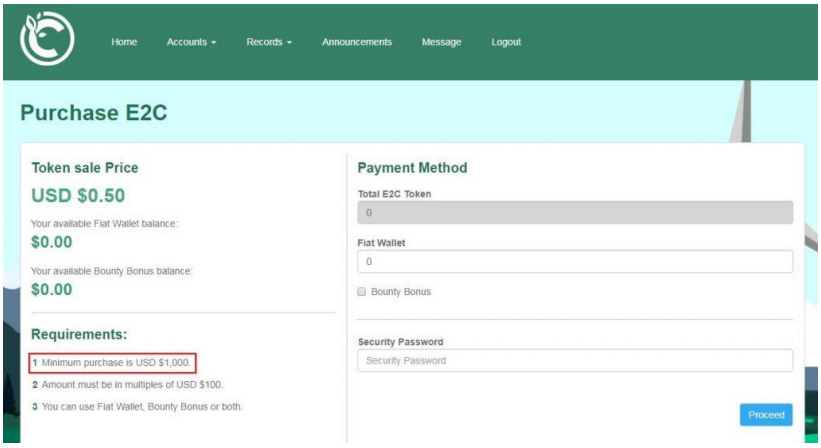
بررسی لینک زیر مجموعه گیری

همانطور که گفتیم، تنها لینک موجود در سایت که به نظر کار می کند لینک مربوط به زیر مجموعه گیری است. پس نتها چیزی که برای امتحان وجود دارد را امتحان کردیم.

ما با استفاده از یک لینک زیر مجموعه گیری در این پروژه ثبت نام کرده و در آن عضو شدیم تا ببینیم برای ما هم یک لینک زیر مجموعه گیری درست می شود یا خیر. هنگامی که در پنل کاربری به جست و جو پرداختیم به این نتیجه رسیدیم که هیچ هیک زیر مجموعه گیری برای ما وجود ندارد.

این موضوع نشان دهنده ی این است که تنها افراد محدودی می توانند لینک زیر مجموعه گیری داشته و افراد جدید را عضو کنند. در واقع این افراد، از اعضای اصلی گروه کلاهبرداری e2cهستند که با معرفی این پروژه به افراد نا آگاه سعی دارند عضو اضافه کنند.

نکته بعدی اما وجود یک محدودیت جالب است. حداقل میزان خرید توکن در این وب سایت ۱۰۰۰ دلار در نظر گرفته شده است. تقریبا می توان گفت هر فرد عاقلی باید با مشاهده ی این مبلغ نگران شود!



این مبلغ زمانی بسیار بیشتر به چشم می آید که بدانید بسیاری از پروژه های معروف و معتبر مبالغ حداقلی خود را حتی تا مبلغ ۲۰ دلار نیز پایین می آورند. یعنی شما می توانید تنها با ۲۰ دلار در یک پروژه معتبر و مطمئن یک مشخصات تمام افراد پشت آن مشخص و تایید شده است سرمایه گذاری کنید.

وجود نشانه هایی مبنی بر سابقه ی کلاهبرداری

اگر کمی در اینترنت به جست و جو بپردازید و منابعی برخورد می کنید که از کلاهبرداری تیم پشت پرده ی ارز دیجیتال e2cصحبت می کنند. نام این تیم پشت پرده creator academy است.

افراد موجود در این تیم قبلا چندین سابقه ی کلاهبرداری داشته اند. از جمله ی این سوابق می توان به کلابرداری پروژه های VGMCو Adrows و Unifunds و اخیرا World Wide Energy اشاره کرد. این تیم هم اکنون قصد دارد از طریق electronicenergycoin.com کلاهبرداری جدیدی را شروع کند.

در ارتباط با همین تیم کلاهبردار دو مطلب در سایت های «ایران هشدار» و «وزارت اطلاعات» منتشر شده است.

تصویر خبر مربوط به سایت وزارت اطلاعات را می توانید در زیر مشاهده کنید


وزارت اطلاعات جمهوری اسلامی ایران

سال حمایت از کالای ایرانی

نسخه قابل چاپ

اطلاعیه

دوشنبه ۱۳۹۷/۸/۱۴

برخورد با شبکه هرمی ورد وایند انرژی

سربازان گمنام امام زمان(عج) در راستای تأمین نظم و امنیت اقتصادی و جلوگیری از اخلال در نظام اقتصادی کشور، ضمن شناسایی و برخورد با یک شبکه هرمی به نام (ورد وایند انرژی) تعداد ۱۰ نفر از مسئولین، لیدرها و اعضای فعال این شبکه هرمی نوظهور را در استان های تهران، همدان و اصفهان دستگیر و تحویل مراجع قضایی نمودند.

این شبکه هرمی در پوشش دوره های آموزشی مؤسسه کریتور آکادمی (Creator Academy)، در گذشته با نام شرکت هایی همچون وی جی ام سی (VGMC)، ادروز (Adrows) و یونیفاندز (Unifunds) و اخیراً با نام ورد وایند انرژی (World Wide Energy)، مردم را فریفته و از این طریق توانسته میلیاردها تومان کلاهبرداری نماید.

شرکت مذکور با ادعای دروغین سرمایه‌گذاری در ارتقاء و پیشرفت انرژی سبز و سوخت های زیستی و غیرفسیلی، اقدام به جذب سرمایه افراد و انعقاد قرارداد صوری با آنها نموده و از همان سرمایه جمع شده مجدد به سرمایه گذاران سود پرداخت می نمود.

شایان ذکر است استفاده از ارزهای رمز نگار شده جهت امور غیرقانونی و پولشوئی، ترغیب و اغفال افراد از طریق برگزاری همایش ها، سمینارها و دوره های آموزشی در خارج از کشور، خروج ارز از کشور و اقدام به شبکه سازی هرمی، بخشی از فعالیت های غیرقانونی و مخرب این مجموعه کلاهبرداری و اخلال گر اقتصادی است.

با عنایت به شکل‌گیری مجدد شبکه های هرمی با ترفندهای جدید و کلاهبرداری آن ها و احتمال مال باخته شدن افراد، مقتضی است مردم شریف از هرگونه سرمایه گذاری در طرح هایی از این قبیل، خودداری و در صورت مشاهده هر گونه موارد مشکوک مراتب را به شماره ۱۱۳ منعکس نمایند.

روابط عمومی و اطلاع رسانی وزارت اطلاعات

کلیه حقوق این پایگاه متعلق به وزارت اطلاعات است و استفاده از مطالب آن با ذکر منبع بلامانع می باشد.

تصویر خبر مربوط به سایت ایران هشدار را می توانید در زیر مشاهده کنید.

ورد وایِد انرژی و جذب سرمایه به صورت هرمی

تاریخ:بیست و سوم بهمن 1396 ساعت 11:31 | کد : 28657

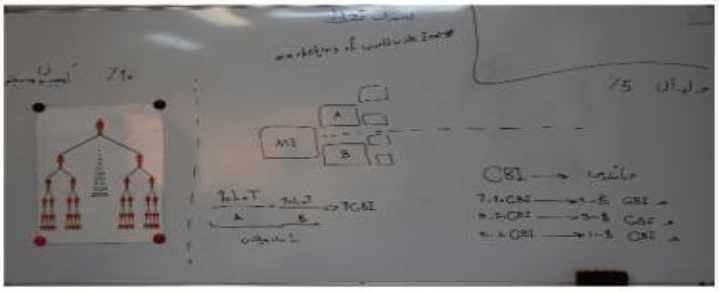
این شرکت ها با فریب و تقلب، از نام شرکت های مطرح خارجی استفاده و اقدام به جذب سرمایه از طریق فروش سهام شرکت های خارجی می نمایند که البته هم نام شرکت را به دروغ به یدک می کشند و هم اینکه در پشت پرده فعالیت این شرکت ها، هیچ سرمایه گذاری و فعالیت اقتصادی وجود ندارد

اختصاصی ایران هشدار - یکی از شیوه های جذب افراد در شرکت های هرمی، شیوه جذب سرمایه است. این شرکت ها با فریب و تقلب، از نام شرکت های مطرح خارجی استفاده و اقدام به جذب سرمایه از طریق فروش سهام شرکت های خارجی می نمایند که البته هم نام شرکت را به دروغ به یدک می کشند و هم اینکه در پشت پرده فعالیت این شرکت ها، هیچ سرمایه گذاری و فعالیت اقتصادی وجود ندارد و کار صرفا در فریب و کلاهبرداری خلاصه می شود.

مدتی است شرکتی به نام ورد وایِد انرژی (**world wide energy**) با ادعای سرمایه گذاری در راستای ارتقا و پیشرفت انرژی سبز و سوخت های زیستی و غیر فسیلی، اقدام به جذب سرمایه می نماید و با تقلب و نیرنگ، خود را شرکتی قانونی در خرید و فروش سهام در بورس معرفی می کند.

شرکت ادعا می کند که در معاملات فارکس و **cfd** فعالیت داشته و به سرمایه گذاری در این حوزه می پردازد. این شرکت در واقع در ادامه فعالیت شرکت های هرمی چون **unifounds** و **adrows** به فعالیت می پردازد و پس از اینکه این شرکت ها به دلیل کلاهبرداری از قشر بسیار زیادی از مردم، با عدم رغبت و گرایش به آنها کنار رفتند، ظهور پیدا کرد و در واقع می توان گفت ورد وایِد انرژی همان شرکت های هرمی قبلی با نامی جدید است که به دنبال کلاهبرداری از افراد نا آگاه می باشد.

قرارداد این شرکت با سرمایه گذاران 24 ماهه است و شرکت ادعا می کند سود اشخاص را به صورت روزانه محاسبه می نماید و در صفحه شخصی آنها نشان می دهد و برای هر 1000 دلار سرمایه گذاری، روزانه سه تا 4 دلار سود در نظر می گیرد. علاوه بر این شرکت با این وعده که با معرفی دو نفر عضو جدید و به ازای هر نفر 10 هزار دلار سرمایه گذاری، در هر شاخه زیر مجموعه، 1000 دلار پورسانت پرداخت می کند، به فریب افراد برای بدست آوردن سرمایه آنها می پردازد.



در سیستم این شرکت خرید سهام از طریق بیت کوین انجام می شود و تمام مبادلات از طریق این ارز مجازی صورت می گیرد. اما نکته حائز اهمیت اینکه شرکت ورد وایِد انرژی حتی نام دامنه خود را نیز به تقلب از شرکتی قانونی در آمریکا به آدرس **worldwideenergy.com** به سرقت برده و با تغییری جزئی در آن، نام دامنه خود را با آدرس تقلبی **world wide.energy** انتخاب کرده و از این طریق می خواهد خود را معتبر و قانونی جلوه دهد.

پلتفرم های wwe

در پلتفرم های طراحی شده در این شرکت، سه پلن برنزی، نقره ای، طلایی، پلاتینیو و **VIP** در نظر گرفته شده که ادعا می شود در هر یک از این طرح ها، پس از مدت زمان تعیین شده، که بین 24 تا 36 ماه است، بین 200 تا 650 درصد سود پرداخت می شود اما واضح است که در پس این سرمایه گذاری، فقط فریب و خسران و زیان برای سرمایه گذار وجود دارد و تحت هیچ شرایطی چنین سودهای نجومی پرداخت نخواهد شد و این شرکت نیز مانند یونی فاندز و ادروز پس از مدتی منحل و در قالب نامی جدید، به فریب افراد جدیدی می پردازد.

تاپیک ارز دیجیتال e2c

اگر تاپیک مربوط به ارز دیجیتال e2cرا در فروم Bitcointalk را بررسی کنیم هم به نکات جالب و نامعتبری برخورد می کنیم.

این تاپیک توسط یک حساب کاربری با نام e2cایجاد شده است. این حساب کاربری به صورت self-moderatedدرست شده است. در این تاپیک هم افردی به ارتباط بین کریتور آکادمی و ارز دیجیتال e2c اشاره کرده اند.

منطور از تاپیک self-moderated یعنی این که شخص سازنده و مدیر صفحه کنترل کامل بر روی تمام پیام های ارسالی دارد و می تواند به راحتی پیام ها را حذف کند. به همین دلیل به احتمال زیاد پست های زیادی در این صفحه حذف شده اند تا از دید سایرین پنهان شوند.

XxKryptX
Newbie
Activity: 12
Merit: 0
Trust: 0: -0 / +0
Ignore

Re: [ICO][E2C] - ELECTRONIC ENERGY COIN ✅ NEW TECHNOLOGY ✅
November 19, 2018, 12:11:09 AM
quote #628

Quote from: wz3r0 on November 18, 2018, 01:39:21 PM
Quote from: XxKryptX on November 18, 2018, 06:06:02 AM
Quote from: BillieGin on November 17, 2018, 08:49:45 PM
Quote from: Diamond on November 17, 2018, 08:47:47 PM
I think this project would be cost-effective in eastern Europe, where green energy was not developed, and this market is not yet occupied by large corporations.
I don't agree with you, due to the fact that the countries of Eastern Europe are large suppliers of electricity to Western Europe.

Wake up! it is not about energy or E2C or anything else. It's a scam, a big scam. It is run by a team called creator academy in Malaysia. since 2015 creator academy is actively scamming people by selling advertising campaigns or shares of companies that do not really exist. E2C is their latest scam. It is not about energy or cost efficiency, WAKE up....it's just something that seems interesting but in reality is either impossible or costs too much to be implemented. Anyhow, consider this: Everything creator academy has done turned into such a big scam, it started in UAE, then spread into Malaysia, Turkey and elsewhere.
Go and ask about creator academy from Malaysian Authorities and you will be amazed. So far all they have done was violations of several different laws and regulations in several countries.
just ask the Malaysian Authorities at www.sc.com.my

Where did u find such information?
Do u have any facts or is it only words ?

Since 2015, a team calling themselves creator academy started running similar stuff, they call it projects! their first project was called Adrows which was selling online advertisements and after a while it turned out to be a BIG scam in UAE, so this team fled from UAE. Their next project was called Unifunds which they started selling shares of a company called Unifunds. After a while it turned out to a another SCAM! many complaints were filed against them in Kuala Lumpur and they had to settle some of it. what I say is from experience and not just words! I know the people who lost their money in creator academy scams! you can ask them if you can find them! or you can ask Malaysian Authorities at www.sc.com.my
creator academy which is a team of Iranian scammers claim to have been registered and claims to have license for what they do. After you contact Malaysian Authorities you will see not only they do not have any license but also the Malaysian Authorities will ask you to provide them with info. about any activity of creator academy, simply because everything they do is not legal. They design websites and make people believe that the website belongs to a company that is among the best in the world! and make people invest in that company's projects through a referral program which is a pyramid scheme. if you invest and bring more investors to the project then the reward is a percentage! after a while people found out the websites are designed by creator academy and there was NO company at all, or the company existed but only as a name and a website with absolutely no documentation. The very obvious reason is that creator academy claimed Unifunds was an international company and it was among the best in the world and was to be listed soon! Unifunds never made it to any stock market. It is now on OTC Market! and because of lack of info. and lack of documentation, OTC gave it a very serious warning! Unifunds never ever existed as creator academy claimed! it was all but lies after lies.
What you read is not just words! it is fact and it comes from the people who lost their money in creator academy scams! All they do is scam! they are fugitives! investigate them in Malaysia! you will see for yourself.

Report to moderator

در پست مورد نظر ما ادعا شده است که تیم پشت پرده ی ارز دیجیتال e2c، یک تیم ایرانی است که خود را با نام کریتور آکادمی معروف کرده اند.

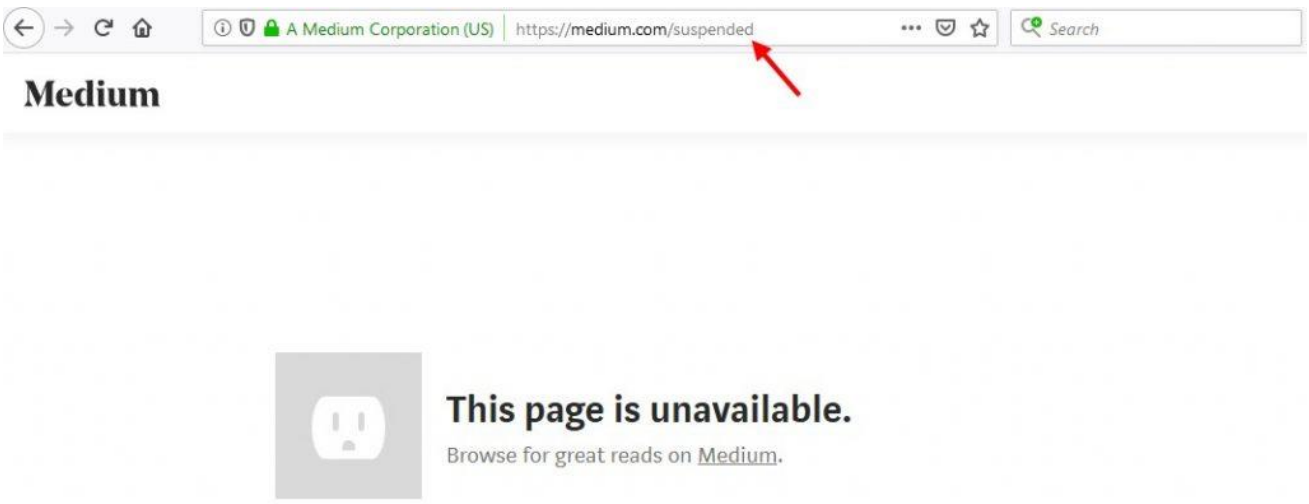
با توجه به بازاریابی این پروژه و اخبار منتشر شده این طور به نظر می آید که هدف از کلاهبرداری e2c کاربران ایرانی باشند.

مسدود شدن حساب ها در سایت medium.com

این سایت به تمام افراد و کسب و کار ها کمک می کند تا به صورت کاملا رایگان برای خود و کسب و کارشان یک بلاگ ایجاد کنند. در واقع این سایت یک پلتفرم انتشار محتوا است که افراد می توانند از آن برای انتشار اخبار و پیام های خود استفاده کنند.

ارز دیجیتال e2cدر این وبسایت یک حساب کاربری ساخته است. این حساب توسط یک کاربر با نام e2coinساخته شده است.

هنگامی که در شبکه های اجتماعی مربوط به ارز دیجیتال e2cبر روی لینک های داده شده به سایت مدیوم کلیک کنید، به صفحه ی Suspended وارد می شوید. این صفحه نشان می دهد که حساب این اشخاص در این سایت مسدود شده است.



لینک صفحه را در این لینک می توانید مشاهده کنید.

به احتمال زیاد دلیل مسدود شدن این صفحه ارسال گزارش کاربران از کلاهبرداری e2cاست.

عدم وجود هیچ ویدیویی از این پروژه

ارز دیجیتال e2cدارای یک کانال یوتیوب است. نکته جالب اینجاست که حتی یک ویدیو هم در این صفحه وجود ندارد. به طور معمول در این گونه صفحه ها باید ویدئو هایی از مصاحبه افراد پروژه و یا معرفی پروژه وجود داشته باشد.

از ارز دیجیتال e2cتنها یک ویدئو تاکنون منتشر شده است که در آن هم چهره هیچ کدام از افراد مربوط به این پروژه نشان داده نمی شود.

البته در این بین وجود دارند کاربرانی که به چند تصویر از یک کنفرانس نا معلوم و با حضور چهره ها و افراد ناشناس استناد کرده و این تصاویر گنگ را نشانه ی معتبر بودن این پروژه می دانند. از این کنفرانس های ناشناس فقط چند تصویر بی کیفیت منتشر شده که تصویر هیچ کس در آن مشخص نیست و حتی هیچ ویدئویی هم از این کنفرانس وجود ندارد.

البته در سایت مدیوم یک پست قرار داشت که تصویر چند نفر را در ارتباط با پروژه ارز دیجیتال e2cنشان می داد اما این تصویر هم بعد از چند روز به کلی از خروجی این وبسایت حذف شد.

در هر حال چیزی که مشخص است، چه این عکس واقعی بوده باشد و یا خیر، باز هم دلیلی بر کلاهبردار نبودن پروژه ی ارز دیجیتال e2cنیست.

وجود نداشتن یک محل آزاد برای تبادل نظر درباره ی پروژه

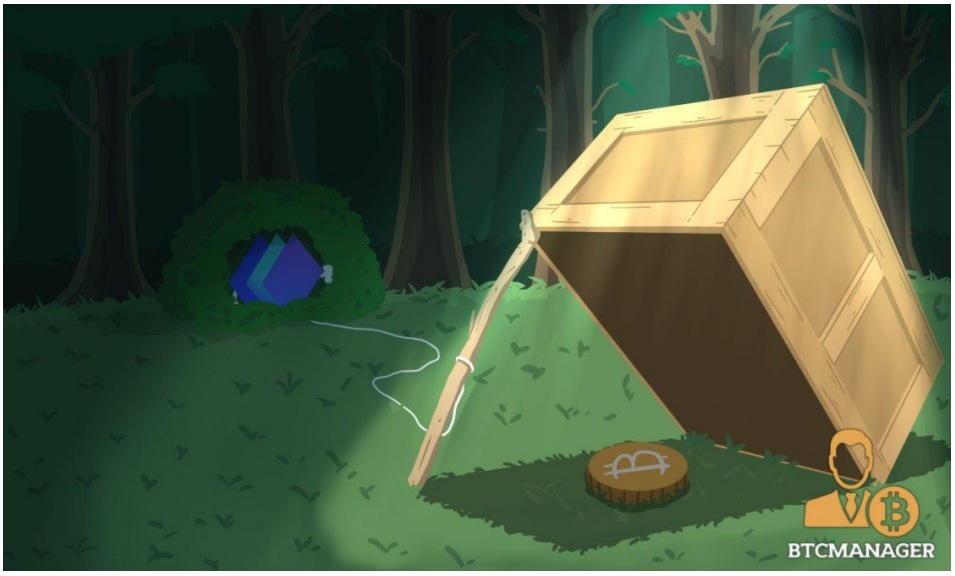
می توان گفت که تمام پروژه های ICOدر شبکه های اجتماعی و پیام رسان ها مانند تلگرام، یک گروه رسمی دارند که در آن به پرسش های کاربران پاسخ می دهند. در این گروه ها همچنین گفت و گوی کاملا آزاد کاربران هم امکان پذیر است.

اما این گروه ها در مورد ارز دیجیتال e2cاصلا وجود خارجی ندارند.

هیچ لینکی از سوی این گروه برای پرسش و پاسخ و گفت و گوی کاربران درباره ی این تیم اعلام نشده است و با سرچ در فضای اینترنت هم به هیچ نتیجه ای نخواهید رسید.

تنها لینک رسمی اعلام شده از سوی تیم ارز دیجیتال e2c، تاپیک این پروژه در سایت بیت کوین تاک است که همان طور که اشاره کردیم، ادمین این صفحه کاملا اختیار پاک کردن پیام ها را دارد.

در این تاپیک افرادی وجود دارند که در ازای دریافت پاداش و توکن های رایگان، آمده و بسیار پر شور و حرارت از این ارز دیجیتال تعریف و حمایت می کنند.



نتیجه گیری پایانی

تمام مواردی که برای شما معرفی و بررسی کردیم مواردی بوده است که باید در ارتباط با یک پروژه وجود داشته باشد.

قطعا هر فرد عاقل و هرکسی که به سرمایه خود اهمیت دهد با بررسی این موارد به این نتیجه می رسد که بهتر است کاری با این پروژه نداشته باشد. اگر این موارد را با پروژه های معتبر مقایسه کنید کاملا به ناقص بودن و نا معتبر بودن ارز دیجیتال e2cپی خواهید برد.

اگر می خواهید سرمایه گذاری انجام دهید بهتر است که پول خود را بر روی پروژه های معتبر سرمایه گذاری کنید.

همچنین برای سرمایه گذاری از مشاوره گرفتن غافل نشوید. مشاوران ارز های دیجیتال در این زمینه تخصص دارند و بهتر از هر کس دیگری می توانند شما را راهنمایی کنند.

مشاور ارز دیجیتال کیست و چگونه میتوان از مشاوره نتایج مثبت کسب کرد

سه کلاهبرداری بزرگ

در این قسمت از مقاله می خواهیم شما را با سه پروژه کلاهبرداری بزرگ و البته معروف در دنیای ارز های دیجیتال آشنا کنیم. در این بخش پروژه های کلاهبرداری بیت کانکت، وان کوین و بیت پتیت را مورد بررسی قرار می دهیم.

افزایش قیمت و ارزش ارز های دیجیتال مانند بیت کوین قطعا پای کلاهبردار ها را به این صنعت باز می کند. این پروژه های کلاهبرداری که در ادامه آن ها را برای شما توضیح خواهیم اتفاق افتاده اند و سرمایه های افراد را بر باد داده اند. اما هنوز هم می توان از این کلاهبرداری ها درس گرفت و حواس خود را جمع کرد.

این درس ها واقعا ارزشمند هستند، زیرا سرمایه های ما یک شبه بدست نیامده اند که بتوانیم به راحتی آن ها را یک شبه در اختیار کلاهبردار ها قرار دهیم و مشکلی هم برایمان پیش نیاید. سرمایه های هر کس با زحمت و سختی بدست آمده اند و اگر قصد دارید آن ها را در جایی و با نیت افزایش سرمایه و سود کردن استفاده کنید، باید بسیار با دقت عمل کنید.

کلاهبرداری باعث نقض اخلاقیات می شود

کلاهبرداری و سوء استفاده کردن از اعتماد افراد اصلا اقدام درستی نیست. این افراد برای سرمایه گذاری به صداقت و درستی شما اعتماد کرده اند و در صورت هرگونه سوء استفاده از آن، این افراد دیگر به هیچ کس در این گونه موارد اعتماد نخواهند کرد.

البته نمی توان این حقیقت را انکار کرد که کلاهبرداری های این چنینی هم در نوع خود هنر به حساب می آید. در این زمینه افرادی باهوش و با علم بالا، از این اطلاعات خود در جهت تقلب استفاده می کنند. همه ی این ماجرا ها اما برای افرادی که می خواهند به این صنعت وارد شوند درس ها و قوانین بسیار خوبی را آموزش می دهد.

این گونه کلاهبرداری ها دیر یا زود مشخص شده و پس از آن تکنیک های استفاده شده در سرقت مشخص می شوند. ما می توانیم با بررسی این موارد اطلاعات خود را بالا برده و همچنین با آگاه کردن سایر افراد از این موارد می توانیم جلوی گول خوردن اطرافیانمان را بگیریم.

ترفند پانزی

در ادامه ی مقاله با نام «پانزی» برخورد خواهید کرد. چارلز پانزی را می توان بنیان گذار این شیوه معرفی کرد. این نوع کلاهبرداری آن قدر معروف و پر استفاده است که در صنف کلاهبردار ها، این روش را «ترفند پانزی» نامیده اند.

اگر بخواهیم خیلی کوتاه این ترفند را به شما توضیح دهیم، ترفند پانزی یعنی دادن وعده ی سود های نا متعارف که از سود های عادی بسیار بالاتر هستند. در این ترفند، از سرمایه افراد تازه وارد استفاده شده و با آن سود افراد قدیمی تر پرداخت می شود. این کار آن قدر ادامه پیدا می کند و بزرگ می شود تا آن که دیگر امکان انجام این کار ممکن نیست.

Lending Amount	Interest (Accrued Daily)	Capital Back
$100 - $1000	Volatility Software Interest (up to 40 % Per Month)	After 299 Days
$1010 - $5000	Volatility Software Interest + 0.10% Daily (up to 40 % Per Month)	After 239 Days
$5010 - $10000	Volatility Software Interest + 0.20% Daily (up to 40 % Per Month)	After 179 Days
$10010 - $100000	Volatility Software Interest + 0.25% Daily (up to 40 % Per Month)	After 120 Days

در نهایت فرد پشت پرده ی این ترفند، با تمام پول های باقی مانده ناپدید خواهد شد. در این ترفند هرچه سود وعده داده شده بیشتر باشد، فروپاشی هم سرعت بیشتری پیدا خواهد کرد.

کلاهبرداری پروژه بیت کانکت

پروژه بیت کانکت دست به کاری زد که در زمینه ی کلاهبرداری واقعا نامش را ماندگار کرد. این پروژه درست در جلوی چشم تمام مردم دست به یک کلاهبرداری چند میلبارد دلاری زد.

اگر برایتان این سوال پیش آمده است که مگر می شود چند میلیارد دلار از جلوی چشمان کاربران به سرقت برود باید در جواب بگوییم بله! بیت کانکت این کار را با موفقیت هر چه تمام تر انجام داده است.

البته این کار یک شبه انجام نشد. فرایند تبدیل بیت کانکت به یک ارز دیجیتال حدود یک سال زمان برد. البته موسسان و نگهدارندگان این ارز به دلیل تبدیل شدن آن به یک سکه و پلتفرم سرمایه گذاری خواهان آن نبوده اند. بیت کانکت تقریبا بلافاصله بعد از اینکه به سکه تبدیل شد موفق به کسب چند سود دهی بسیار خوب دست پیدا کند.

بازگشت دو رقمی سرمایه آن هم به صورت ماهیانه و صد در صد تضمینی! این همان سود و وعده ی فضایی بود که پیشتر درباره ی آن به شما گفتیم.

وعده هایی فضایی و امکان پذیر؟!

در واقع باید این نکته را بدانید که وعده های داده شده هر چقدر هم که فضایی و عجیب باشند اما باز هم به مدت کوتاهی امکان انجام شدن را دارند.

قیمت های ارزی قطعا افزایش خواهند داشت اما یک فاجعه در انتظار بیت کانکت است.

ممکن است در این بین این شرکت یک ربات معاملاتی اختراع کرده باشد که می تواند بازار ارز را پیش بینی کند. این صحبت ها مربوط به سال ۲۰۱۷ است:

نگران نباشید، نرم افزار اختصاصی و بدون هرگونه ریسک ما را دانلود کرده و به تماشای جادوی آن بنشینید.

بیت کانکت به سرمایه گذاران یک وعده ی بسیار خوب داد. سرمایه گذاری ۱۰.۰۰۰ دلاری، ۲۵ درصد بازگشت سرمایه طی یک دوره ی چهار ماهه، همراه با سود دهی و به همراه ۹۰۰۰ دلار اضافه! این پیشنهاد واقعا شگفت انگیز است!

برنامه ی زیر مجموعه گیری

برنامه ی زیر مجموعه گیری یا همان referral programیک نقطه اتکا کلاسیک برای این شرکت ها است. این پیشنهادات شگفت انگیز مطرح شده در سالیان بسیار دور توسط پانزی انجام می شد.

باید بدانید که این شرکت ها می توانند با عضو گیری و جذب سرمایه های جدید، حداقل تا مدتی پول و سود سرمایه گذاران قدیمی را پرداخت کنند.

درست است که در آن سال و با توجه به شور و اشتیاقی که در بازار ارز های دیجیتال وجود داشت بیت کانکت توانست مدتی خود را زنده نگه دارد. اما هیچ چیز نمی تواند این حقیقت را انکار کند که این شرکت به همراه مشتریانش یک طوفان بسیار سهمگین را تجربه کردند و در این میان هیچ کس به غیر از سرمایه گذاران ضرر نکرد.

کلاهبرداری پروژه وان کوین

وان کوین هم یکی دیگر از شرکت های کلاهبردار است. کلاهبرداری این شرکت حتی از پروژه ی بیت کانکت هم واضح تر است. اما به نظر می آید همیشه پیدا می شوند افرادی که با دلایل پوچی که برای خودشان درست می کنند در این شرکت ها سرمایه گذاری می کنند.

این افراد این باور را دارند که فعالیت این گونه سایت ها کاملا بر پایه ی قانون است. البته اگر این افراد نباشند کار و کاسبی کلاهبردار ها هم کساد می شود!

دو منطقه دبی و بیلیز شاید از نظر جغرافیایی و ویژگی های انسانی با یکدیگر تفاوت هایی داشته باشند. اما در این دو منطقه افراد تمایل دارند با پانزی در ارتباط باشند و با آن کار کنند.

نتیجه ی این همکاری به وجود آمدن وان کوین بود. این شرکت برای بسیاری از سرمایه گذارانش هزینه های سنگینی را به وجود آورد.

بسته های سرمایه گذاری

وان کوین در پذیرش سرمایه تقریبا محدودیتی نداشت. افراد می توانستند با مبالغ اندک مانند چند دلار تا ده ها هزار دلار در این برنامه شرکت کرده و توکن تهیه کنند. اما خود این بسته های ارائه شده به نوعی کلاهبرداری بودند.

این شرکت این گونه ادعا می کرد که خدماتی که ارائه می دهد ارزشمند از فروش ارز است اما واقعا به این صورت نبود.

وان کوین به مدت کوتاهی شروع به مبادله یورو در بازار های ارزی خصوصی کرد. در این بازار بسته های خریداری شده مقدار دسترسی به کوین ها را تعیین می کرد. وان کوین بازار کوین های خودش را محدود نگه داشت و با پایین نگه داشتن عرضه باعث شد ارزش سکه هایش در بازار زیاد شود.

تعطیلی های ناگهانی

این شرکت فاصله های زمانی تصادفی خودش را به بهانه ی تعمیرات تعطیل کرد. اما اتفاقی که در این میان می افتاد این بود که پس از بازگشایی، برخی و سفارش ها و مبادلات کاملا ناپدید شده بود.

این اتفاق ها باعث شد برخی از سرمایه گذاران و مدیران اولیه از شرکت خارج شوند. البته ناگفته نماند که آن ها سود فراوانی بدست آوردند.

دولت ها در تمام نقاط جهان وان کوین را تحت نظر داشتند و آن را بررسی می کردند. این گونه کلاهبرداری ها تبعات زیادی برای ارز های دیجیتال داشته و دارد. دولت ها از کلاهبرداری این گونه شرکت ها استفاده کرده و از آن ها به جهت قانون گذاری در مورد ارز های دیجیتال استفاده می کنند.

در واقع این گونه کلاهبرداری ها به تمام دولت ها این اختیار و دلیل را می دهد که محدودیت های بیشتری را در مورد ارز های دیجیتال در نظر بگیرند. از آن جا که ارز های دیجیتال را می توان تهدیدی برای سیستم بانک داری قدیمی دانست، دولت ها از این کلاهبرداری ها نهایت استفاده را می کنند.

کلاهبرداری پروژه بیت پتیت

bitpètite

در بین این سه پروژه که به شما معرفی کردیم. پروژه بیت پتیت تقریبا از همه جدید تر است. این پروژه کاملا ناگهانی به همراه پول های نقد سرمایه گذاران محو شد و هیچ اثری هم از آن ها باقی نماند.

این شرکت این گونه ادعا کرده بود که می تواند بازگشت سه رقمی سرمایه را تضمین کند. البته این ادعای «سه رقمی» به حقیقت پیوست، اما نه دقیقا آن طور که وعده داده شده بود. این شرکت سود سه رقمی نکرد، بلکه ضرری ۱۴۷ درصدی کرد. البته این شرکت با وجود این مقدار ضرر، هنوز هم با وعده دادن سود ۱۵۰ درصدی سعی در جمع آوری سرمایه داشت.

البته در نهایت این کار ها باعث شد پیگیری قضایی و قانونی در مورد آن صورت بگیرد.

وب سایت این شرکت برای مدت زمان کوتاهی فعال شده و کار می کرد اما در مدت زمان کوتاهی غیر فعال شد. از کار افتادن و تعطیل شدن این شرکت برای سرمایه گذارانش بسیار ناراحت کننده بود زیرا تمام صفحات مربوط به این شرکت در شبکه های اجتماعی نیز به کلی پاک شده و از بین رفتنه اند.

بیت پتیت دروغ گفت، تظاهر کرد و اعتماد افراد را هدف قرار داد. هیچ کدام از وعده های آنان قابلیت عملی شدن در دنیای واقعی نداشت. در نهایت هم نتیجه ی کار همان شد که باید می شد.

کلاهبرداری با استفاده از ارز های دیجیتال

افزایش قیمت ارز های دیجیتال در دو سال گذشته باعث شده توجه بسیاری از افراد به آن ها جلب شود. در میان این ارز ها اما، افزایش قیمت بیت کوین بیشتر از سایر ارز ها بیشتر به چشم می آید.

تقریبا هیچ روزی نیست که خبر مهمی درباره ی این ارز های منتشر نشود. رادیو، تلویزیون، اینترنت و شبکه های اجتماعی پر شده است از اخبار دنیای کریپتو و هر روز بر حجم این خبر ها افروزده می شود.

تمام این خبرسازی ها و جلب توجه ها باعث شده است تا کلاهبردار ها هم از این فرصت استفاده کرده و به دنیای ارز های دیجیتال وارد شوند.

طریقه به سرقت بردن بیت کوین های شما

در این قسمت از مقاله می خواهیم سه روش بسیار رایج در زمینه ی کلاهبرداری و سرقت ارز های دیجیتال را به شما معرفی کنیم، مخصوصا روش هایی را که برای سرقت بیت کوین استفاده می شود. بخش آخر مقاله را از دست ندهید.

معرفی ساده ترین نوع کلاهبرداری در ارز های دیجیتال

ساده ترین نوع کلاهبرداری را می توان روش cryptophishing aka معرفی کرد. این روش مربوط به ایمیل های تقلبی و اسپم است. این روش یکی از قدیمی ترین روش ها است و خیلی سال است که وجود دارد.

چنین ایمیل هایی در نگاه اول این طور به نظر می آیند که از طرف شرکت های معتبر و ارائه دهنده ی خدمات ارسال شده اند. در زمینه ی ارز های دیجیتال، این ایمیل ها معمولا به صورتی ارسال می شوند که القا کننده ی ارسال از سوی صرافی ها و کیف پول ها و موارد مشابه هستند.

البته این ایمیل ها آنقدر که فکر می کنید هم ساده و مشخص نیستند. در حال حاضر این ایمیل ها هم پیشرفت کرده اند و دیگر به سادگی قابل تشخیص نیستند.

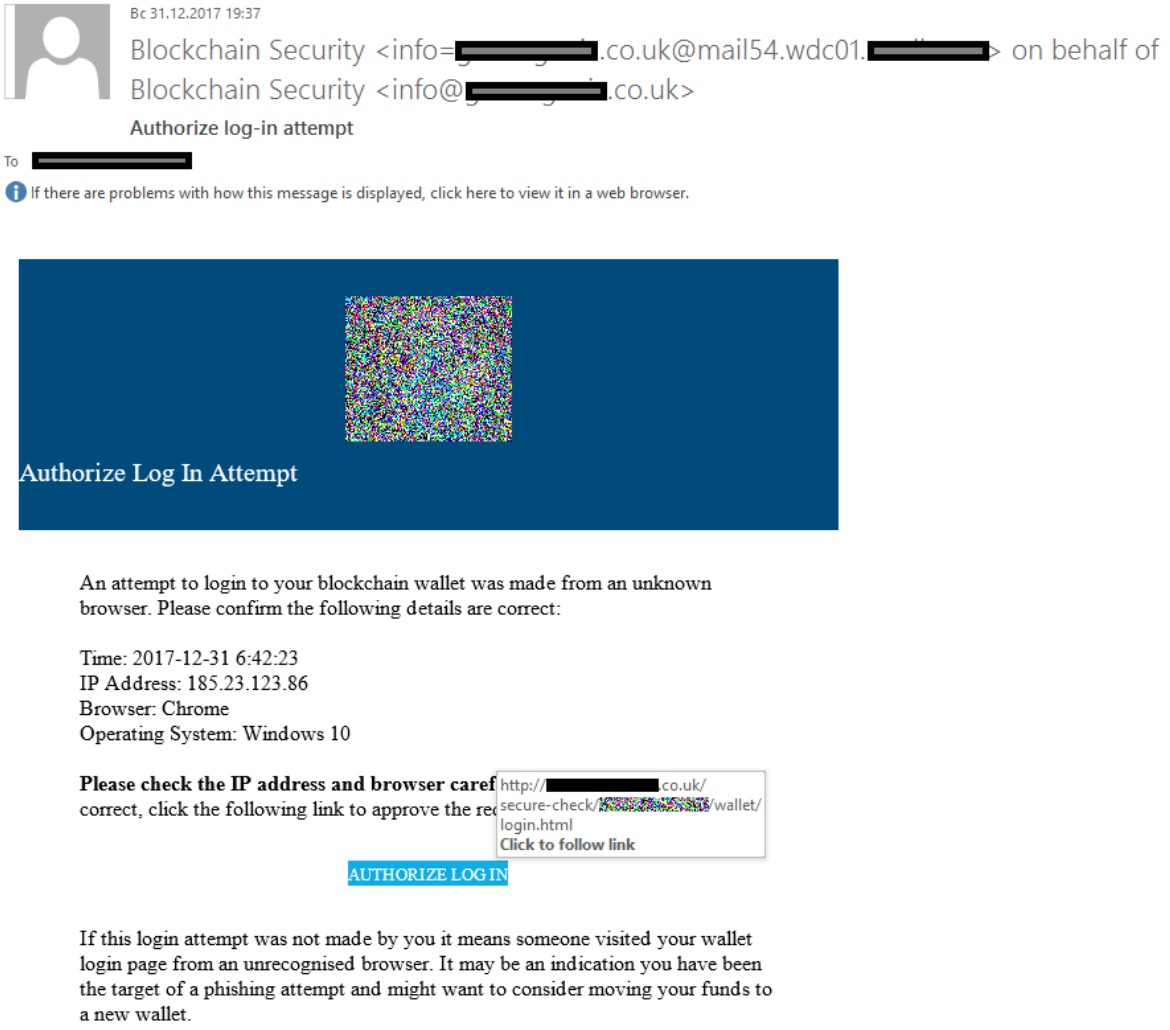
اخطار ورود غیر مجاز

برای مثال ممکن است ایمیلی تحت عنوان زیر برای شما ارسال شود:

«افرادی قصد داشته اند از طریق آدرس xoxو توسط مرورگر xoxوارد حساب کاربری شما شوند»

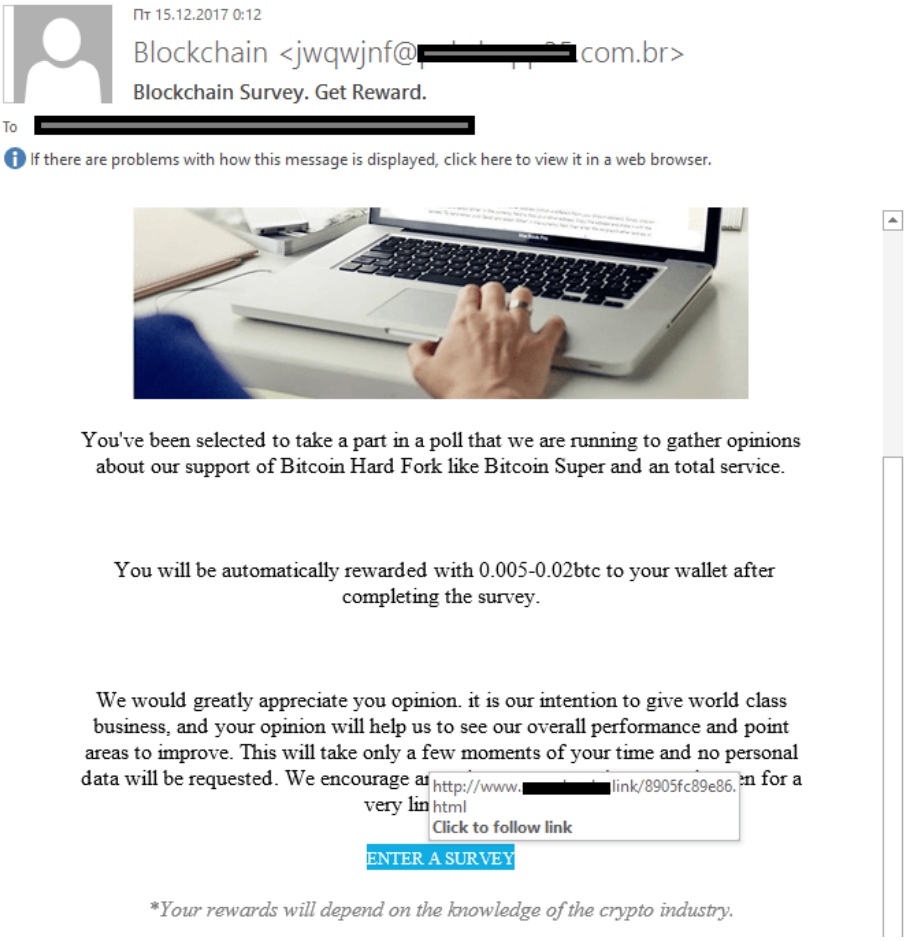
در این نوع ایمیل ها از شما خواسته می شود تا بر روی یک لینک که برای شما فرستاده شده کلیک کنید تا حساب کاربری شما از نظر امنیتی بررسی شود.

این پیام ها حتی ممکن است در وب سایت کیف پول شما دریافت شود. متاسفانه هیچ اعلانی نیست که شما را مطلع کرده و به شما هشدار دهد.



ارسال دعوتنامه

در نوع دیگری از این ایمیل ها ممکن است برای شما ایمیلی مبنی در دعوتنامه شرکت در یک پیش فروش و یا هر موضوع دیگری مربوط به ارز های دیجیتال باشد. در این نوع ایمیل ها علاوه بر لینکی که برای کلیک و ثبت نام به شما داده می شود، به شما دعوه یک جایزه قابل قبول هم داده می شود.

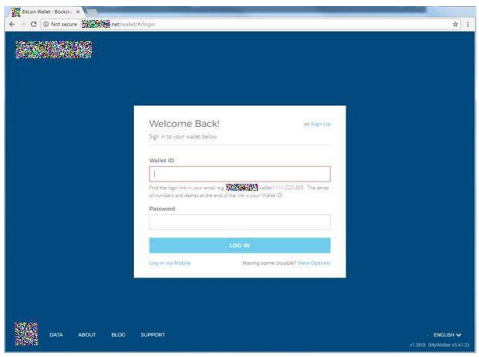


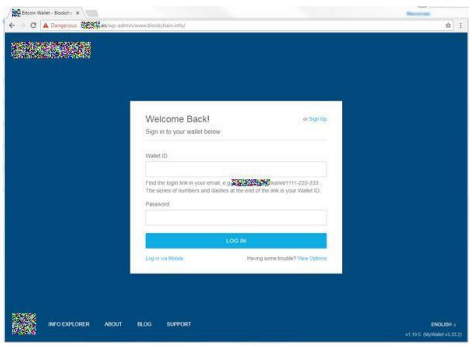
مثلا وعده جایزه ۰.۰۰۵ بیت کوین در صورت شرکت و ثبت نام را می دهند. می توانید این گونه پیام را در تصویر زیر مشاهده کنید.

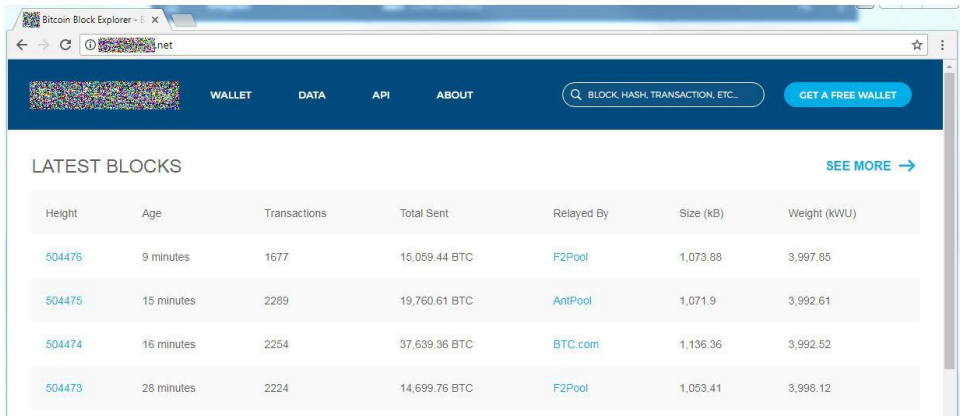
نتیجه همیشه یکسان است

نتیجه ی ارسال این گونه ایمیل ها همیشه مشخص است. قربانی به یک وب سایت شبیه سازی شده و جعلی وارد می شود. سپس از او خواسته می شود به حساب کیف پول خود وارد شود. پس از وارد کردن مشخصات، سارقین آن ها را در وب سایت اصلی وارد کرده و تمام ارز های موجود را به سرقت می برند.

متاسفانه در این میان طراحی و ظاهر وب سایت های کیف پول بیت کوین آنقدر ساده هستند که پیاده سازی و شبیه سازی آن ها کار خیلی پیچیده ای نیست و برای اکثر کاربران جعلی بودن سایت قابل تشخیص نیست.







باید بدانید که در این روش سارقین تمامی موجودی را سرقت می کنند و یک سنت هم برای کسی باقی نمی گذارند. آن ها همیشه ساده ترین و مستقیم ترین راه ها را برای دسترسی به حساب ها انتخاب می کنند. باید همیشه دقت کنید و به ایمیل های مشکوک توجه نکنید.

کلاهبرداری های نوین و مبتکرانه

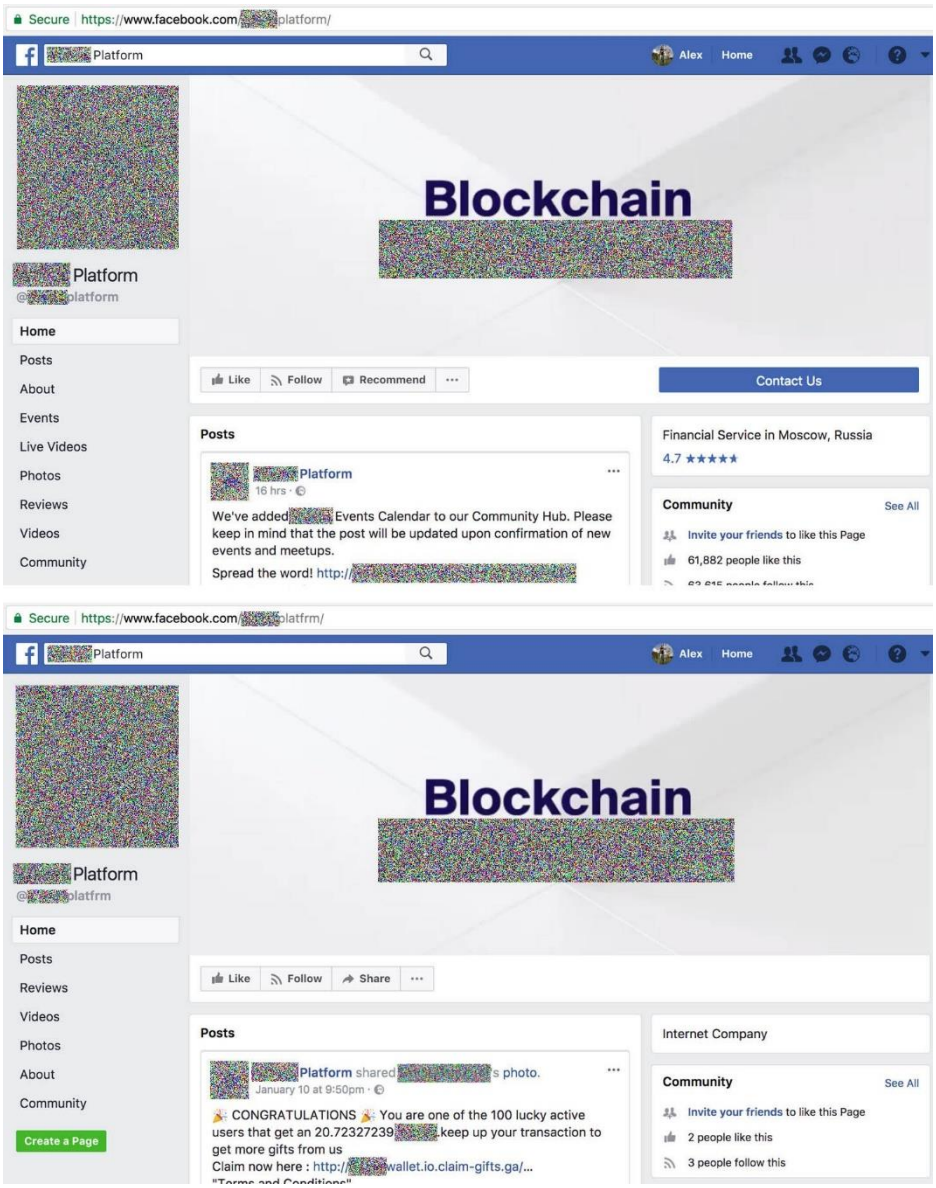
به تازگی یک روش پیچیده برای کلاهبرداری کشف شده است که در آن از برخی ویژگی های جالب فیسبوک استفاده شده است.

این کلاهبرداری تقریبا جدید و پیچیده را در سه مرحله به شما توضیح می دهیم.

مرحله اول)

کلاهبرداران در ابتدا یک انجمن رمز ارز را هدف قرار می دهند. سپس اقدام به درست کردن یک صفحه ی فیسبوک با نام و طراحی مشابه انجمن اصلی درست می کنند. برای این صفحه ی تقلبی یک آدرس مانند صفحه اصلی انتخاب می کنند. تفاوت آدرس صفحه اصلی و تقلبی تنها در یک حرف و به صورتی است که در نگاه اول اصلا متوجه نمی شوید.

تشخیص دادن این آدرس ها و صفحات از یکدیگر کار چندان ساده ای نیست. شما در فیسبوک می توانید هر اسمی برای خودتان و یا شرکتتان انتخاب کنید و این اسم ها خیلی بیشتر از آدرس ها به چشم می آیند.



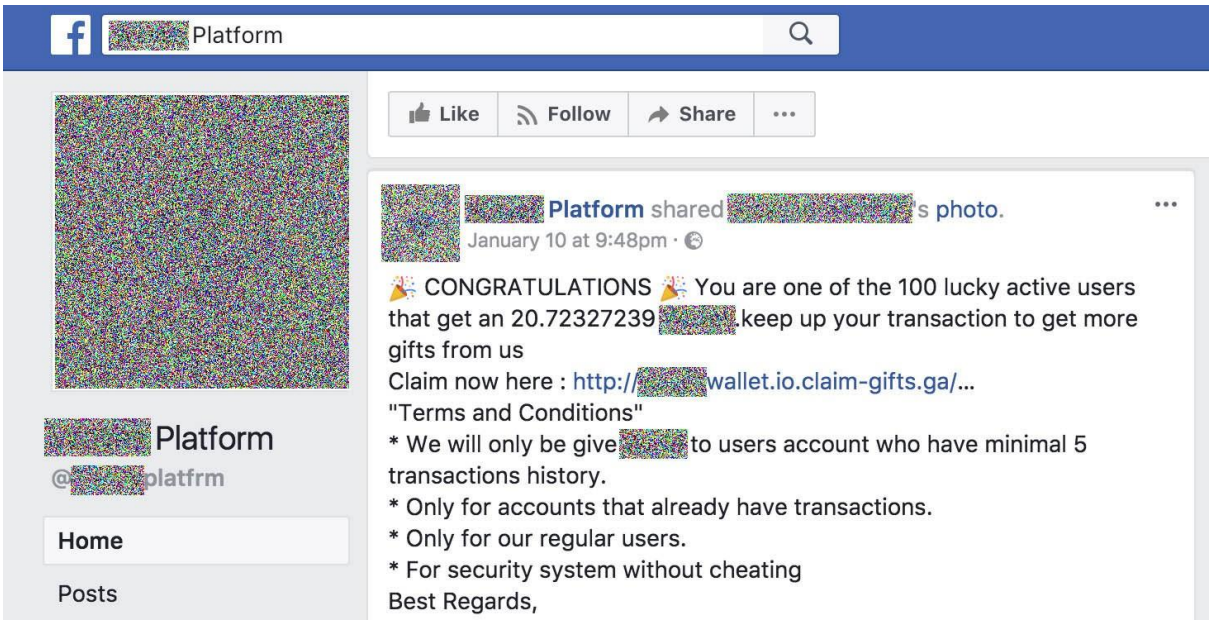
مرحله دوم)

کلاهبرداران در مرحله ی بعدی شروع به ارسال پیام های فریبنده برای کاربران مورد نظر خود می کنند. البته در این روش کاملا حرفه ای عمل می کنند! کلاهبردار ها می دانند که ارسال پیام شخصی مناسب این کار نیست. زیرا کدام شرکت و انجمن است که برای کاربر خود پیام شخصی ارسال کند!

آن ها یک ابتکار به خرج داده اند! از تصویر پروفایل سوژه مورد نظرشان استفاده می کنند. آن ها عکس مشترک مورد نظر را در صفحه جعلی خودشان به اشتراک می گذارند و سپس هدف را بر روی عکس تگ کرده تا آن ها به طرف خود بکشند.

نکته ای که در این جا وجود دارد این است که عکس پروفایل را نمی توان مخفی کرد و همه ی افراد قادر به دسترسی به آن هستند و می توانند به راحتی آن را به اشتراک بگذارند. به همین دلیلی است که این ترفند را می توان برای همه ی افراد استفاده کرد.

برای این که تا حدودی از این ترفند دور بمانید فقط یک کار می توان انجام داد. به صفحه تنظیمات رفته و نوتیفیکشن را برای تگ هایی که از سوی کاربران، صفحه ها و انجمن های ناشناس صورت می گیرد تا غیر فعال کنید.



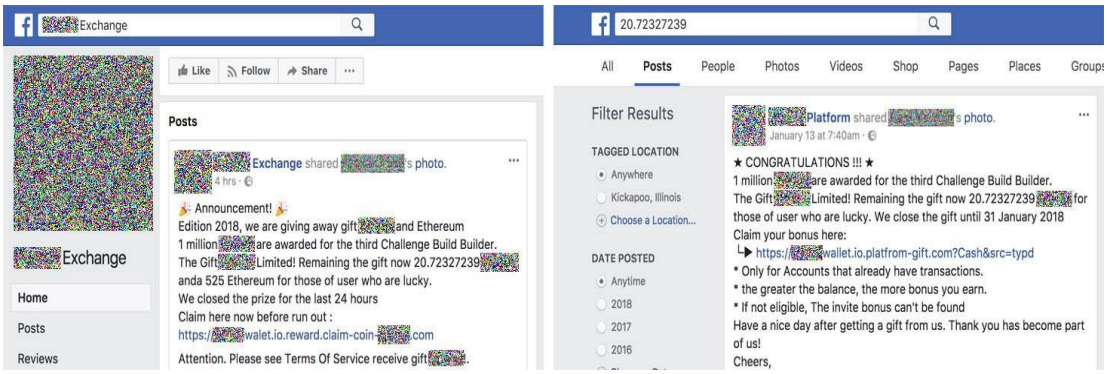
مرحله سوم)

کلاهبردار ها در این مرحله شخص قربانی را به عنوان یک شخص برتر و منتخب معرفی می کنند.

برای مثال ممکن است در پستی که شما را تگ کرده اند این طور عنوان کرده باشند که شما یکی از ده نفر خوش شانس برای دریافت ۲۰.۷۲۳۲۷۲۳۹ واحد ارز دیجیتال هستید. باید بدانید که آن ها واقعا رقم های این چنینی را پیشنهاد می دهند! سپس در انتهای پست لینکی وجود دارد که با ورود به آن می توانید جایزه ی پوچ خود را دریافت کنید.

به این نکته توجه داشته باشید که این پیام ها و لینک ها کاملا حرفه ای و از روی اصول نوشته و طراحی شده اند. مثلا در لینک ها کاملا قوانین و نقررات صرافی ها و محدودیت های ارزی نوشته شده است.

باید بدانید که سرویس ها و شرکت های ارائه دهنده ی خدمات رمز ارز های موسسه خیریه نیستند و هیچ پولی برای سرگرمی افراد در نظر نمی گیرند.



ارز دیجیتال رایگان! فریبی دروغین و همیشگی

اگر شخصی و یا اکانتی به شما وعده ی ارز رایگان را داد مساله خیلی ساده است، دارد دروغ می گوید! هیچ کس بی دلیل به کس دیگری پول دیجیتال، کاغذی یا هر نوع دیگری نمی دهد.

همیشه این سه مورد را در نظر داشته باشید:

اول) تمام لینک هایی که برای شما ارسال می شود را با دقت بررسی کنید. البته کاملا بهتر است اگر بر روی لینک های ناشناس اصلا کلیک نکنید. اگر فکر می کنید باید به سایت مورد نظر وارد شوید، خودتان آدرس مورد تاییدی که دارید را دستی در مرورگر خود وارد کنید.

دوم) تنظیمات مربوط به اطلاعات خصوصی خودتان را به دقت پیکربندی کنید.

سوم) از آنتی ویروس ها استفاده کنید. برای مثال Kaspersky آنتی ویروس قابل اعتمادی است.

سخن پایانی

در این مقاله سعی کردیم به طور کامل و جامع روش های کلاهبرداری در ارز های دیجیتال را به شما معرفی کنیم. فراموش نکنید که این ها فقط بخشی از روش های شناخته شده هستند و افراد کلاهبردار همواره در حال طراحی روش های خلاقانه برای به دست آوردن پول افراد دیگر هستند. اما هرچقدر هم که روش های جدید خلق شود شما می توانید با رعایت ساده ترین نکات مانند محافظت از کلید خصوصی خود، تا حد بسیار زیادی از خطر کلاهبرداری در امان بمانید.