Market Talks
مرکز آموزش

کریپتو · مبتدی · درس ۱۴ از ۱۵

کلاهبرداری، راگ‌پول و نشانه‌های هشدار

رایج‌ترین کلاهبرداری‌های کریپتو چطور کار می‌کنند، از راگ‌پول و پامپ و دامپ تا پلتفرم‌های سرمایه‌گذاری جعلی، جعل هویت و درینرهای کیف پول، و چه نشانه‌های هشداری میانشان مشترک است

۱۱ دقیقه مطالعه ۸ سؤال آزمون همراه با کلید پاسخ

کریپتو · مبتدی · درس ۱۴ از ۱۵

کلاهبرداری، راگ‌پول و نشانه‌های هشدار

در یک جمله

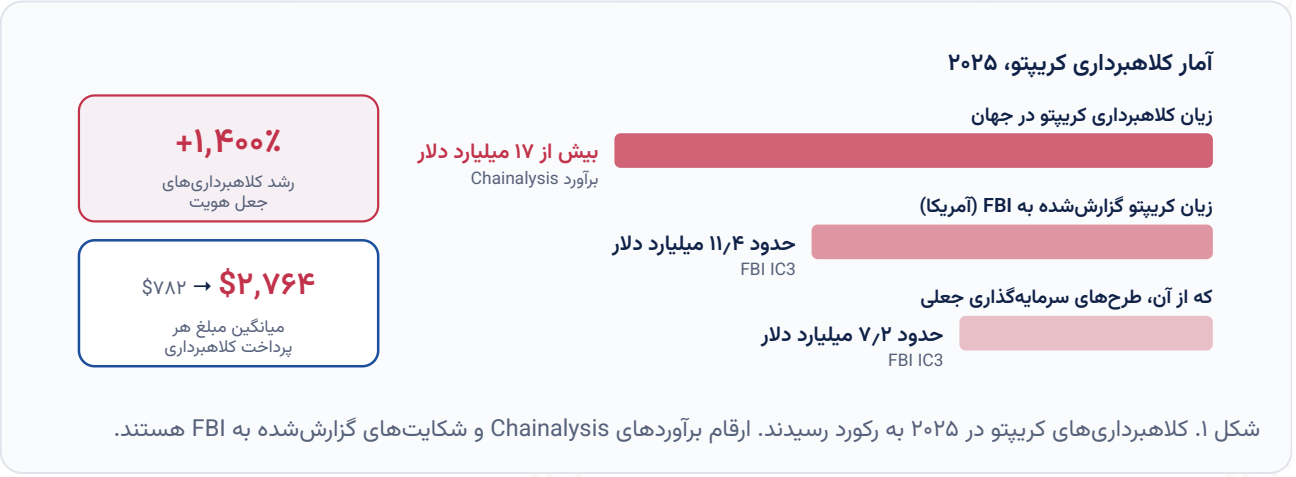
کلاهبرداری‌های کریپتو هر سال میلیاردها دلار می‌برند. بیشتر آن‌ها از چند الگوی محدود پیروی می‌کنند، و وقتی این الگوها را بشناسید، دیدن نشانه‌های هشدار بسیار آسان‌تر می‌شود.

چرا کلاهبرداری بخش بزرگی از کریپتو است

تراکنش‌های کریپتو سریع و جهانی‌اند و برگشت‌پذیر نیستند. هیچ بانکی نیست که بشود با آن تماس گرفت و پول را پس خواست، و هیچ مرکزی نیست که بتواند پرداختی را که از کیف پولتان خارج شده مسدود کند. همین ویژگی‌هایی که کریپتو را مفید می‌کنند، آن را برای کلاهبرداران هم جذاب می‌کنند.

ارقام بزرگ‌اند. شرکت تحلیل بلاک‌چین Chainalysis برآورد کرد که کلاهبرداری‌های کریپتو در ۲۰۲۵ **بیش از ۱۷ میلیارد دلار** بردند، که یک رکورد بود. فقط در ایالات متحده، مرکز شکایات جرائم اینترنتی FBI (IC3) در ۲۰۲۵ شکایت‌هایی مرتبط با کریپتو دریافت کرد که زیان گزارش‌شده آن‌ها حدود **۱۱٫۴ میلیارد دلار** بود، ۲۲٪ بیشتر از سال قبل. حدود ۷٫۲ میلیارد دلار از این رقم از طرح‌های سرمایه‌گذاری جعلی بود.

کلاهبرداری‌ها حرفه‌ای‌تر هم می‌شوند. Chainalysis دریافت که کلاهبرداری‌های جعل هویت در ۲۰۲۵ بیش از ۱٬۴۰۰٪ رشد کردند و میانگین مبلغ برده‌شده در هر پرداخت از حدود ۷۸۲ دلار به حدود ۲٬۷۶۴ دلار رسید. بسیاری از این گروه‌ها اکنون از هوش مصنوعی برای نوشتن پیام، ترجمه گفت‌وگوها و ساخت ویدیوهای جعلی استفاده می‌کنند.



شکل ۱. کلاهبرداری‌های کریپتو در ۲۰۲۵ به رکورد رسیدند. ارقام برآوردهای Chainalysis و شکایت‌های گزارش‌شده به FBI هستند.

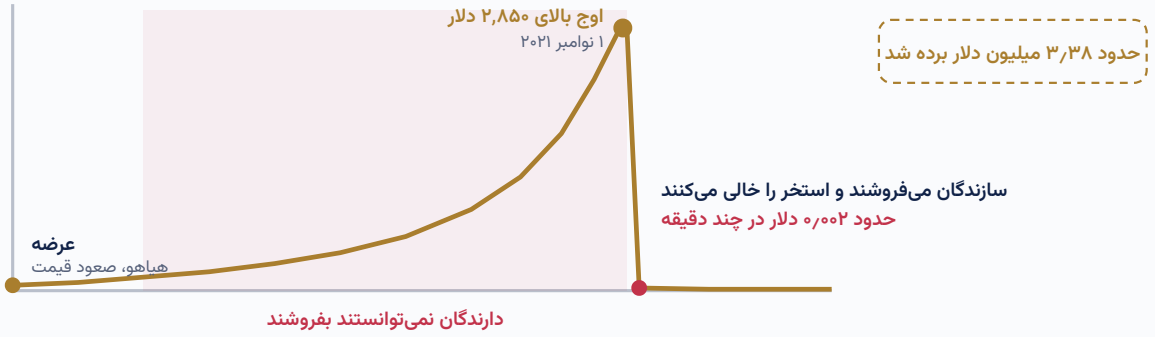
راگ‌پول و هانی‌پات

راگ‌پول (rug pull) زمانی رخ می‌دهد که افراد پشت یک توکن یا پروژه ناگهان پول را برمی‌دارند و ناپدید می‌شوند و به تعبیری «فرش را از زیر پای خریداران می‌کشند». این بیشتر در توکن‌های تازه روی صرافی‌های غیرمتمرکز رخ می‌دهد، جایی که هر کسی می‌تواند در چند دقیقه یک توکن و یک استخر معاملاتی بسازد (درس‌های ۷ و ۹).

انواع رایج آن:

- **کشیدن نقدینگی:** سازندگان سرمایه را از استخر معاملاتی خارج می‌کنند. وقتی چیزی برای معامله در برابرش باقی نمانده، قیمت توکن تقریباً به صفر سقوط می‌کند.
- **دامپ تیم:** سازندگان سهم بزرگی از عرضه را در اختیار دارند و همه را یک‌جا در بازار می‌فروشند.
- **هانی‌پات** (honeypot): قرارداد هوشمند توکن طوری نوشته شده که مردم بتوانند بخرند اما نتوانند بفروشند. نمودار قیمت فقط بالا می‌رود، چون هیچ‌کس جز سازندگان نمی‌تواند بفروشد.

کالبدشکافی یک راگ‌پول: توکن Squid Game



شکل ۲. نمایی ساده از راگ‌پول توکن Squid Game. دارندگان در حالی که قیمت بالا می‌رفت نمی‌توانستند بفروشند، سپس سازندگان استخر را خالی کردند.

مثال: توکن Squid Game (بازی مرکب)، ۲۰۲۱

در اواخر ۲۰۲۱ توکنی غیررسمی به نام این سریال پرطرفدار تلویزیونی روی PancakeSwap، یک صرافی غیرمتمرکز، ظاهر شد. قیمتش در چند روز ده‌ها هزار درصد بالا رفت و در ۱ نوامبر ۲۰۲۱ از **۲٬۸۵۰ دلار** گذشت. خریداران خیلی زود فهمیدند نمی‌توانند آن را بفروشند. سپس سازندگان دارایی‌شان را فروختند و استخر را خالی کردند، و در عرض چند دقیقه قیمت به حدود **۰٫۰۰۲ دلار** رسید. سازندگان با حدود ۳٫۳۸ میلیون دلار رفتند. سازندگان سریال هیچ ارتباطی با آن نداشتند.

پامپ و دامپ

در **پامپ و دامپ** (pump and dump)، گروهی یک کوین کوچک و کم‌معامله را بی‌سروصدا می‌خرند و سپس با پست‌های شبکه‌های اجتماعی، اینفلوئنسرهای پولی یا گروه‌های چت، پرسروصدا تبلیغش می‌کنند. با هجوم خریداران تازه، قیمت جهش می‌کند. سپس گردانندگان کوین‌هایشان را به همین خریداران دیرهنگام می‌فروشند («دامپ» می‌کنند) و قیمت برمی‌گردد، اغلب به زیر نقطه شروع.

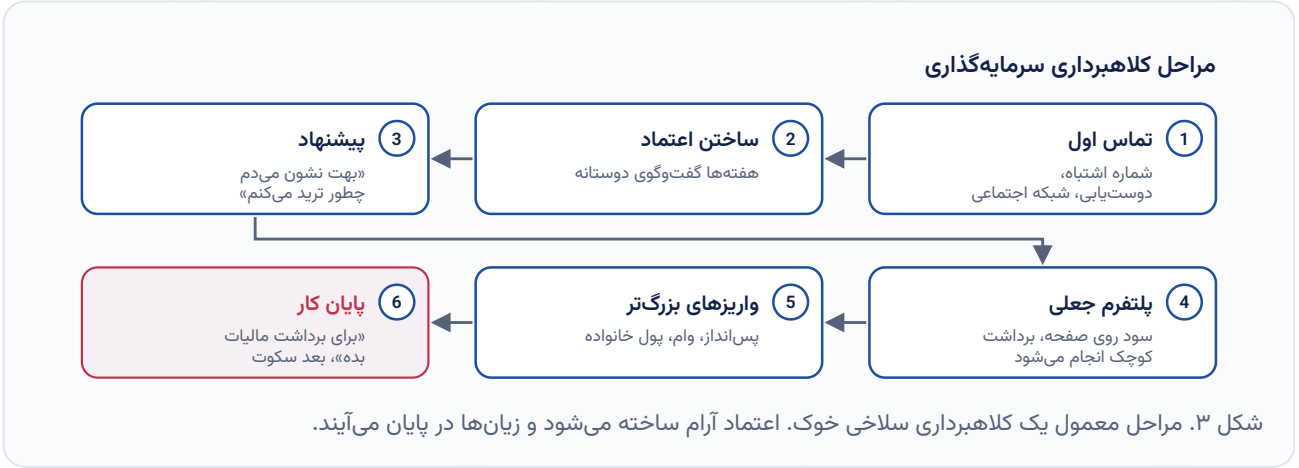
پامپ و دامپ‌ها جواب می‌دهند چون کوین‌های کوچک نقدینگی بسیار کمی دارند (درس ۸)، پس مقدار متوسطی خرید می‌تواند قیمت را بسیار جابه‌جا کند. سیلی ناگهانی از پست‌هایی که همه درباره یک کوین ناشناخته یک چیز می‌گویند، اغلب با شمارش معکوس و هدف قیمتی، نشانه‌ای رایج است.

پلتفرم‌های سرمایه‌گذاری جعلی و «سلاخی خوک»

بزرگ‌ترین دسته زیان‌ها از طرح‌های سرمایه‌گذاری جعلی می‌آید. یکی از شکل‌های شناخته‌شده آن **سلاخی خوک** (pig butchering) نام دارد، ترجمه عبارتی چینی که خود کلاهبرداران به کار می‌برند: قربانی را با اعتماد «پروار» می‌کنند و بعد «سلاخی».

معمولاً با پیامی شروع می‌شود که بی‌خطر به نظر می‌رسد: پیامکی با «شماره اشتباه»، یک آشنایی در اپلیکیشن دوست‌یابی یا یک مخاطب تازه در شبکه‌های اجتماعی. طی چند هفته، کلاهبردار یک دوستی یا رابطه عاطفی می‌سازد. سرانجام اشاره می‌کند که از معامله کریپتو درآمد خوبی دارد و پیشنهاد می‌دهد روشش را نشان دهد.

قربانی به سمت یک وب‌سایت یا اپلیکیشن معاملاتی هدایت می‌شود که حرفه‌ای به نظر می‌رسد اما جعلی است. موجودی روی صفحه سریع بالا می‌رود، و حتی برداشت‌های کوچک اولیه ممکن است انجام شوند، که اعتماد می‌سازد. واریزها بزرگ‌تر می‌شوند. وقتی قربانی می‌خواهد مبلغ زیادی برداشت کند، پلتفرم ناگهان اول یک «مالیات»، «کارمزد» یا «سپرده آزادسازی» می‌خواهد. پس از پرداخت آن، پلتفرم و آن دوست ناپدید می‌شوند.



شکل ۳. مراحل معمول یک کلاهبرداری سلاخی خوک. اعتماد آرام ساخته می‌شود و زیان‌ها در پایان می‌آیند.

مثال: از درون چطور به نظر می‌رسد

لورا پیامکی از مایکل دریافت می‌کند: «سلام دیوید، شنبه برای گلف هنوز قرارمان سر جایش است؟» او جواب می‌دهد که شماره را اشتباه گرفته است. مایکل عذرخواهی می‌کند و گفت‌وگویشان شروع می‌شود. شش هفته بعد، او اسکرین‌شات‌هایی از سودهای معاملاتی‌اش نشان می‌دهد و کمک می‌کند لورا در پلتفرمی که خودش استفاده می‌کند حساب باز کند. ۱,۰۰۰ دلار اول لورا روی صفحه به ۱,۶۰۰ دلار می‌رسد، و یک برداشت ۲۰۰ دلاری به کیف پولش می‌رسد. او ۲۵,۰۰۰ دلار واریز می‌کند. وقتی درخواست برداشت می‌دهد، پشتیبانی می‌گوید اول باید ۲۰٪ «مالیات» روی سودش بپردازد. اعداد روی صفحه هرگز واقعی نبودند.

جعل هویت، پشتیبانی جعلی و کلاهبرداری بازیابی وجه

بسیاری از کلاهبرداری‌ها با تظاهر به کسی که به او اعتماد دارید کار می‌کنند:

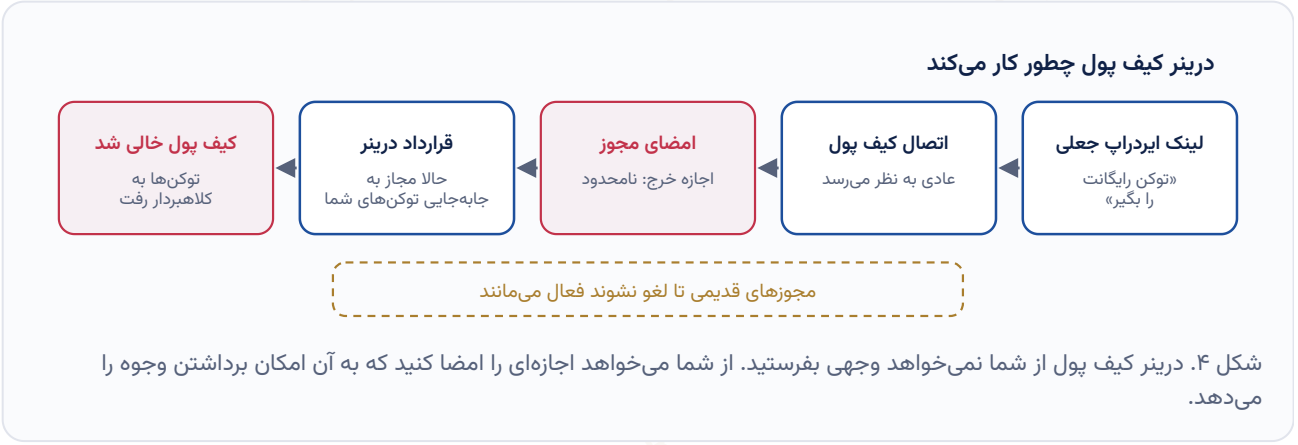
- **پشتیبانی جعلی:** پس از این‌که سؤالی در یک انجمن یا گروه چت عمومی می‌پرسید، کسی پیام خصوصی می‌فرستد و ادعا می‌کند از تیم پشتیبانی صرافی یا کیف پول است. تیم‌های پشتیبانی واقعی گفت‌وگوی خصوصی را شروع نمی‌کنند و هرگز عبارت بازیابی یا رمز عبور نمی‌خواهند.
- **تماس جعلی از طرف صرافی یا دولت:** تماسی تلفنی، ایمیل یا پیامکی می‌گوید حسابتان در خطر است و باید فوراً دارایی‌تان را به یک کیف پول «امن» منتقل کنید.
- **چهره‌های مشهور و جایزه‌های جعلی:** ویدیو یا پستی فردی مشهور را نشان می‌دهد که وعده می‌دهد هر مقدار کریپتو که بفرستید دو برابرش را پس بفرستد. ویدیوهای دیپ‌فیک (deepfake) ساخته‌شده با هوش مصنوعی اکنون این‌ها را باورپذیر می‌کنند. هیچ جایزه واقعی‌ای این‌طور کار نمی‌کند.
- **کلاهبرداری بازیابی وجه:** پس از این‌که کسی پولی از دست می‌دهد، یک «متخصص بازیابی» یا مؤسسه حقوقی جعلی پیشنهاد می‌کند در ازای کارمزدی پیشاپیش آن را برگرداند. هدف این‌ها کسانی است که یک بار کلاهبرداری را تجربه کرده‌اند.

درینرهای کیف پول، مجوزها و ایردراپ‌های جعلی

برخی کلاهبرداری‌ها نیازی ندارند شما چیزی بفرستید. در عوض، شما را فریب می‌دهند تا به یک قرارداد هوشمند مخرب اجازه جابه‌جایی توکن‌هایتان را بدهید.

وقتی از یک اپلیکیشن دیفای استفاده می‌کنید، کیف پولتان اغلب از شما می‌خواهد به یک قرارداد **مجوز** (approve) بدهید تا توکنی مشخص را از طرف شما خرج کند (درس ۱۲). یک وب‌سایت جعلی، که اغلب به‌عنوان **ایردراپ** رایگان، مینت یا دریافت جایزه تبلیغ می‌شود، از شما می‌خواهد کیف پولتان را وصل کنید و امضا کنید. آن‌چه در واقع امضا می‌کنید یک مجوز است، گاهی برای مقدار نامحدود، که به قرارداد کلاهبردار اجازه می‌دهد توکن‌هایتان را بردارد. به این نوع ابزار **درینر کیف پول** (wallet drainer) می‌گویند.

ترفندهای رایج دیگر شامل اپلیکیشن‌های کیف پول و افزونه‌های مرورگر جعلی است که عبارت بازیابی را هنگام تایپ می‌دزدند، آدرس‌های وب‌سایت مشابه، و مسمومسازی آدرس (درس ۱۰). هر کسی که **عبارت بازیابی** شما را داشته باشد کنترل کامل کیف پولتان را دارد، همان‌طور که در درس ۹ دوره بلاک‌چین دیدیم. مجوزهای قدیمی تا زمانی که حذف نشوند فعال می‌مانند، و ابزارهایی مثل Revoke.cash و برخی بلاک اکسپلوررها نشان می‌دهند یک کیف پول چه مجوزهایی داده است.



شکل ۴. درینر کیف پول از شما نمی‌خواهد وجهی بفرستید. از شما می‌خواهد اجازه‌ای را امضا کنید که به آن امکان برداشتن وجوه را می‌دهد.

نشانه‌های هشداری که بیشتر کلاهبرداری‌ها مشترک دارند

داستان‌ها عوض می‌شوند، اما نشانه‌های هشدار تکرار می‌شوند:

- **سود تضمینی یا بسیار بالا**، مثل «روزی ۲٪» یا «بدون ریسک».
- **عجله و فشار:** همین حالا اقدام کنید، پیشنهاد امشب تمام می‌شود، حسابتان بسته خواهد شد.
- **درخواست عبارت بازیابی یا کلید خصوصی**، به هر دلیلی.
- **تماس ناخواسته** که آرام‌آرام به سرمایه‌گذاری می‌رسد.
- **پلتفرمی که شناخته‌شده نیست**، به پیشنهاد یک دوست اینترنتی تازه، یا اپلیکیشنی که از منابع رسمی پیدا نشده است.
- **برداشت‌هایی که اول کارمزد می‌خواهند.**
- **«کریپتو بفرست، دو برابر پس بگیر».**
- **توکن‌هایی که نمی‌توانید بفروشید**، تیمی ناشناس که بیشتر عرضه را در اختیار دارد، یا نقدینگی قفل‌نشده.

یک نشانه هشدار به‌تنهایی اثبات کلاهبرداری نیست، اما چند نشانه با هم هشداری جدی است.



شکل ۵. نشانه‌های هشدار رایجی که بیشتر کلاهبرداری‌های کریپتو مشترک دارند.

پس از کلاهبرداری چه اتفاقی می‌افتد

چون انتقال‌های بلاک‌چینی قطعی‌اند، پولی که به کلاهبردار فرستاده شده به‌ندرت بازیابی می‌شود. گاهی اگر وجوه سریع به یک صرافی تحت نظارت برسد، آن صرافی می‌تواند آن‌ها را مسدود کند، و صادرکنندگان استیبل‌کوین مثل Tether و Circle در برخی موارد وجوه سرقت‌شده را مسدود کرده‌اند.

مراحلی که مقاماتی مثل FBI برمی‌شمارند شامل گزارش کلاهبرداری به پلیس و، در آمریکا، به IC3؛ اطلاع دادن به صرافی یا پلتفرمی که استفاده شده؛ نگه داشتن سوابقی مثل هش تراکنش‌ها، آدرس کیف پول‌ها، پیام‌ها و لینک وب‌سایت‌ها؛ و حذف مجوزهای کیف پولی است که داده شده‌اند. بسیاری از افراد هم اگر فکر کنند کیف پول قدیمی لو رفته، دارایی باقی‌مانده را به کیف پولی تازه با عبارت بازیابی تازه منتقل می‌کنند.

مقامات همچنین هشدار می‌دهند که با کسانی که زیانی را گزارش می‌کنند اغلب بعداً کلاهبرداران بازیابی وجه تماس می‌گیرند، پس زیان دوم ممکن است به دنبال زیان اول بیاید.

چرا این برای معامله‌گران مهم است

- **سودهای سریع کلاهبرداری را جذب می‌کنند.** توکن‌های تازه با رشدهای روزانه عظیم دقیقاً همان جایی‌اند که راگ‌پول، هانی‌پات و پامپ و دامپ رخ می‌دهد. بررسی این‌که یک توکن قابل فروش است یا نه، چه کسانی عرضه را در اختیار دارند و آیا نقدینگی قفل شده است، بخشی از تحقیق پایه‌ای است که بسیاری از معامله‌گران انجام می‌دهند.
- **پیشنهادهای «معاملاتم را کپی کن».** گروه‌هایی که در ازای واریز، وعده نکات معاملاتی خصوصی یا مدیریت حساب می‌دهند، دروازه ورود رایجی به پلتفرم‌های جعلی‌اند.
- **مجوزها انباشته می‌شوند.** کاربران فعال دیفای ممکن است به مرور زمان مجوزهای قدیمی زیادی برای توکن‌ها جمع کنند. اگر قرارداد روزی در معرض نفوذ قرار بگیرد، هر کدام ریسکی بالقوه است.
- **همان عادت‌های امنیتی از حساب‌های معاملاتی هم محافظت می‌کنند.** حساب‌های صرافی هم هدف‌اند: ایمیل‌های فیشینگ، صفحه‌های ورود جعلی و سیم‌سواپ (SIM swap) با هدف تصاحب حساب و برداشت دارایی انجام می‌شوند. درس ۱۵ محافظت‌های پایه‌ای را که صرافی‌ها ارائه می‌کنند بررسی می‌کند.

اصطلاحات کلیدی

راگ‌پول (rug pull)	وقتی سازندگان یک پروژه ناگهان پول را برمی‌دارند، مثلاً با خارج کردن نقدینگی یا دامپ توکن‌هایشان، و توکن تقریباً بی‌ارزش می‌ماند.
هانی‌پات (honeypot)	توکنی که قرارداد هوشمندش خرید را مجاز می‌کند اما فروش را برای همه به جز سازندگان مسدود می‌کند.
پامپ و دامپ	طرحی که در آن گردانندگان یک کوین کوچک را می‌خرند، با هیاهو قیمت را بالا می‌برند و سپس به خریداران دیرهنگام می‌فروشند.
سلاخی خوک (pig butchering)	کلاهبرداری طولانی‌ای که در آن کلاهبردار طی چند هفته اعتماد می‌سازد و سپس قربانی را به واریز مبالغ بزرگ در یک پلتفرم سرمایه‌گذاری جعلی می‌کشاند.
فیشینگ	پیام‌ها، ایمیل‌ها یا وب‌سایت‌های جعلی که از یک سرویس واقعی تقلید می‌کنند تا مردم را به لو دادن رمز عبور، کد یا عبارت بازیابی فریب دهند.
درینر کیف پول (wallet drainer)	کدی مخرب در یک وب‌سایت جعلی که کاربران را فریب می‌دهد تا مجوزها یا تراکنش‌هایی را امضا کنند که توکن‌هایشان را به کلاهبردار منتقل می‌کند.
مجوز توکن (approval)	اجازه‌ای که امضا می‌کنید تا یک قرارداد هوشمند بتواند توکنی مشخص را از کیف پول شما خرج کند، تا سقفی معین یا بدون سقف.

دیپ‌فیک	ویدیو یا صدای جعلی، معمولاً ساخته‌شده با هوش مصنوعی، که فردی واقعی را در حال گفتن چیزی نشان می‌دهد که هرگز نگفته است.
کلاهبرداری بازیابی وجه	کلاهبرداری بعدی که کسانی را هدف می‌گیرد که از قبل پول از دست داده‌اند و وعده می‌دهد در ازای کارمزدی پیشاپیش آن را برگرداند.

نکات کلیدی

1. پرداخت‌های کریپتو سریع و قطعی‌اند و همین آن‌ها را برای کلاهبرداران جذاب می‌کند. Chainalysis زیان کلاهبرداری‌ها در ۲۰۲۵ را بیش از ۱۷ میلیارد دلار برآورد کرد.
2. راگ‌پول، هانی‌پات و پامپ و دامپ بیشتر در توکن‌های تازه و کوچک رایج‌اند. توکن Squid Game در چند دقیقه از بالای ۲,۸۵۰ دلار به تقریباً صفر رسید.
3. پلتفرم‌های سرمایه‌گذاری جعلی، که اغلب از راه یک دوستی اینترنتی طولانی به آن‌ها می‌رسند، بیشترین زیان را به بار می‌آورند. موجودی‌های ساختگی و برداشت‌های کوچک اولیه اعتماد می‌سازند.
4. جاعلان هویت خود را کارمند پشتیبانی، صرافی، مقام رسمی یا چهره مشهور جا می‌زنند. پشتیبانی واقعی هرگز عبارت بازیابی نمی‌خواهد.
5. درینرهای کیف پول به جای درخواست ارسال وجه، از مجوزهای امضاشده استفاده می‌کنند. مجوزهای قدیمی تا زمان حذف فعال می‌مانند.
6. سود تضمینی، عجله، درخواست عبارت بازیابی و کارمزد برای برداشت رایج‌ترین نشانه‌های هشدارند.

خودتان را محک بزنید

برای هر سؤال دور یک گزینه را خط بکشید. کلید پاسخ‌ها همراه با توضیح در صفحه بعد آمده است. این آزمون را می‌توانید به‌صورت آنلاین هم در markettalks.info انجام دهید و نتیجه را فوراً ببینید.

۱. چرا پرداخت‌های کریپتو برای کلاهبرداران جذاب‌اند؟

- A) همیشه ناشناس و نامرئی‌اند
- B) سریع و جهانی‌اند و برگشت‌پذیر نیستند
- C) صرافی‌ها سود کلاهبرداران را تضمین می‌کنند
- D) فقط شب‌ها می‌توان آن‌ها را فرستاد

۲. توکن هانی‌پات چیست؟

A توکنی با پشتوانه عسل واقعی
B توکنی که پاداش استیکینگ بالایی می‌دهد
C توکنی که قراردادش اجازه خرید می‌دهد اما اجازه فروش نه
D استیبل‌کوینی متصل به طلا

۳. در نوامبر ۲۰۲۱ چه بر سر توکن Squid Game آمد؟

A در همه صرافی‌های بزرگ لیست شد
B سازندگانش استخر را خالی کردند و قیمت از بالای ۲,۸۵۰ دلار به حدود ۰٫۰۰۲ دلار رسید
C سازندگان سریال کل عرضه را خریدند
D به یک استیبل‌کوین تبدیل شد

۴. در پامپ و دامپ معمولاً چه کسی پول از دست می‌دهد؟

A گردانندگانی که اول خریدند
B خریداران دیرهنگامی که به خاطر هیاهو وارد شدند
C اعتبارسنج‌های بلاک‌چین
D هیچ‌کس، بدون ریسک است

۵. در کلاهبرداری سلاخی خوک، چرا برداشت‌های کوچک اولیه اغلب انجام می‌شوند؟

A چون پلتفرم واقعی است
B برای ساختن اعتماد پیش از واریزهای بزرگ‌تر
C به خاطر قواعد بلاک‌چین
D چون بانک آن را اجباری می‌کند

۶. کسی در پیام خصوصی می‌گوید از تیم پشتیبانی کیف پول شماست و برای رفع یک مشکل عبارت بازیابی‌تان را می‌خواهد. این چیست؟

A روال عادی پشتیبانی
B یک بررسی امنیتی الزامی
C یک کلاهبرداری جعل هویت معمول
D یک به‌روزرسانی نرم‌افزار

۷. درینر کیف پول معمولاً چطور توکن‌ها را می‌برد؟

A با حدس زدن رمز عبور شما

B با وادار کردن شما به امضای یک مجوز یا تراکنش در یک سایت جعلی

C با هک کردن کل بلاک‌چین

D با تغییر دادن قیمت توکن

۸. کدام‌یک از این‌ها نشانه هشدار رایجی از کلاهبرداری است؟

A پلتفرمی که پیش از برداشت از شما کارمزد می‌خواهد

B این‌که بتوانید هر زمان توکنی را بفروشید

C صرافی شناخته‌شده‌ای با حسابرسی‌های عمومی

D قیمتی که هم بالا و هم پایین می‌رود

کلید پاسخ‌ها

۱ **B**

سریع و جهانی‌اند و برگشت‌پذیر نیستند

وقتی یک انتقال تأیید شود، هیچ بانک یا شرکت پرداختی نمی‌تواند آن را برگرداند، و وجوه می‌توانند در چند دقیقه از مرزها بگذرند.

۲ **C**

توکنی که قراردادش اجازه خرید می‌دهد اما اجازه فروش نه

قرارداد فروش را برای دارندگان عادی مسدود می‌کند، پس قیمت فقط ظاهراً بالا می‌رود تا وقتی سازندگان پولشان را نقد کنند.

۳ **B**

سازندگانش استخر را خالی کردند و قیمت از بالای ۲,۸۵۰ دلار به حدود ۰٫۰۰۲ دلار رسید

خریداران نمی‌توانستند بفروشند، سپس سازندگان فروختند و نقدینگی را بردند و قیمت در عرض چند دقیقه سقوط کرد.

۴ **B**

خریداران دیرهنگامی که به خاطر هیاهو وارد شدند

گردانندگان زود می‌خرند و به کسانی می‌فروشند که پس از تبلیغات می‌رسند، و آن‌ها با کوینی در حال سقوط تنها می‌مانند.

۵ **B**

برای ساختن اعتماد پیش از واریزهای بزرگ‌تر

اجازه خروج مبلغی کوچک پلتفرم جعلی را واقعی جلوه می‌دهد، پس قربانی با خیال راحت مبلغ بسیار بیشتری واریز می‌کند.

۶ **C**

یک کلاهبرداری جعل هویت معمول

هر کسی که عبارت بازیابی شما را داشته باشد کیف پولتان را کنترل می‌کند. تیم‌های پشتیبانی واقعی هرگز آن را نمی‌خواهند.

۷ **B**

با وادار کردن شما به امضای یک مجوز یا تراکنش در یک سایت جعلی

کاربر اجازه‌ای را امضا می‌کند، که اغلب به شکل دریافت یک ایردراپ نشان داده می‌شود، و این اجازه به قرارداد کلاهبردار امکان جابه‌جایی توکن‌ها را می‌دهد.

۸ **A**

پلتفرمی که پیش از برداشت از شما کارمزد می‌خواهد

درخواست مالیات، کارمزد یا سپرده پیش از آزاد کردن برداشت، نشانه کلاسیک یک پلتفرم جعلی است.

منابع

- Decrypt، هوش مصنوعی و جعل هویت زیان کلاهبرداری‌های کریپتو در ۲۰۲۵ را به رکورد ۱۷ میلیارد دلار رساندند (Chainalysis): https://decrypt.co/354624/ai-impersonation-drove-crypto-scam-losses-record-17-billion-2025-chainalysis
- Yahoo Finance، گزارش FBI از رشد ۲۲ درصدی زیان کلاهبرداری کریپتو در ۲۰۲۵: https://finance.yahoo.com/markets/crypto/articles/fbi-reports-22-rise-crypto-191510401.html

- Cointelegraph، فروپاشی کلاهبرداری کریپتویی الهام‌گرفته از Squid Game با سقوط قیمت از ۲٫۸ هزار دلار به صفر: https://cointelegraph.com/news/game-over-squid-game-inspired-crypto-scam-collapses-as-price-crashes-from-2-8k-to-zero
- Cointelegraph، کاربران نمی‌توانند توکن Squid Game را بفروشند: https://cointelegraph.com/news/users-not-able-to-sell-squid-game-token-clocking-45-000-gains

Market Talks

ادامه یادگیری

درس بعدی: درس ۱۵ واقعاً چطور شروع کنیم: صرافی‌ها، احراز هویت و کیف پول‌ها

این درس بخشی از دوره کریپتو در مرکز آموزش MARKET TALKS است. درس‌های سطح مبتدی رایگان‌اند و هر کدام یک آزمون و یک فایل PDF قابل دانلود دارند. درس‌های سطح متوسط و پیشرفته ویژه اعضا هستند.

مرکز آموزش
درس‌هایی از اصول پایه تا موضوعات پیشرفته

تحلیل بازارها
تحلیل تکنیکال و بنیادی بازارهای اصلی

گزارش‌ها
بیت‌کوین، طلا، نقره، SPX و بیشتر

markettalks.info

تلگرام @MARKET_TALKS

فقط برای آموزش. هیچ‌یک از مطالب این سند توصیه مالی نیست. © ۲۰۲۶ MARKET TALKS. می‌توانید این PDF را بدون تغییر به اشتراک بگذارید.