رازهای کلاهبرداری در رمزارزها

از طرح پانزی تا فیشینگ

شرکت نرم افزاری جادوی فکر - (مجری پروژه نرم افزاری حوزه هوش مصنوعی و بلاکچین)

www.jadoosoft.com

۱. مقدمه‌ای بر دنیای رمزارزها و ریسک‌های پنهان
(Introduction to Cryptocurrencies and Hidden Risks)

۲. انواع رایج کلاهبرداری در بازار رمزارز
(Common Types of Crypto Scams)

۳. طرح پانزی (Ponzi Scheme): فریب با وعده سود تضمینی
(Ponzi Schemes: The Illusion of Guaranteed Profits)

۴. طرح‌های هرمی (Pyramid Scheme): دعوت به فریب جمعی
(Pyramid Schemes: Collective Deception)

۵. پروژه‌های اسکم و راگ پول (Rug Pull & Exit Scam): خروج ناگهانی بنیان‌گذاران
(Rug Pull & Exit Scam: Sudden Founder Exits)

۶. کلاهبرداری ICO و توکن‌های جعلی
(Fake ICOs and Tokens)

۷. فیشینگ (Phishing): دامی برای سرقت دارایی‌های دیجیتال
(Phishing: The Trap for Stealing Digital Assets)

۸. کلاهبرداری‌های صرافی و کیف پول جعلی
(Exchange and Fake Wallet Scams)

۹. سوءاستفاده از شبکه‌های اجتماعی و تبلیغات فریبنده
(Social Media Manipulation and Influencer Scams)

۱۰. بدافزارها و حملات هکری به دارایی‌های رمزارزی
(Malware and Hacking Attacks)

۱۱. نشانه‌های پروژه‌های مشکوک و راه‌های شناسایی آنها
(How to Spot Suspicious Crypto Projects)

۱۲. استانداردها و ابزارهای امنیتی برای مقابله با کلاهبرداری
(Security Standards and Tools to Combat Scams)

۱۳. قوانین، مقررات و نقش نهادهای نظارتی در پیشگیری از کلاهبرداری
(Regulations and the Role of Supervisory Authorities)

۱۴. تجربه‌های واقعی: روایت قربانیان و بررسی پرونده‌های مشهور
(Real Stories: Victims' Narratives and Famous Cases)

۱۵. جمع‌بندی و توصیه‌های طلایی برای حفظ امنیت در بازار رمزارزها
(Conclusion and Golden Tips for Crypto Security)

پیشگفتار

در سال‌های اخیر، بازار رمزارزها (Cryptocurrencies) با سرعتی خیره‌کننده رشد کرده و میلیون‌ها نفر در سراسر جهان را به سوی فرصت‌های مالی نوین جذب نموده است. این انقلاب دیجیتال، در کنار وعده‌های وسوسه‌کننده‌ای چون آزادی مالی، حذف واسطه‌ها و شفافیت، مخاطرات و چالش‌هایی را نیز با خود به همراه آورده است که اگر نادیده گرفته شوند، می‌توانند سرمایه و حتی آرامش روانی افراد را به خطر اندازند.

آنچه این بازار را از سایر بازارهای سنتی متمایز می‌سازد، ماهیت غیرمتمرکز، ناشناس بودن تراکنش‌ها و نبود چارچوب‌های نظارتی یکپارچه است. همین ویژگی‌ها، زمینه‌ای مناسب برای ظهور انواع کلاهبرداری‌های خلاقانه و پیچیده فراهم آورده که گاه تشخیص آن‌ها حتی برای افراد باتجربه نیز دشوار است.

در دنیای رمزارزها، کلاهبرداران با بهره‌گیری از دانش روانشناسی، فناوری‌های نوین و ضعف‌های قانونی، از طرح‌های پانزی و هرمی گرفته تا پروژه‌های اسکم، فیشینگ، صرافی‌ها و کیف پول‌های جعلی، دام‌های گوناگونی برای سرمایه‌گذاران و کاربران پهن می‌کنند. در بسیاری از موارد، قربانیان این دام‌ها افرادی هستند که با امید رسیدن به سودهای کلان و بدون آگاهی کافی از ریسک‌های پنهان، وارد بازی خطرناکی می‌شوند که گاهی بازگشتی برای آن متصور نیست.

هدف از نگارش این کتاب، ارائه‌ی راهنمایی جامع، کاربردی و به‌روز برای شناسایی، پیشگیری و مقابله با انواع کلاهبرداری‌های رایج در دنیای رمزارزهاست. تلاش شده است با استفاده از مثال‌های واقعی، تحلیل روانشناسی کلاهبرداران، بررسی پرونده‌های مشهور و ارائه ابزارها و راهکارهای عملی، سطح آگاهی و امنیت خوانندگان به طرز چشمگیری افزایش یابد.

امید است مطالعه‌ی این کتاب، شما را در مسیر سرمایه‌گذاری هوشمندانه و ایمن در بازار رمزارزها یاری رسانده و گامی مؤثر در جهت کاهش آسیب‌های مالی و روانی ناشی از کلاهبرداری‌های دیجیتال بردارد.

به دنیای شفاف‌سازی، آموزش و هوشیاری خوش آمدید.

فصل اول: مقدمه‌ای بر دنیای رمزارزها و ریسک‌های پنهان

Introduction to Cryptocurrencies and Hidden Risks

۱.۱ رمزارز چیست و چرا محبوب شد؟

رمزارزها (Cryptocurrencies) گونه‌ای از دارایی‌های دیجیتال هستند که از فناوری رمزنگاری برای امنیت و صحت تراکنش‌ها بهره می‌برند. بیت‌کوین (Bitcoin) اولین رمزارزی بود که در سال ۲۰۰۹ معرفی شد و پس از آن هزاران رمزارز دیگر مانند اتریوم(Ethereum) ، بایننس‌کوین(Binance Coin) ، سولانا (Solana)و... به بازار آمدند.

ویژگی‌های جذاب رمزارزها عبارتند از:

- **غیرمتمرکز بودن** :(Decentralization)یعنی هیچ نهاد مرکزی مانند بانک یا دولت کنترل مستقیم بر شبکه ندارد.
- **ناشناس بودن** :(Anonymity)کاربران می‌توانند بدون افشای هویت خود، تراکنش انجام دهند.
- **امکان انتقال سریع و کم‌هزینه** :(Fast & Low-Cost Transfers)انتقال دارایی‌ها در هر نقطه از جهان با هزینه پایین و سرعت بالا.
- **پتانسیل سودآوری بالا** :(High Profit Potential)نوسانات زیاد و رشد چشمگیر برخی رمزارزها موجب جذب سرمایه‌گذاران شده است.

اما همین جذابیت‌ها، باعث شده عده‌ای سودجو نیز به این بازار وارد شوند و از بی‌اطلاعی، طمع یا بی‌تجربگی افراد سوءاستفاده کنند.

۱.۲ ریسک‌های پنهان در بازار رمزارزها

بازار رمزارزها اگرچه فرصت‌های جذابی دارد، اما با ریسک‌ها و خطرات جدی نیز همراه است. مهم‌ترین این ریسک‌ها عبارتند از:

الف) نبود نظارت مرکزی و قانون‌گذاری شفاف

در بسیاری از کشورها، رمزارزها خارج از چارچوب‌های نظارتی رایج معامله می‌شوند و قوانین مشخصی برای حفاظت از سرمایه‌گذاران وجود ندارد. این موضوع زمینه مناسبی برای ظهور انواع کلاهبرداری‌ها فراهم کرده است.

ب) غیرقابل بازگشت بودن تراکنش‌ها

برخلاف بانک‌ها که در صورت بروز اشتباه یا سرقت ممکن است امکان پیگیری یا بازگرداندن پول وجود داشته باشد، تراکنش‌های رمزارزی اصولاً برگشت‌ناپذیر هستند. اگر دارایی شما به آدرس اشتباهی ارسال شود یا فریب بخورید، عملاً بازیابی آن غیرممکن است.

ج) ناشناس بودن طرفین

در بسیاری از کلاهبرداری‌ها، فرد کلاهبردار با هویت جعلی یا ناشناس فعالیت می‌کند و شناسایی یا پیگیری او بسیار دشوار است.

د) تکنولوژی پیچیده و نیاز به دانش تخصصی

بسیاری از کاربران بدون آشنایی کافی با مفاهیم فنی وارد این حوزه می‌شوند. همین ناآگاهی، آن‌ها را طعمه‌ای آسان برای کلاهبرداران می‌کند.

هـ) وسوسه سودهای کلان و وعده‌های غیرواقعی

تبلیغات اغواکننده و وعده‌های سود نجومی، بسیاری را فریب می‌دهد. طرح‌هایی که سودهای تضمینی، دو برابر شدن سرمایه در مدت کوتاه یا سود بدون ریسک وعده می‌دهند، تقریباً همیشه کلاهبرداری‌اند.

۱.۳ چرا کلاهبرداری در رمزارزها گسترده و پیچیده است؟

برخلاف بازارهای سنتی مثل بورس یا بانک، در دنیای رمزارزها، نظارت و شفافیت کافی وجود ندارد. این فضا، بستری مناسب برای شکل‌گیری مدل‌های مختلف کلاهبرداری و فریبکاری است. برخی دلایل گسترش کلاهبرداری در رمزارزها عبارتند از:

- **رشد سریع فناوری و نوآوری‌های مالی**
- **ورود سرمایه‌گذاران مبتدی و غیرحرفه‌ای**
- **نبود مرجع پاسخگو و پشتیبانی رسمی**
- **امکان پنهان کردن هویت واقعی کلاهبرداران**
- **دسترسی جهانی و فرامرزی بودن بازار**

مثال واقعی

در سال ۲۰۲۱، پروژه‌ای به نام Squid Game Tokenبا الهام از سریال محبوب «بازی مرکب» راه‌اندازی شد و تبلیغات گسترده‌ای در شبکه‌های اجتماعی داشت. تنها در چند روز، هزاران نفر با امید کسب سودهای بزرگ، دارایی خود را در این توکن سرمایه‌گذاری کردند. اما تیم سازنده به‌صورت ناگهانی همه دارایی‌ها را برداشت و ناپدید شد. قربانیان هیچ مرجعی برای پیگیری نداشتند.

۱.۴ انواع کلاهبرداری‌ها در بازار رمزارزها

کلاهبرداران در این بازار، از روش‌های متنوع و خلاقانه‌ای استفاده می‌کنند. برخی از رایج‌ترین روش‌ها عبارتند از:

- طرح‌های پانزی و هرمی
- پروژه‌های اسکم و راگ‌پول
- فیشینگ و سرقت اطلاعات
- کیف پول و صرافی‌های جعلی
- بدافزارها و حملات هکری
- سوءاستفاده از اینفلوئنسرها و شبکه‌های اجتماعی

در فصل‌های بعدی، هر یک از این روش‌ها با جزئیات و مثال‌های واقعی بررسی خواهد شد.

۱.۵ چه کسانی بیشترین ریسک قربانی شدن را دارند؟

- افراد تازه‌وارد و بدون دانش تخصصی
- کسانی که به دنبال سود سریع و آسان هستند
- افرادی که فریب تبلیغات شبکه‌های اجتماعی را می‌خورند
- کاربرانی که امنیت دارایی‌های خود را جدی نمی‌گیرند

۱.۶ چگونه می‌توان از این ریسک‌ها در امان ماند؟

۱ .**آگاهی و آموزش مداوم:**
مطالعه منابع معتبر و به‌روز درباره رمزارزها و امنیت آن‌ها.

۲ .**بررسی دقیق پروژه‌ها و تیم توسعه‌دهنده:**
هر پروژه‌ای که وعده سود غیرعادی می‌دهد یا اطلاعات شفاف ارائه نمی‌کند، مشکوک است.

۳ .**استفاده از کیف پول‌ها و صرافی‌های معتبر:**
همیشه از سرویس‌هایی استفاده کنید که سابقه و اعتبار خوبی دارند.

۴ .**حفظ امنیت اطلاعات شخصی:**
رمز عبور قوی، احراز هویت دومرحله‌ای و عدم اشتراک‌گذاری کلید خصوصی با هیچ‌کس.

۵ .**عدم اعتماد به پیام‌های تبلیغاتی و وعده‌های اغواکننده:**
هیچ سرمایه‌گذاری بدون ریسک یا با سود تضمینی در دنیای رمزارز وجود ندارد.

جمع‌بندی فصل اول

بازار رمزارزها، مانند هر بازار مالی نوظهور، در کنار فرصت‌های بی‌شمار، تهدیدها و ریسک‌های پنهانی نیز دارد. تنها راه موفقیت و امنیت در این فضا، داشتن دانش کافی، هوشیاری و دوری از طمع و شتاب‌زدگی است. در ادامه کتاب، با انواع کلاهبرداری‌ها، شگردهای کلاهبرداران و راه‌های مقابله با آن‌ها آشنا خواهید شد تا سرمایه‌گذاری شما در این بازار، آگاهانه و ایمن باشد.

فصل دوم: انواع رایج کلاهبرداری در بازار رمزارز

Common Types of Crypto Scams

دنیای رمزارزها با وجود فرصت‌های بی‌نظیر برای رشد سرمایه، بستری مناسب برای انواع مختلف کلاهبرداری نیز فراهم آورده است. کلاهبرداران با استفاده از تکنیک‌های روانشناسی، فناوری‌های نوین و ضعف‌های نظارتی، هر روز روش‌های تازه‌ای برای فریب کاربران ابداع می‌کنند. در این فصل، مهم‌ترین و رایج‌ترین شیوه‌های کلاهبرداری در بازار رمزارزها را به تفصیل معرفی می‌کنیم.

۲.۱ طرح‌های پانزی(Ponzi Schemes)

تعریف

طرح پانزی یکی از قدیمی‌ترین روش‌های کلاهبرداری مالی است که با وعده پرداخت سودهای ثابت و بالا، سرمایه افراد را جذب می‌کند. سود پرداختی به سرمایه‌گذاران قدیمی، در واقع از سرمایه جذب‌شده افراد جدید تأمین می‌شود و هیچ فعالیت اقتصادی واقعی در کار نیست.

ویژگی‌ها و نشانه‌ها

- وعده سود تضمینی و بالا در مدت کوتاه
- عدم شفافیت در مورد نحوه فعالیت و منبع درآمد پروژه
- تأکید بر جذب زیرمجموعه و گسترش شبکه
- عدم وجود محصول یا خدمت واقعی

مثال واقعی

در سال ۲۰۱۹ پروژه‌ای به نام PlusTokenدر چین با وعده سود ماهانه بالا موفق به جذب بیش از دو میلیارد دلار شد. پس از مدتی، مؤسسان پروژه ناپدید شدند و سرمایه هزاران نفر از بین رفت.

۲.۲ طرح‌های هرمی(Pyramid Schemes)

تعریف

طرح هرمی شباهت زیادی به پانزی دارد اما تأکید آن بر جذب زیرمجموعه است. شرکت‌کنندگان برای کسب سود، باید افراد جدیدی را وارد سیستم کنند و بخشی از سرمایه ورودی آن‌ها به عنوان سود پرداخت می‌شود.

ویژگی‌ها و نشانه‌ها

- دعوت از دوستان و آشنایان به بهانه سرمایه‌گذاری یا خرید محصول
- دریافت پاداش یا سود در قبال عضوگیری
- نبود کسب‌وکار واقعی و تمرکز صرف بر جذب اعضای جدید

مثال واقعی

در برخی کشورها، پروژه‌هایی با عنوان "بازاریابی شبکه‌ای رمزارزی" فعال شدند که عمدتاً هدفشان جذب سرمایه از طریق فروش توکن یا بسته‌های آموزشی بی‌ارزش بود.

۲.۳ پروژه‌های اسکم و راگ پول(Rug Pull & Exit Scam)

تعریف

در این روش، توسعه‌دهندگان یک پروژه رمزارزی یا توکن، با تبلیغات گسترده، سرمایه زیادی جذب می‌کنند. اما پس از جمع‌آوری پول، ناگهان پروژه را رها کرده و ناپدید می‌شوند.

ویژگی‌ها و نشانه‌ها

- تبلیغات هیجانی و وعده سود بالا
- عدم شفافیت تیم توسعه‌دهنده
- قفل نبودن نقدینگی (Liquidity) در صرافی‌های غیرمتمرکز

- حذف ناگهانی وب‌سایت و شبکه‌های اجتماعی پروژه

مثال واقعی

توکن Squid Gameدر سال ۲۰۲۱ یکی از معروف‌ترین راگ‌پول‌ها بود. ارزش توکن ظرف چند دقیقه از چند هزار دلار به نزدیک صفر رسید و تیم سازنده ناپدید شد.

۲.۴ فیشینگ (Phishing) و سرقت اطلاعات

تعریف

فیشینگ نوعی حمله سایبری است که در آن کلاهبرداران با جعل سایت، ایمیل یا پیامک، اطلاعات حساس کاربران (مانند کلید خصوصی یا رمز عبور) را سرقت می‌کنند.

ویژگی‌ها و نشانه‌ها

- ارسال ایمیل یا پیامک جعلی با ظاهری شبیه به صرافی یا کیف پول معتبر
- ساخت سایت‌های فیک با آدرس بسیار مشابه به سایت‌های اصلی
- درخواست فوری برای وارد کردن اطلاعات ورود یا کلید خصوصی

مثال واقعی

بسیاری از کاربران متامسک (MetaMask) قربانی صفحات جعلی و فیشینگ شدند که در ظاهر کاملاً مشابه سایت اصلی بودند و کلید خصوصی آن‌ها را سرقت کردند.

۲.۵ کیف پول‌ها و صرافی‌های جعلی

تعریف

کلاهبرداران با طراحی نرم‌افزارها یا سایت‌هایی مشابه کیف پول یا صرافی‌های معتبر، سرمایه کاربران را پس از واریز به سرقت می‌برند.

ویژگی‌ها و نشانه‌ها

- نام و آیکون مشابه با برنامه‌های معتبر در فروشگاه‌های نرم‌افزاری
- عدم وجود پشتیبانی یا پاسخگویی واقعی
- دریافت ناگهانی یا مسدود شدن دارایی پس از واریز

مثال واقعی

در سال ۲۰۲۰ صدها نسخه جعلی از اپلیکیشن کیف پول "ترزور (Trezor) "در گوگل پلی منتشر شد و بسیاری از کاربران دارایی خود را از دست دادند.

۲.۶ بدافزارها و حملات هکری

تعریف

بدافزارها برنامه‌های مخربی هستند که برای سرقت اطلاعات رمزارزی یا کنترل کیف پول کاربران طراحی می‌شوند. همچنین، حملات هکری به صرافی‌ها یکی از دلایل اصلی از دست رفتن دارایی کاربران است.

ویژگی‌ها و نشانه‌ها

- دانلود نرم‌افزار از منابع غیررسمی
- آلوده شدن سیستم به ویروس و برنامه‌های جاسوسی
- هک شدن صرافی‌ها و سرقت گسترده دارایی‌ها

مثال واقعی

در سال ۲۰۱۴ صرافی معروف "Mt.Gox" مورد حمله هکری قرار گرفت و بیش از ۴۰۰ هزار بیت‌کوین سرقت شد.

۲.۷ سوءاستفاده از شبکه‌های اجتماعی و تبلیغات فریبنده

تعریف

کلاهبرداران با استفاده از تبلیغات در شبکه‌های اجتماعی، جلب اعتماد از طریق صفحات اینفلوئنسرها یا حتی جعل حساب افراد مشهور، کاربران را به سرمایه‌گذاری در پروژه‌های کاذب ترغیب می‌کنند.

ویژگی‌ها و نشانه‌ها

- تبلیغات وعده سود سریع و بدون ریسک
- درخواست ارسال ارز به آدرس مشخص برای دریافت جایزه یا دو برابر شدن دارایی
- کامنت‌ها و نظرات جعلی برای افزایش اعتبار پروژه

مثال واقعی

در سال ۲۰۲۰، توییتر حساب کاربری ایلان ماسک، بیل گیتس و چند چهره سرشناس دیگر هک شد و پیام‌هایی منتشر شد که کاربران را به ارسال بیت‌کوین به آدرس خاصی دعوت می‌کرد. هزاران نفر قربانی شدند.

۲.۸ پروژه‌های جعلی عرضه اولیه(Fake ICO & Token Sales)

تعریف

در دوران رونق عرضه اولیه سکه(ICO) ، پروژه‌های جعلی با سایت و وایت‌پیپر جذاب، اقدام به جمع‌آوری سرمایه کردند و پس از جذب پول، پروژه تعطیل شد.

ویژگی‌ها و نشانه‌ها

- نبود اطلاعات کافی درباره تیم و پروژه
- سایت و وایت‌پیپر حرفه‌ای اما بدون سابقه مشخص
- وعده‌های مبهم و اغراق‌آمیز درباره آینده پروژه

مثال واقعی

پروژه "Pincoin" در ویتنام پس از جذب ۶۶۰ میلیون دلار سرمایه، ناگهان تعطیل شد و تیم سازنده ناپدید گردید.

۲.۹ طرح‌های پامپ و دامپ(Pump & Dump Schemes)

تعریف

در این روش، گروهی با تبلیغات گسترده یا هماهنگی، قیمت یک توکن بی‌ارزش را به طور مصنوعی افزایش می‌دهند. پس از جذب سرمایه افراد ناآگاه، به‌سرعت اقدام به فروش دارایی و ریزش شدید قیمت می‌کنند.

ویژگی‌ها و نشانه‌ها

- تبلیغات ناگهانی و غیرعادی درباره یک توکن خاص
- افزایش سریع و غیرمنطقی قیمت در مدت کوتاه
- سقوط قیمت بلافاصله پس از اوج گرفتن

مثال واقعی

در سال‌های اخیر بارها توکن‌های ناشناخته در گروه‌های تلگرامی پامپ شده و پس از چند ساعت قیمت آنها سقوط کرده است.

۲.۱۰ NFT اسکم و پروژه‌های جعلیNFT

تعریف

با رونق بازارNFT ، کلاهبرداران اقدام به ساخت NFT جعلی، فروش آثار هنری کپی یا پروژه‌های فاقد پشتوانه می‌کنند.

ویژگی‌ها و نشانه‌ها

- فروش NFT از هنرمندان بدون اجازه یا اعتبار
- وعده سود کلان از خرید و فروشNFT
- پروژه‌های بدون برنامه مشخص یا نقشه راه واقعی

مثال واقعی

در سال ۲۰۲۱، بسیاری ازNFT های جعلی با استفاده از آثار هنری دزدی فروخته شد و خریداران متضرر شدند.

جمع‌بندی فصل دوم

در این فصل با مهم‌ترین و رایج‌ترین انواع کلاهبرداری در بازار رمزارز آشنا شدیم. نکته کلیدی این است که شیوه‌های کلاهبرداری همواره در حال تغییر و به‌روزرسانی است و آگاهی، نخستین گام برای محافظت از دارایی دیجیتال شماست.
در فصل‌های بعدی هر یک از این روش‌ها با جزئیات و مثال‌های عمیق‌تر تحلیل خواهند شد تا راه‌های شناسایی و مقابله با آن‌ها را بیاموزید.

پرسش و پاسخ فصل دوم

۱ .**پرسش:**
چرا طرح پانزی و هرمی در بازار رمزارزها محبوبیت زیادی دارد؟
پاسخ:
به دلیل وعده سود سریع، نبود قانون‌گذاری دقیق و سهولت جذب افراد جدید، این طرح‌ها به‌راحتی قربانیان زیادی پیدا می‌کنند.

۲ .**پرسش:**
مهم‌ترین نشانه‌های یک پروژه اسکم یا راگ‌پول چیست؟
پاسخ:

تبلیغات اغراق‌آمیز، تیم ناشناس، نبود قفل نقدینگی، و حذف ناگهانی کانال‌های ارتباطی از نشانه‌های مهم این نوع پروژه‌ها هستند.

۳ .**پرسش:**
چرا فیشینگ در رمزارزها خطرناک‌تر از بانک‌هاست؟
پاسخ:
چون تراکنش‌های رمزارزی برگشت‌ناپذیر هستند و افشای کلید خصوصی می‌تواند به سرقت کل دارایی منجر شود.

تمرین عملی فصل دوم

۱ .**تشخیص پروژه مشکوک:**
به یک پروژه رمزارزی در شبکه‌های اجتماعی برخورد کرده‌اید که وعده سود ماهانه ۲۰ درصدی می‌دهد. مراحل بررسی و تصمیم‌گیری خود را بنویسید.

۲ .**تحلیل یک نمونه واقعی:**
داستان یک قربانی پروژه اسکم را در اینترنت جستجو و خلاصه کنید:

- پروژه چه وعده‌هایی داد؟
- نشانه‌های هشدار چه بود؟
- چگونه می‌توانست از این کلاهبرداری جلوگیری کند؟

۳ .**ساخت چک‌لیست امنیتی:**
یک چک‌لیست برای بررسی اعتبار یک پروژه رمزارزی تهیه کنید (حداقل ۵ معیار مهم).

جدول مقایسه‌ای: تفاوت پانزی، هرمی، و راگ پول

راگ پول(Rug Pull)	طرح هرمی(Pyramid)	طرح پانزی(Ponzi)	ویژگی
جذب سرمایه و خروج ناگهانی	با جذب زیرمجموعه	از پول افراد جدید	مدل سود
غالباً محصول یا توکن جدید	ممکن است محصولی جعلی داشته باشد	غالباً بی‌محصول	نقش محصول
نه، فقط جذب سرمایه	بله، سود با جذب افراد	نه، سود با جذب سرمایه	نیاز به عضوگیری
خروج ناگهانی سازندگان	فروپاشی هرم	فرار بنیان‌گذار	نحوه پایان

جمع‌بندی تصویری

در یک نگاه، به خاطر بسپارید:

- **هیچ وعده سود تضمینی در بازار رمزارز واقعی نیست.**
- **همیشه پیش از سرمایه‌گذاری، پروژه را به‌دقت بررسی کنید.**
- **از منابع و افراد معتبر مشورت بگیرید.**

فصل سوم: طرح پانزی — (Ponzi Scheme) فریب با وعده سود تضمینی

Ponzi Schemes: The Illusion of Guaranteed Profits

۳.۱ تعریف طرح پانزی و تاریخچه آن

طرح پانزی، نام خود را از یک کلاهبردار ایتالیایی به نام **چارلز پانزی (Charles Ponzi)** گرفته است که در سال ۱۹۲۰ میلادی در آمریکا با وعده سودهای خارق‌العاده، هزاران نفر را فریب داد. در این مدل کلاهبرداری، سود پرداختی به سرمایه‌گذاران قدیمی از پول افراد جدید تأمین می‌شود و نه از یک فعالیت اقتصادی واقعی. این روند تا زمانی ادامه می‌یابد که جذب سرمایه‌گذاران جدید ادامه داشته باشد؛ اما با توقف ورودی‌ها، سیستم فرو می‌پاشد و اکثر افراد متضرر می‌شوند.

ویژگی اصلی:
در طرح پانزی، هیچ فعالیت واقعی و سودآوری در پس‌زمینه وجود ندارد و تنها با چرخش پول سرمایه‌گذاران جدید، به افراد قبلی سود داده می‌شود.

۳.۲ ساختار و مراحل اجرای یک طرح پانزی

۱. **راه‌اندازی یک ظاهر فریبنده:**
معمولاً یک شرکت یا پلتفرم رمزارزی با سایت و بروشور حرفه‌ای راه‌اندازی می‌شود.

۲. **وعده سودهای ثابت و بالا:**
به سرمایه‌گذاران وعده داده می‌شود که مثلاً ماهانه ۱۰ تا ۳۰ درصد سود ثابت دریافت خواهند کرد؛ بدون هیچ ریسک و با تضمین بازگشت اصل پول.

۳. **پرداخت سود اولیه به سرمایه‌گذاران:**
افراد اولیه سود وعده‌داده‌شده را دریافت می‌کنند و با دیدن این سود، مبلغ بیشتری سرمایه‌گذاری یا دیگران را نیز دعوت می‌کنند.

4. **تبلیغات دهان‌به‌دهان و شبکه‌ای:**
با رشد اعتماد، افراد بیشتری جذب می‌شوند و چرخهٔ ورودی پول جدید ادامه می‌یابد.

5. **فروپاشی طرح:**
زمانی که جذب سرمایه‌گذاران جدید متوقف شود یا تعداد برداشت‌ها زیاد شود، بنیان‌گذار طرح پول‌ها را جمع‌آوری کرده و ناپدید می‌شود.

۳.۳ چرا مردم جذب طرح‌های پانزی می‌شوند؟

- **طمع سود کلان و آسان**
- **نمونه‌های جعلی موفقیت(Testimonials)**
- **نداشتن دانش مالی و تکنولوژیک کافی**
- **اعتماد به دوستان یا آشنایان (شبکه‌سازی انسانی)**
- **استفاده از زبان فنی و اصطلاحات پیچیده برای فریب دادن افراد مبتدی**

۳.۴ نشانه‌های هشداردهنده یک طرح پانزی

- وعده سود تضمینی و بسیار بالا
- عدم شفافیت در مدل درآمدی و فعالیت واقعی
- فشار برای عضوگیری و جذب سرمایه‌گذار جدید
- عدم وجود اطلاعات معتبر درباره تیم و مدیران
- مجوزهای ساختگی یا ناشناس بودن محل فعالیت شرکت
- نبود قرارداد یا قراردادهای مبهم و غیرحرفه‌ای

۳.۵ نمونه‌های واقعی طرح پانزی در بازار رمزارز

مثال ۱PlusToken :

یک کیف پول رمزارزی که بیش از دو میلیارد دلار سرمایه جذب کرد و با وعده سود ماهانه بالا، هزاران نفر را فریب داد. پس از مدتی بنیان‌گذاران ناپدید شدند و سرمایه‌ها از بین رفت.

مثال ۲BitConnect :

این پروژه با وعده سودهای خارق‌العاده، سرمایه زیادی جذب کرد. پس از رشد چشمگیر قیمت توکن اختصاصی خود(BCC) ، ناگهان فروپاشید و سرمایه‌گذاران ضرر هنگفتی کردند.

مثال ۳Mining Max :

این طرح با شعار استخراج رمزارز و تضمین سود ماهانه، حدود ۲۵۰ میلیون دلار جذب کرد و پس از مدتی فعالیت، تمامی سایت‌ها و حساب‌ها را بستند و متواری شدند.

۳.۶ چگونه طرح پانزی رمزارزی را تشخیص دهیم؟

۱ .**بررسی شفافیت مدل درآمدی:**
آیا پروژه دقیقاً توضیح می‌دهد چگونه سود را تولید می‌کند یا فقط به وعده‌ها بسنده می‌کند؟

۲ .**تحقیق درباره تیم و سوابق آنان:**
وجود تیم ناشناس یا افراد بدون سابقه معتبر یک علامت خطر جدی است.

۳ .**عدم وجود محصول یا خدمت واقعی:**
اگر پروژه فقط وعده سود می‌دهد و محصولی وجود ندارد، به احتمال زیاد طرح پانزی است.

۴ .**خواندن نقد و نظرات کاربران در انجمن‌ها:**
بررسی نظرهای کاربران در سایت‌هایی مثل Reddit یا Bitcointalk می‌تواند هشدارهای جدی به شما بدهد.

۵ .**پرهیز از اعتماد به اثبات پرداخت:(Payment Proofs)**
این اسناد به راحتی قابل جعل هستند و نباید ملاک قرار گیرند.

۳.۷ نقش قانون و پلیس در مقابله با طرح‌های پانزی

در بسیاری از کشورها، طرح پانزی جرم محسوب می‌شود. با این حال، در فضای رمزارزها به دلیل ناشناس بودن تراکنش‌ها و نبود قانون‌گذاری جامع، پیگیری و دستگیری مجرمان بسیار دشوار است. بنابراین بهترین راه، **آگاهی و پیشگیری** است، نه امید به بازگرداندن سرمایه پس از وقوع جرم.

۳.۸ مسئولیت اخلاقی و اجتماعی

افرادی که با علم یا بی‌اطلاعی، دیگران را به این طرح‌ها دعوت می‌کنند، مسئولیت اخلاقی سنگینی دارند. اگر سود شما از ورود افراد جدید تأمین می‌شود، احتمالاً در یک طرح پانزی هستید even—اگر خودتان سود بگیرید، در نهایت گروه زیادی متضرر می‌شوند.

پرسش و پاسخ فصل سوم

۱ .**پرسش:**
چگونه می‌توان به صحت ادعای یک پروژه رمزارزی درباره سود ماهانه پی برد؟
پاسخ:
باید مدل درآمدی پروژه، محصول واقعی، و شفافیت مالی آن را دقیقاً بررسی کنید؛ اگر تنها منبع درآمد، پول افراد جدید باشد، نشانه طرح پانزی است.

۲ .**پرسش:**
آیا همیشه ارائه پرداخت‌های اولیه نشانه مشروعیت طرح است؟
پاسخ:
خیر، پرداخت اولیه معمولاً با پول ورودی افراد جدید تأمین می‌شود و نشانه مشروعیت نیست.

۳ .**پرسش:**
چه اقداماتی برای پیشگیری از گرفتار شدن در طرح پانزی موثر است؟

پاسخ:
آموزش، تحقیق درباره تیم، پرسیدن سؤال‌های دقیق درباره مدل درآمدی، و پرهیز از طمع سودهای غیرمنطقی.

تمرین عملی فصل سوم

۱ .**تحلیل پروژه:**
یک پروژه رمزارزی با وعده سود ماهانه ۱۵ درصد به شما معرفی شده است. پنج سؤال کلیدی که باید قبل از سرمایه‌گذاری بپرسید را بنویسید.

۲ .**مطالعه موردی:**
داستان یکی از قربانیان PlusToken یا BitConnect را در اینترنت جستجو کنید و بنویسید چه عواملی باعث شد او فریب بخورد و چگونه می‌توانست از این خطر پیشگیری کند.

۳ .**شبیه‌سازی گفتگو:**
فرض کنید دوست شما قصد دارد شما را به یک پروژه با سود تضمینی دعوت کند. با چه دلایل منطقی و شواهدی می‌توانید او را از این کار منصرف کنید؟

جدول مقایسه‌ای: طرح پانزی با سایر مدل‌های کلاهبرداری

ویژگی	طرح پانزی(Ponzi)	هرمی(Pyramid)	راگ پول(Rug Pull)
نحوه جذب سرمایه	وعده سود تضمینی	جذب زیرمجموعه	فروش توکن یا محصول جعلی
مدل پرداخت سود	پول افراد جدید	پول افراد جدید	وجود ندارد
محصول یا خدمت واقعی	ندارد	ممکن است جعلی باشد	ندارد یا کاملاً صوری
نحوه پایان	توقف ورودی جدید	فروپاشی هرم	خروج ناگهانی تیم

ویژگی	طرح پانزی(Ponzi)	هرمی(Pyramid)	راگ پول(Rug Pull)
ریسک قربانی شدن	بسیار بالا	بسیار بالا	بسیار بالا

جمع‌بندی تصویری فصل سوم

- هر وعده سود ثابت و بالاتر از عرف بازار، هشدار جدی است.
- فریب پرداخت اولیه را نخورید؛ منبع این پول افراد تازه‌وارد است.
- قبل از هر سرمایه‌گذاری، به مدل درآمدی، محصول واقعی و تیم توسعه‌دهنده توجه ویژه داشته باشید.
- مسئولیت اخلاقی خود را در دعوت دیگران به پروژه‌های مشکوک جدی بگیرید.

فصل چهارم: طرح‌های هرمی — (Pyramid Schemes) فریب در قالب شبکه

Pyramid Schemes: Deception in the Name of Networking

۴.۱ تعریف و ماهیت طرح‌های هرمی

طرح هرمی (Pyramid Scheme) نوعی کلاهبرداری است که ساختار آن به صورت یک هرم سازمانی طراحی می‌شود. افراد جدید برای ورود به سیستم باید مبلغی پرداخت کنند و پس از ورود، تشویق می‌شوند تا با جذب افراد دیگر، از ورود اعضای جدید سود دریافت کنند.
در این مدل، سود به جای فعالیت اقتصادی واقعی یا تولید محصول، صرفاً از ورودی اعضای جدید تأمین می‌شود. هرچه به رأس هرم نزدیک‌تر باشید، شانس بیشتری برای دریافت سود دارید و هرچه پایین‌تر باشید، بیشتر در معرض ضرر قرار می‌گیرید.

۴.۲ تفاوت طرح هرمی با طرح پانزی

اگرچه هر دو مدل بر پایه جذب سرمایه افراد جدید و وعده سود کلان طراحی شده‌اند، اما تفاوت‌های کلیدی دارند:

ویژگی	طرح پانزی(Ponzi)	طرح هرمی(Pyramid)
نحوه عضوگیری	معمولاً مرکزی و از سوی یک نفر انجام می‌شود	هر عضو موظف به عضوگیری است
پرداخت سود	مرکزی و به همه پرداخت می‌شود	توسط اعضا و به صورت لایه‌لایه
تأکید اصلی	وعده سود مالی	عضوگیری بیشتر و گسترش شبکه
وجود محصول	معمولاً بی‌محصول	گاهی محصول جعلی یا کم‌ارزش

۴.۳ ساختار اجرایی یک طرح هرمی

۱ .**شروع با یک هسته مرکزی:**
معمولاً یک نفر یا گروه کوچک به عنوان "بنیان‌گذار" هرم در رأس قرار می‌گیرند.

2. **ورود افراد جدید با پرداخت مبلغ:**
افراد برای ورود به هرم، مبلغی را به عنوان سرمایه‌گذاری یا خرید محصول (غالباً بی‌ارزش) پرداخت می‌کنند.

3. **تشویق به عضوگیری:**
هر عضو با هدف دریافت سود یا پورسانت بیشتر، افراد جدیدی را به سیستم معرفی می‌کند.

4. **توزیع سود در سطوح مختلف:**
بخشی از پول اعضای جدید به اعضای سطوح بالاتر اختصاص می‌یابد و با رشد هرم، افراد بالاتر درآمد بیشتری کسب می‌کنند.

5. **فروپاشی هرم:**
با اشباع بازار و توقف ورود اعضای جدید، پرداخت سود به اعضای پایین‌تر ممکن نمی‌شود و اکثریت اعضا دچار ضرر جدی می‌شوند.

۴.۴ چرا طرح‌های هرمی جذاب به نظر می‌رسند؟

- **وعده استقلال مالی و درآمد غیرفعال**
- **ادعای آموزش حرفه‌ای، محصول نوآورانه یا خدمات استثنایی**
- **استفاده از عبارات انگیزشی و موفقیت‌محور**
- **برگزاری سمینارها و وبینارهای انگیزشی با افراد مشهور یا موفق ساختگی**
- **ایجاد حس تعلق به یک جامعه یا خانواده بزرگ**

۴.۵ مدل‌های جدید طرح‌های هرمی در بازار رمزارزها

در سال‌های اخیر، کلاهبرداران برای تطبیق با فضای رمزارز و جلب اعتماد بیشتر، طرح‌های هرمی را با عناوینی مانند «ماینینگ ابری»، «ترید گروهی»، «پلتفرم آموزشی»، «عرضه اولیه توکن»، یا حتی NFT ارائه می‌کنند.
نمونه‌هایی از این مدل‌ها:

- **طرح‌های استخراج ابری:(Cloud Mining)**
  افراد با پرداخت مبلغی، به ظاهر در سود استخراج رمزارز شریک می‌شوند اما سود تنها از پول ورودی اعضای جدید تأمین می‌شود.
- **پلتفرم‌های آموزشی با پورسانت عضوگیری:**
  محصول اصلی آموزش‌های بی‌ارزش یا تکراری است و ساختار مالی بر پایه عضوگیری می‌چرخد.
- **توکن یاNFT های فاقد پشتوانه:**
  فروش توکن یا NFT فقط برای جذب سرمایه و جذب افراد بیشتر است و محصول واقعی یا ارزش افزوده وجود ندارد.

۴.۶ نشانه‌های هشداردهنده یک طرح هرمی رمزارزی

- تأکید افراطی بر عضوگیری و کسب درآمد از زیرمجموعه
- تبلیغ درآمد غیرفعال و زندگی لوکس با ورود به طرح
- فروش محصولاتی که قیمت آنها غیرواقعی یا صرفاً بهانه‌ای برای عضوگیری است
- نبود شفافیت مالی و گزارش‌های درآمدی واقعی
- ارائه قراردادهای مبهم یا صرفاً دعوت‌نامه‌های شفاهی
- تشویق به «همه چیز را به دوستان و خانواده بگو«!

۴.۷ مثال‌های واقعی طرح هرمی در بازار رمزارز

مثال ۱BitClub Network :

یک شبکه استخراج بیت‌کوین که با وعده سود بالا و عضویت در شبکه ماینینگ، هزاران نفر را فریب داد و پس از جذب چندصد میلیون دلار سرمایه، مؤسسان آن بازداشت شدند.

مثال ۲OneCoin :

یکی از بزرگ‌ترین طرح‌های هرمی رمزارزی در تاریخ، با وعده یک رمزارز جهانی و سودهای خارق‌العاده، بیش از چهار میلیارد دلار سرمایه از مردم جهان جذب کرد و پس از چند سال، گردانندگان آن تحت تعقیب قرار گرفتند.

مثال ۳: پروژه‌های آموزشی با پورسانت بالا

در ایران و بسیاری کشورها، پروژه‌هایی با عناوین «آموزش ترید»، «کسب درآمد دلاری» یا «فروش توکن انحصاری» با مدل هرمی فعال شدند که در نهایت، اکثریت اعضای جدید ضرر کردند.

۴.۸ پیامدهای حقوقی و اجتماعی طرح‌های هرمی

در بسیاری از کشورها، فعالیت در طرح هرمی جرم بوده و شرکت‌کنندگان آن حتی اگر سود کرده باشند، تحت پیگرد قرار می‌گیرند.
پیامدهای اجتماعی این طرح‌ها شامل از دست رفتن اعتماد عمومی، خسارت مالی گسترده و آسیب به روابط خانوادگی و دوستانه است.

۴.۹ راهکارهای شناسایی و مقابله با طرح‌های هرمی

۱ .**پرسش از مدل درآمدی واقعی:**
اگر درآمد شما فقط از عضوگیری تأمین می‌شود، به احتمال زیاد در یک طرح هرمی قرار دارید.

۲ .**بررسی محصول یا خدمت ارائه شده:**
آیا محصولی واقعی، کاربردی و با قیمت معقول وجود دارد یا فقط بهانه‌ای برای عضوگیری است؟

۳ .**پرهیز از تبلیغات اغراق‌آمیز و وعده سودهای آسان:**
هر طرحی که وعده درآمد غیرمنطقی یا بدون ریسک بدهد، مشکوک است.

۴ .**تحقیق درباره مجوز و سوابق شرکت:**
اغلب طرح‌های هرمی فاقد مجوز معتبر یا سابقه فعالیت شفاف هستند.

۵ .**مشورت با افراد آگاه و منابع معتبر:**
پیش از ورود، با کارشناسان حوزه رمزارز یا مشاوران حقوقی مشورت کنید.

پرسش و پاسخ فصل چهارم

۱ .**پرسش:**
تفاوت اصلی بین طرح هرمی و یک کسب‌وکار بازاریابی شبکه‌ای مشروع چیست؟
پاسخ:
در کسب‌وکار مشروع، محصول واقعی و قیمت منصفانه وجود دارد و درآمد عمدتاً از فروش محصول است، نه صرفاً عضوگیری. اما در طرح هرمی درآمد صرفاً از ورود افراد جدید تأمین می‌شود.

۲ .**پرسش:**
چرا اغلب افراد تازه‌وارد قربانی طرح‌های هرمی می‌شوند؟
پاسخ:
به دلیل تبلیغات فریبنده، فشار دوستان و عدم آگاهی کافی از ساختار کلاهبرداری، افراد جدید جذب این طرح‌ها می‌شوند.

۳ .**پرسش:**
آیا شرکت در طرح هرمی حتی با سودآوری، کار قانونی و اخلاقی است؟
پاسخ:
خیر، حتی اگر سود کنید، مسئولیت حقوقی و اخلاقی به دلیل ضرر دیگران متوجه شما خواهد بود.

تمرین عملی فصل چهارم

۱ .**بررسی یک پروژه:**
یک پروژه رمزارزی با تبلیغ «درآمد دلاری بدون تخصص» و تأکید بر جذب زیرمجموعه را شناسایی کنید. حداقل سه نشانه مشکوک در آن بیابید.

۲ .**شبیه‌سازی گفت‌وگو:**
یکی از دوستان شما قصد دارد شما را به یک شبکه بازاریابی رمزارزی دعوت کند. چه سؤالاتی می‌پرسید تا مطمئن شوید این پروژه هرمی نیست؟

۳ .**مطالعه موردی:**
داستان شکست یک پروژه هرمی رمزارزی) مانند (OneCoin را بخوانید و بنویسید چگونه قربانیان می‌توانستند از ضرر جلوگیری کنند.

جدول مقایسه‌ای: طرح هرمی، پانزی و کسب‌وکار بازاریابی شبکه‌ای مشروع

ویژگی	طرح هرمی(Pyramid)	طرح پانزی(Ponzi)	بازاریابی شبکه‌ای مشروع
مدل درآمدی	عضوگیری بیشتر	جذب سرمایه جدید	فروش محصول واقعی
وجود محصول	معمولاً بی‌ارزش یا جعلی	ندارد	واقعی و باکیفیت
منبع سود	ورودی اعضای جدید	ورودی سرمایه‌گذاران	فروش و خدمات
وضعیت قانونی	غیرقانونی	غیرقانونی	قانونی (با شرایط خاص)
دوام سیستم	کوتاه‌مدت، فروپاشی سریع	کوتاه‌مدت	بلندمدت (در صورت مشروعیت)

جمع‌بندی تصویری فصل چهارم

- هیچ طرحی که تأکید اصلی‌اش جذب زیرمجموعه و وعده درآمد آسان باشد، سالم نیست.

- محصول یا خدمت واقعی با قیمت منصفانه، نشانه مشروعیت کسب‌وکار است.
- تحقیق و پرسش از منابع معتبر قبل از هرگونه عضویت، حیاتی است.
- سود شما در طرح هرمی به ضرر دیگران منتهی می‌شود و مسئولیت اخلاقی و حقوقی دارد.

فصل پنجم: پروژه‌های اسکم و راگ‌پول – خروج ناگهانی بنیان‌گذاران

Rug Pull & Exit Scam: When Founders Vanish Overnight

۵.۱ تعریف پروژه‌های اسکم و راگ‌پول

در دنیای رمزارزها، یکی از رایج‌ترین روش‌های کلاهبرداری، راه‌اندازی پروژه‌های ظاهراً نوآورانه و جذاب است که پس از جذب سرمایه قابل توجه از سرمایه‌گذاران، بنیان‌گذاران یا توسعه‌دهندگان پروژه به طور ناگهانی ناپدید می‌شوند و سرمایه را با خود می‌برند.
این نوع کلاهبرداری‌ها به دو شکل اصلی دیده می‌شوند:

- **راگ‌پول:(Rug Pull)**
بنیان‌گذاران یا تیم توسعه، پس از جمع‌آوری سرمایه یا تزریق نقدینگی، به طور ناگهانی کل دارایی موجود در قرارداد هوشمند یا صرافی غیرمتمرکز را خارج می‌کنند.
- **اسکم خروج:(Exit Scam)**
معمولاً در پروژه‌های عرضه اولیه(ICO/IDO) ، پس از فروش توکن‌ها و جمع‌آوری سرمایه، تیم پروژه سایت و تمام راه‌های ارتباطی را حذف کرده و هیچ محصول یا سرویس واقعی ارائه نمی‌شود.

۵.۲ مراحل اجرای یک پروژه اسکم یا راگ‌پول

۱ .**ایجاد یک پروژه ظاهراً جذاب:**
راه‌اندازی سایت حرفه‌ای، طراحی وایت‌پیپر، وعده نوآوری و آینده‌نگری در رمزارز.

۲ .**تبلیغات گسترده و هیجان‌انگیز:**
استفاده از شبکه‌های اجتماعی، اینفلوئنسرها و تبلیغات گسترده برای جلب اعتماد سرمایه‌گذاران.

3. **تشویق به خرید توکن یا سرمایه‌گذاری:**
عرضه توکن‌های جدید، وعده رشد قیمت سریع یا سودهای استثنایی.

4. **جذب سرمایه یا تزریق نقدینگی:**
جمع‌آوری مبالغ هنگفت از کاربران یا افزودن نقدینگی به صرافی غیرمتمرکز.

5. **خروج ناگهانی:**
برداشت کل سرمایه از قرارداد هوشمند یا حساب‌های پروژه و قطع همه راه‌های ارتباطی.
قیمت توکن یا ارزش دارایی صفر می‌شود و کاربران متضرر می‌گردند.

۵.۳ انواع رایج پروژه‌های اسکم و راگ‌پول در رمزارزها

الف (توکن‌ها و کوین‌های جدید بدون پشتوانه

بسیاری از پروژه‌ها با تبلیغ یک توکن جدید و ایجاد داستان‌های فریبنده (مانند پروژه با هدف کمک به محیط زیست یا حمایت از فقرا)، سرمایه‌گذاران را جذب کرده و پس از فروش توکن‌ها، بازار را رها می‌کنند.

ب (پروژه‌های DeFi و Yield Farming اسکم

پروتکل‌های مالی غیرمتمرکز که وعده سودهای غیرواقعی می‌دهند و با جمع‌آوری نقدینگی، ناگهان دارایی‌ها را خارج می‌کنند.

ج NFT (و GameFi اسکم

پروژه‌های بازی یا فروش NFT که با وعده سود یا ارزش افزوده بالا، کاربران را جذب کرده و پس از جمع‌آوری پول، سایت و سرورها را از دسترس خارج می‌کنند.

د (پروژه‌های عرضه اولیه (ICO/IDO جعلی

ایجاد توکن و فروش اولیه به هزاران نفر با تبلیغات فراوان، بدون ارائه محصول یا برنامه واقعی و در نهایت خروج تیم پروژه.

۵.۴ نشانه‌های هشداردهنده یک پروژه اسکم یا راگ‌پول

- **تیم ناشناس یا بدون سابقه:**
عدم وجود اطلاعات معتبر درباره بنیان‌گذاران یا توسعه‌دهندگان.
- **عدم قفل نقدینگی:(Liquidity Lock)**
نبود تضمین برای باقی ماندن نقدینگی در قرارداد هوشمند یا صرافی غیرمتمرکز.
- **کدهای قرارداد هوشمند بسته یا غیربازرسی‌شده:**
نبود شفافیت و Audit برای کدها و قراردادها.
- **تبلیغات اغراق‌آمیز و وعده سود نجومی:**
استفاده از اینفلوئنسرهای نامعتبر و جو هیجان کاذب.
- **نداشتن نقشه راه یا برنامه توسعه واقعی:**
فقط یک وایت‌پیپر تکراری یا مبهم وجود دارد و هیچ نشانه‌ای از پیشرفت پروژه دیده نمی‌شود.
- **حجم معاملات غیرواقعی یا رشد غیرعادی قیمت توکن:**
پامپ مصنوعی قیمت و نمایش حجم معاملات جعلی برای جلب اعتماد.
- **حذف ناگهانی وب‌سایت، کانال‌های ارتباطی یا محدود شدن برداشت‌ها:**
اولین نشانه‌های خروج و فروپاشی پروژه.

۵.۵ مثال‌های واقعی پروژه‌های اسکم و راگ‌پول

مثال ۱(Squid Game Token (SQUID) :

این توکن با الهام از سریال محبوب نتفلیکس به سرعت رشد کرد و هزاران نفر با وعده رشد قیمت خارق‌العاده سرمایه‌گذاری کردند. پس از مدت کوتاهی، توسعه‌دهندگان کل نقدینگی را برداشتند و قیمت توکن به صفر رسید. سرمایه‌گذاران دسترسی به تیم یا حتی امکان فروش توکن خود را از دست دادند.

مثال ۲AnubisDAO :

پروژه دیفای AnubisDAO در سال ۲۰۲۱ تنها چند ساعت پس از جمع‌آوری ۶۰ میلیون دلار نقدینگی، بنیان‌گذاران دارایی‌ها را از قرارداد خارج کردند و ناپدید شدند.

مثال ۳Meerkat Finance :

پروژه Yield Farming روی زنجیره هوشمند باینس (BSC) که پس از جمع‌آوری بیش از ۳۰ میلیون دلار، به طور ناگهانی وب‌سایت و کانال‌های ارتباطی را بست و همه دارایی‌ها را سرقت کرد.

۵.۶ روش‌های پیشگیری و مقابله با پروژه‌های اسکم و راگ‌پول

۱ .**بررسی تیم و سوابق توسعه‌دهندگان:**
هرگز در پروژه‌هایی با تیم ناشناس یا بدون سابقه روشن سرمایه‌گذاری نکنید.

۲ .**بررسی قرارداد هوشمند و:Audit**
فقط پروژه‌هایی که قرارداد آن‌ها توسط شرکت‌های معتبر Auditing بررسی و منتشر شده را انتخاب کنید.

۳ .**اطمینان از قفل نقدینگی:(Liquidity Lock)**
بررسی کنید که نقدینگی پروژه حداقل برای مدت معقولی قفل شده باشد و امکان برداشت ناگهانی وجود نداشته باشد.

۴ .**مطالعه وایت‌پیپر و نقشه راه پروژه:**
از کلی‌گویی، وعده‌های نامعقول و عدم شفافیت بپرهیزید.

۵ .**بررسی حجم معاملات و رشد قیمت:**
افزایش سریع و غیرمنطقی قیمت توکن معمولاً نشانه پامپ مصنوعی است.

۶ .**دوری از پروژه‌های صرفاً تبلیغاتی و وابسته به جو هیجان:**
هیجان بازار، مهم‌ترین ابزار کلاهبرداران است؛ همیشه تحلیل منطقی داشته باشید.

۷ .**مشاوره با افراد آگاه و بررسی نظرات کاربران:**
نظرات کاربران و کارشناسان در سایت‌هایی مانندReddit ، Bitcointalkو توییتر می‌تواند زنگ خطرها را برای شما به صدا درآورد.

پرسش و پاسخ فصل پنجم

۱ .**پرسش:**
نشانه کلیدی یک پروژه راگ‌پول چیست؟
پاسخ:
قفل نبودن نقدینگی، تیم ناشناس، و تبلیغات اغراق‌آمیز از نشانه‌های کلیدی یک پروژه راگ‌پول است.

۲ .**پرسش:**
آیا Audit قرارداد هوشمند به تنهایی برای اطمینان کافی است؟
پاسخ:
خیر، علاوه بر Audit باید به سابقه تیم، قفل نقدینگی و شفافیت پروژه نیز توجه کرد.

۳ .**پرسش:**
چرا پروژه‌های اسکم معمولاً با سرعت و هیجان زیاد تبلیغ می‌شوند؟
پاسخ:
ایجاد جو هیجان و FOMO (ترس از دست دادن) باعث می‌شود افراد بدون تحقیق کافی سرمایه‌گذاری کنند.

تمرین عملی فصل پنجم

۱ .**تحلیل پروژه:**
پروژه‌ای با توکن جدید و وعده رشد ۱۰۰۰ درصدی در یک ماه را مشاهده کرده‌اید.

- پنج معیار مهم برای ارزیابی ریسک این پروژه را بنویسید.

۲ .**مطالعه موردی:**
یکی از پروژه‌های اسکم یا راگ‌پول) مانند Squid Game Token یا (Meerkat Finance را در اینترنت جستجو کنید و پاسخ دهید:

- نشانه‌های هشداردهنده چه بود؟
- سرمایه‌گذاران چگونه می‌توانستند از این پروژه دوری کنند؟

۳ .**چک‌لیست پیشگیری:**
یک چک‌لیست پنج‌گانه برای بررسی امنیت پروژه‌های رمزارزی بنویسید.

جدول مقایسه‌ای: پروژه‌های اسکم، راگ‌پول و ICO قانونی

ویژگی	پروژه اسکم(Scam)	راگ‌پول(Rug Pull)	ICOقانونی(Legal ICO)
شفافیت تیم	ندارد	ندارد یا جعلی	شفاف و قابل بررسی
قفل نقدینگی	ندارد	ندارد یا کوتاه‌مدت	معمولاً دارد
قرارداد هوشمندAudit	ندارد	معمولاً ندارد	معمولاً دارد
محصول یا برنامه واقعی	ندارد	ندارد یا صوری	دارد و قابل پیگیری
رشد قیمت	انفجاری و ساختگی	ناگهانی و اغراق‌آمیز	معقول و تدریجی
امکان پیگیری حقوقی	عملاً غیرممکن	عملاً غیرممکن	تا حدی امکان‌پذیر

جمع‌بندی تصویری فصل پنجم

- هر پروژه‌ای که تیم و نقشه راه شفاف ندارد و وعده رشد انفجاری می‌دهد، احتمالاً اسکم یا راگ‌پول است.
- قفل نقدینگی، قرارداد هوشمند باز وAudit شده، و سابقه تیم توسعه‌دهنده از مهم‌ترین معیارهای امنیت سرمایه‌گذاری هستند.
- جو هیجان و تبلیغات گسترده، بزرگ‌ترین دام کلاهبرداران رمزارزی است.
- همیشه تحقیق کنید و از ورود به پروژه‌هایی که به نظر «بیش از حد خوب» می‌آیند، دوری کنید.

فصل ششم: کلاهبرداری ICO و توکن‌های جعلی

Fake ICOs and Token Scams

۶.۱ تعریف ICO و نقش آن در بازار رمزارز

ICO (عرضه اولیه سکه یا Initial Coin Offering) یک روش جمع‌آوری سرمایه است که در آن یک پروژه رمزارزی، توکن‌های جدیدی را در ازای دریافت رمزارزهای معتبر مانند بیت‌کوین یا اتریوم به سرمایه‌گذاران می‌فروشد. هدف پروژه معمولاً توسعه یک محصول یا پلتفرم جدید است.
ICOها در سال‌های ۲۰۱۷ و ۲۰۱۸ به شدت محبوب شدند و صدها پروژه، میلیاردها دلار سرمایه جمع‌آوری کردند.

اما درست همین محبوبیت، فرصت طلایی را برای کلاهبرداران فراهم کرد تا پروژه‌هایی کاملاً جعلی و توکن‌های بی‌ارزش را به مردم بفروشند.

۶.۲ سازوکار کلاهبرداری ICO و توکن‌های جعلی

۱. **راه‌اندازی سایت وایت‌پیپر حرفه‌ای:**
تیم یا افراد ناشناس با ساخت سایت شیک، وایت‌پیپر پر زرق و برق و وعده فناوری انقلابی، اعتماد سرمایه‌گذاران را جلب می‌کنند.

۲. **تبلیغات گسترده در شبکه‌های اجتماعی:**
با انتشار اخبار ساختگی، نمایش تیم جعلی، مصاحبه‌های دروغین و حتی استفاده از تصاویر چهره‌های سرشناس، برای پروژه اعتبارسازی می‌کنند.

۳. **پیشنهاد تخفیف‌های ویژه و FOMO:**
وعده عرضه محدود توکن با تخفیف ویژه به مدت کوتاه (فومو: ترس از دست دادن فرصت) و القای این که پروژه به‌زودی به پایان می‌رسد.

۴. **جمع‌آوری سرمایه:**
با جذب سرمایه‌گذاران از سراسر دنیا، مقدار قابل توجهی رمزارز معتبر جمع‌آوری می‌شود.

۵ .**خروج تیم و ناپدید شدن:**
تیم پس از پایان فروش یا حتی زودتر، سایت و شبکه‌های اجتماعی را می‌بندد و بدون تحویل محصول یا توسعه پلتفرم، با دارایی‌ها ناپدید می‌شود.

۶.۳ انواع کلاهبرداری‌های ICO و توکن

الف (پروژه‌های کاملاً جعلی

هیچ تیم، محصول یا فناوری واقعی در کار نیست. صرفاً یک سایت و وایت‌پیپر جعلی و وعده‌های پوچ.

ب (پروژه‌های نیمه‌کاره

تیمی با نمایش اولیه و حتی انتشار نسخه بتا یا دموی ناقص، سرمایه جذب می‌کند اما هیچ تعهدی برای اتمام پروژه ندارد و پس از جذب پول پروژه را رها می‌کند.

ج (توکن‌های شت‌کوین(Shitcoin)

توکن‌هایی با نام و داستان جذاب اما بدون هیچ کاربرد، ارزش یا پشتوانه واقعی که فقط برای جذب سرمایه و پامپ قیمت ساخته شده‌اند.

د (ایردراپ و پیش‌فروش جعلی

وعده دریافت رایگان توکن یا فروش خصوصی (Private Sale) اما با هدف سرقت دارایی‌های کاربران یا فیشینگ.

۶.۴ نشانه‌های هشداردهنده ICO و توکن جعلی

- **تیم ناشناس یا با هویت نامشخص**
- **وایت‌پیپر کلی، تکراری یا بدون توضیح فنی شفاف**
- **عدم وجود قرارداد هوشمند شفاف و Audit شده**

- آدرس شرکت یا دفتر ثبت‌شده نامعتبر یا غیرقابل ردیابی
- عدم وجود نمونه محصول، دموی واقعی یا مستندات توسعه
- حجم زیاد تبلیغات و شلوغی عجیب در شبکه‌های اجتماعی
- زمان‌بندی کوتاه و فشار برای خرید سریع(FOMO)
- پیشنهاد سود یا رشد قیمت تضمینی
- تکرار نام سرمایه‌گذاران و مشاوران مشهور بدون مدرک یا لینک واقعی
- تکرار اخبار مثبت در سایت‌های بی‌نام و نشان یا پولی

۶.۵ مثال‌های واقعی از کلاهبرداری‌های ICO و توکن جعلی

مثال ۱ Pincoin :و) iFan ویتنام(

در سال ۲۰۱۸ دو پروژه Pincoin و iFan بیش از ۶۶۰ میلیون دلار از ۳۲ هزار سرمایه‌گذار جمع‌آوری کردند. سایت‌های حرفه‌ای، وایت‌پیپرهای پرزرق‌وبرق و وعده سودهای تضمینی باعث شد بسیاری فریب بخورند. پس از مدتی، سایت‌ها بسته شد و هیچ محصولی تحویل نشد.

مثال ۲Centra Tech :

یک پروژه ICO در آمریکا که با وعده کارت اعتباری کریپتویی، بیش از ۲۵ میلیون دلار سرمایه جذب کرد و حتی فلوید می‌ودر و دی‌جی خالد آن را تبلیغ کردند. بعدها ثابت شد همه چیز جعلی بوده و مؤسسان دستگیر شدند.

مثال ۳AriseBank :

با تبلیغ "اولین بانک غیرمتمرکز رمزارزی"، میلیون‌ها دلار جمع‌آوری شد اما هیچ محصولی وجود نداشت و تیم پروژه متواری شد.

۶.۶ راه‌های پیشگیری و مقابله با کلاهبرداری ICO و توکن‌های جعلی

۱. **تحقیق کامل درباره تیم و مشاوران:**
بررسی دقیق هویت اعضای تیم، لینکدین، سوابق و حضور آنلاین واقعی.

۲. **مطالعه وایت‌پیپر و مدل اقتصادی:**
وایت‌پیپر باید شامل توضیحات فنی دقیق، نقشه راه عملی و مدل درآمدی شفاف باشد.

۳. **بررسی قرارداد هوشمند و شفافیت فنی:**
کد قرارداد باید عمومی و Audit شده توسط شرکت معتبر باشد.

۴. **درخواست نسخه بتا یا دموی محصول:**
پروژه‌های واقعی دست‌کم یک نسخه آزمایشی یا تست‌نت دارند.

۵. **دوری از پروژه‌هایی با تبلیغات هیجانی و فشار زمانی برای خرید:**
سرمایه‌گذاری عاقلانه نیازمند زمان و تحلیل است، نه عجله.

۶. **بررسی رفرنس‌ها و پوشش خبری:**
اخبار واقعی باید در منابع معتبر و مستقل منتشر شود، نه صرفاً سایت‌های پولی یا بلاگ‌های نامعتبر.

۷. **عدم اعتماد به چهره‌های مشهور و تبلیغات:**
حتی افراد مشهور نیز ممکن است فریب خورده یا صرفاً برای دریافت دستمزد پروژه را تبلیغ کنند.

پرسش و پاسخ فصل ششم

۱. **پرسش:**
آیا هر پروژه‌ای که وایت‌پیپر دارد معتبر است؟
پاسخ:
خیر. بسیاری از پروژه‌های جعلی وایت‌پیپر حرفه‌ای تهیه می‌کنند اما هیچ تیم، محصول یا برنامه واقعی ندارند.

۲ .**پرسش:**

چرا پروژه‌های ICO اغلب با عجله و فشار زمانی تبلیغ می‌شوند؟

پاسخ:

ایجاد حس FOMO باعث می‌شود افراد بدون بررسی کافی سرمایه‌گذاری کنند.

۳ .**پرسش:**

آیا دریافت ایردراپ رایگان همیشه بی‌خطر است؟

پاسخ:

خیر. برخی ایردراپ‌ها برای فیشینگ یا سرقت اطلاعات خصوصی طراحی شده‌اند.

تمرین عملی فصل ششم

۱ .**تحلیل یک پروژه:ICO**

به یک پروژه ICO جدید برخورد کرده‌اید. سه نکته کلیدی برای ارزیابی امنیت و اعتبار آن بنویسید.

۲ .**مطالعه موردی:**

داستان یک پروژه جعلی ICO را در اینترنت جستجو کنید و دلایل شکست یا افشای آن را توضیح دهید.

۳ .**چک‌لیست عملی:**

یک چک‌لیست ۵مرحله‌ای برای بررسی امنیت و اعتبار یک توکن یا ICO بنویسید.

جدول مقایسه‌ای: پروژه ICO جعلی، توکن شت‌کوین، و ICO معتبر

ICOمعتبر	توکن شت‌کوین	ICOجعلی	ویژگی
شفاف و قابل پیگیری	ناشناس یا ساختگی	ناشناس یا ساختگی	تیم توسعه
دقیق و تخصصی	وجود ندارد یا بی‌ارزش	کلی، تکراری، مبهم	وایت‌پیپر

ICOمعتبر	توکن شت‌کوین	ICOجعلی	ویژگی
وجود دارد	وجود ندارد	وجود ندارد	محصول واقعی
عمومی و Auditشده	عمومی نیست/بدونAudit	عمومی نیست/بدون Audit	قرارداد هوشمند
شفاف و معقول	هیجانی و گسترده	هیجانی و گسترده	تبلیغات
تدریجی و واقعی	ساختگی و پامپی	ساختگی و ناگهانی	رشد قیمت
منابع معتبر و رسمی	کانال‌های تلگرامی و اینفلوئنسرهای کوچک	سایت‌های غیرمعتبر	پوشش خبری

جمع‌بندی تصویری فصل ششم

- هر پروژه‌ای که تیم، محصول و مدل اقتصادی شفاف ندارد و صرفاً به تبلیغات و وعده سود اتکا می‌کند، مشکوک است.
- برای هر سرمایه‌گذاری در ICO یا خرید توکن جدید، حتماً تحقیق گسترده انجام دهید.
- از هرگونه شتاب، FOMOیا فشار زمانی دوری کنید؛ موفقیت مالی نیازمند صبر و بررسی دقیق است.

فصل هفتم: فیشینگ — (Phishing) دامی برای سرقت دارایی‌های دیجیتال

Phishing: The Trap for Stealing Digital Assets

۷.۱ فیشینگ چیست؟

فیشینگ (Phishing) یکی از رایج‌ترین و خطرناک‌ترین انواع کلاهبرداری در دنیای رمزارزهاست که هدف آن سرقت اطلاعات حساس کاربران مانند کلید خصوصی(Private Key) ، رمز عبور، عبارات بازیابی (Seed Phrase)یا دسترسی به کیف پول و حساب کاربری است.
کلاهبرداران با جعل ظاهر سایت‌ها، اپلیکیشن‌ها، پیام‌ها یا ایمیل‌های معتبر، سعی می‌کنند کاربر را فریب دهند تا اطلاعات حیاتی خود را در اختیار آن‌ها قرار دهد.

۷.۲ انواع رایج حملات فیشینگ در بازار رمزارز

الف (فیشینگ وب‌سایتی(Website Phishing)

کلاهبرداران وب‌سایت‌هایی با ظاهر و آدرس بسیار مشابه به سایت‌های معتبر (مانند صرافی‌ها یا کیف پول‌ها) می‌سازند. کاربر ناآگاه با وارد کردن اطلاعات ورود یا کلید خصوصی، در واقع داده‌های خود را مستقیماً به دست کلاهبردار می‌دهد.

مثال:
تغییر یک حرف کوچک در دامنه سایت اصلی) مثلاً binance.com به bìnance.com با یک کاراکتر غیرقابل تشخیص (و راه‌اندازی صفحه لاگین جعلی.

ب (فیشینگ ایمیلی(Email Phishing)

ارسال ایمیل‌های ظاهراً رسمی از طرف صرافی، کیف پول یا پروژه‌های رمزارزی با هدف ایجاد نگرانی (مثلاً: حساب شما تعلیق شده یا فعالیت مشکوک رخ داده) و ترغیب کاربر به کلیک روی لینک جعلی و وارد کردن اطلاعات.

مثال:
ایمیل هشدار امنیتی از طرف «صرافی باینس» با لینک به سایت فیک.

ج (فیشینگ شبکه‌های اجتماعی(Social Media Phishing)

کلاهبرداران با ساخت اکانت‌های جعلی به نام صرافی‌ها، پروژه‌های معتبر یا حتی افراد مشهور (اینفلوئنسرها، مدیران پروژه‌ها)، کاربران را به انجام تراکنش یا ارسال اطلاعات حساس دعوت می‌کنند.

مثال:
پروفایل توییتر با نام و عکس مدیرعامل یک پروژه معروف که ایردراپ یا پاداش ویژه را فقط با وارد کردن عبارت بازیابی وعده می‌دهد.

د (فیشینگ پیامکی SMS Phishing) یا(Smishing

ارسال پیامک با ظاهر رسمی (مثلاً پیامک تأیید یا هشدار امنیتی) که حاوی لینکی به سایت جعلی یا درخواست برای ارسال اطلاعات ورود است.

هـ (بدافزار و افزونه مرورگر(Malware & Browser Extensions)

برخی نرم‌افزارها، افزونه‌ها یا اپلیکیشن‌های جعلی، اطلاعات کاربر را هنگام ورود به سایت‌های رمزارزی رهگیری و سرقت می‌کنند.

۷.۳ دلایل موفقیت حملات فیشینگ

- **شباهت زیاد سایت یا پیام جعلی به نمونه اصلی**
- **استفاده از موقعیت‌های اضطراری و استرس‌زا (ایجاد نگرانی و عجله)**
- **استفاده از تکنیک‌های روانشناسی اجتماعی (اعتمادسازی یا ترساندن)**
- **ضعف کاربران در تشخیص دامنه‌ها، ایمیل‌ها یا اپلیکیشن‌های واقعی از جعلی**
- **فقدان آموزش امنیتی مناسب و عادت به کلیک کردن بدون بررسی**

۷.۴ نشانه‌های هشداردهنده حملات فیشینگ

- لینک‌هایی با دامنه‌های ناآشنا، عجیب یا متفاوت از سایت اصلی
- درخواست برای وارد کردن کلید خصوصی یا عبارت بازیابی (هیچ سرویس معتبری این اطلاعات را طلب نمی‌کند!)
- پیام‌های ناگهانی با محتوای استرس‌زا یا هشدارهای غیرمنتظره
- ظاهر متفاوت یا با غلط املایی در سایت، ایمیل یا پیام
- درخواست انتقال وجه به آدرس مشخص برای حل مشکل یا دریافت جایزه

۷.۵ مثال‌های واقعی از حملات فیشینگ رمزارزی

مثال ۱: حمله فیشینگ متامسک(MetaMask)

سایت‌ها و افزونه‌های جعلی زیادی با ظاهر مشابه کیف پول MetaMask منتشر شدند. کاربران با وارد کردن عبارت بازیابی یا کلید خصوصی، دارایی خود را به راحتی از دست دادند.

مثال ۲: فیشینگ توییتری با نام ایلان ماسک

هکرها با ساخت اکانت جعلی ایلان ماسک، کاربران را به شرکت در ایردراپ بیت‌کوین یا اتریوم ترغیب کردند. در برخی موارد حتی حساب رسمی افراد مشهور نیز هک شد و پیام فیشینگ منتشر گردید.

مثال ۳: فیشینگ ایمیلی صرافی کوین‌بیس(Coinbase)

کاربران ایمیل‌هایی مبنی بر تعلیق حساب یا فعالیت مشکوک دریافت کردند و برای رفع مشکل، روی لینک جعلی کلیک کردند و اطلاعات حساس خود را وارد نمودند.

۷.۶ روش‌های پیشگیری و مقابله با حملات فیشینگ

۱. **بررسی دقیق آدرس سایت (URL) قبل از ورود اطلاعات حساس:**
همیشه آدرس سایت را تایپ کنید، نه اینکه روی لینک پیام یا ایمیل کلیک کنید.

۲ .**فعال‌سازی احراز هویت دومرحله‌ای:(2FA)**
حتی در صورت افشای رمز عبور، لایه امنیتی بیشتری خواهید داشت.

۳ .**عدم ارائه کلید خصوصی یا عبارت بازیابی به هیچ کس:**
هیچ‌کس، حتی پشتیبانی رسمی یک صرافی یا کیف پول، این اطلاعات را از شما نمی‌خواهد.

۴ .**استفاده از افزونه‌ها و نرم‌افزارهای معتبر:**
فقط از منابع رسمی دانلود کنید و به افزونه‌های نامعتبر اعتماد نکنید.

۵ .**بررسی ایمیل‌های مشکوک و پیام‌های غیرمنتظره:**
از ارسال اطلاعات از طریق ایمیل، پیامک یا شبکه اجتماعی خودداری کنید.

۶ .**آموزش و آگاهی مستمر:**
اخبار حملات جدید و شیوه‌های فیشینگ را دنبال کنید تا همیشه یک گام جلوتر باشید.

پرسش و پاسخ فصل هفتم

۱ .**پرسش:**
چرا درخواست کلید خصوصی یا عبارت بازیابی توسط هر وب‌سایت یا فردی باید زنگ خطر باشد؟
پاسخ:
این اطلاعات فقط برای مالک کیف پول است و افشای آن مساوی با از دست رفتن کل دارایی است؛ هیچ سرویس معتبری این داده‌ها را نمی‌خواهد.

۲ .**پرسش:**
آیا تنها ظاهر معتبر یک سایت برای اطمینان کافی است؟
پاسخ:
خیر؛ بسیاری از سایت‌های جعلی کاملاً شبیه نمونه اصلی طراحی می‌شوند و فقط تفاوت‌های جزئی در آدرس یا جزئیات دارند.

۳ .**پرسش:**

بهترین راه مقابله با حملات فیشینگ چیست؟

پاسخ:

آگاهی و آموزش مستمر، بررسی دقیق آدرس‌ها و عدم افشای اطلاعات حساس حتی به افراد یا سایت‌های به ظاهر معتبر.

تمرین عملی فصل هفتم

۱ .**شناسایی سایت فیشینگ:**

دو نمونه سایت جعلی از یک صرافی یا کیف پول معروف را در اینترنت جستجو کنید و تفاوت‌های ظاهری یا دامنه آن‌ها را پیدا کنید.

۲ .**مطالعه موردی:**

داستان یک قربانی حمله فیشینگ در حوزه رمزارز را بخوانید و دلایل موفقیت کلاهبردار را تحلیل کنید.

۳ .**چک‌لیست عملی:**

یک چک‌لیست پنج‌مرحله‌ای برای جلوگیری از فیشینگ در معاملات رمزارز بنویسید.

جدول مقایسه‌ای: فیشینگ رمزارزی، هک مستقیم، و بدافزار

ویژگی	فیشینگ(Phishing)	هک مستقیم (Direct Hack)	بدافزار(Malware)
شیوه نفوذ	فریب و سرقت اطلاعات	نفوذ به سیستم و سرقت	نصب نرم‌افزار مخرب
نیاز به همکاری کاربر	بله	معمولاً نه	بله (دانلود/نصب برنامه)
هزینه/مهارت مهاجم	پایین/متوسط	بالا	پایین/متوسط

بدافزار(Malware)	هک مستقیم (Direct Hack)	فیشینگ(Phishing)	ویژگی
بله	تا حدی	بله	قابل پیشگیری با آموزش
سرقت اطلاعات یا کنترل کیف پول	سرقت یا تخریب دارایی	سرقت مستقیم دارایی	تخریب یا سرقت اطلاعات

جمع‌بندی تصویری فصل هفتم

- هر پیام، ایمیل یا سایت که از شما کلید خصوصی یا عبارت بازیابی بخواهد، صددرصد کلاهبرداری است.
- همیشه آدرس سایت‌ها را دقیق بررسی کنید و از تایپ دستی آن اطمینان داشته باشید.
- آموزش و هوشیاری بهترین سپر در برابر فیشینگ است.
- برای هر پیام یا ایمیل مشکوک، از راه‌های رسمی پشتیبانی استعلام بگیرید.
- احراز هویت دومرحله‌ای و نرم‌افزارهای امنیتی را فعال نگه دارید.

فصل هشتم: کلاهبرداری‌های صرافی و کیف پول جعلی

Exchange & Fake Wallet Scams

۸.۱ صرافی و کیف پول رمزارزی چیست؟

صرافی رمزارزی (Cryptocurrency Exchange) بستری آنلاین برای خرید، فروش، تبدیل یا نگهداری رمزارزهاست.
کیف پول رمزارزی (Crypto Wallet) نرم‌افزار یا سخت‌افزاری برای ذخیره، ارسال و دریافت رمزارز است.
هر دو، ابزارهای حیاتی برای فعالیت در بازار رمزارز به شمار می‌روند؛ اما همین اهمیت باعث شده تا کلاهبرداران با ساخت نسخه‌های جعلی از آن‌ها، کاربران را فریب داده و دارایی‌شان را سرقت کنند.

۸.۲ انواع کلاهبرداری‌های صرافی و کیف پول جعلی

الف (صرافی آنلاین جعلی

کلاهبرداران با طراحی سایت‌هایی شبیه صرافی‌های معتبر، کاربران را جذب می‌کنند. پس از واریز وجه یا رمزارز به حساب، یا برداشت دارایی ممکن نیست یا سایت به‌کلی ناپدید می‌شود.

ویژگی‌ها:

- نام و لوگوی شبیه به صرافی‌های مشهور
- وعده نرخ تبدیل یا کارمزدهای غیرواقعی و جذاب
- درخواست ارسال وجه قبل از معامله یا تایید هویت جعلی
- نبود پشتیبانی واقعی یا پاسخ‌گویی سریع پس از جذب سرمایه

مثال:
در سال ۲۰۲۰ چندین صرافی جعلی با دامنه‌هایی بسیار شبیه به Binance و Coinbase فعال شدند و هزاران دلار از کاربران سرقت کردند.

ب (اپلیکیشن و کیف پول نرم‌افزاری جعلی

کلاهبرداران با ارائه اپلیکیشن یا افزونه مرورگر با نام و آیکون مشابه کیف پول‌های مشهور) مانند MetaMask، Trust Wallet، Trezorو غیره(، کاربران را وادار به دانلود، نصب و وارد کردن کلید خصوصی یا عبارت بازیابی می‌کنند و پس از آن دارایی‌ها به سرعت به حساب کلاهبردار منتقل می‌شود.

ویژگی‌ها:

- ظاهر و آیکون مشابه نسخه اصلی
- انتشار در فروشگاه‌های نرم‌افزاری غیررسمی یا حتی گاهی فروشگاه‌های معتبر Google Play) یا App Store)
- نبود اطلاعات پشتیبانی، مستندات یا بروزرسانی
- حذف ناگهانی برنامه پس از سرقت دارایی‌ها

مثال:
در سال ۲۰۲۱، بیش از صد اپلیکیشن جعلی با نام Trezor در Google Play منتشر شد و هزاران کاربر دارایی‌های خود را از دست دادند.

ج (کیف پول سخت‌افزاری جعلی یا دست‌کاری‌شده

برخی کیف پول‌های سخت‌افزاری) مثل Ledger یا (Trezor به صورت دست‌دوم یا از فروشنده غیررسمی خریداری می‌شوند. این دستگاه‌ها ممکن است دستکاری‌شده و اطلاعات کاربر به صورت مخفیانه به سرور کلاهبردار ارسال شود.

ویژگی‌ها:

- بسته‌بندی غیرعادی یا کد فعال‌سازی استفاده‌شده
- قیمت پایین‌تر از بازار
- همراه بودن با دفترچه راهنمای مشکوک

- عدم پذیرش در سایت اصلی تولیدکننده

مثال:
در سال ۲۰۱۹، گروهی از کاربران Ledger پس از خرید از فروشگاه‌های غیررسمی، کل دارایی خود را به دلیل دستکاری سخت‌افزار از دست دادند.

د (صرافی‌های P2P و اسکرو (Escrow) جعلی

برخی سایت‌های معامله همتا به همتا (P2P) یا سرویس‌های اسکرو (واسط اطمینان) با ایجاد پنل‌های جعلی، کاربران را به ارسال رمزارز یا وجه نقد بدون هیچ ضمانت واقعی وادار می‌کنند.

ویژگی‌ها:

- عدم تایید هویت خریدار یا فروشنده
- نبود قرارداد یا تضمین واقعی برای تسویه معامله
- درخواست پرداخت قبل از دریافت دارایی
- پنل پشتیبانی غیرواقعی یا اتوماتیک

۸.۳ نشانه‌های هشداردهنده صرافی و کیف پول جعلی

- دامنه یا نام سایت/برنامه با حروف اضافه، اشتباه تایپی یا دامنه غیررسمی xyz.) به جای(com.
- نبود اطلاعات تماس معتبر یا پشتیبانی واقعی
- عدم وجود آدرس فیزیکی یا تیم مدیریتی شفاف
- وعده سود، کارمزد یا نرخ تبدیل غیرواقعی و بیش از حد جذاب
- اصرار به وارد کردن کلید خصوصی یا عبارت بازیابی
- عدم وجود بررسی‌های معتبر (Review) یا گزارش در منابع تخصصی

- عدم وجود یا ضعف در مستندات و بروزرسانی نرم‌افزار

۸.۴ مثال‌های واقعی کلاهبرداری صرافی و کیف پول جعلی

مثال ۱: صرافی) BitKRX کره جنوبی(

صرافی BitKRX با شبیه‌سازی نام بزرگ‌ترین بورس اوراق بهادار کره جنوبی، اعتماد سرمایه‌گذاران را جلب کرد و پس از جذب میلیون‌ها دلار ناپدید شد.

مثال ۲: اپلیکیشن جعلیTrezor

برنامه‌هایی با نام و آیکون Trezor Wallet در Google Play منتشر شد که کاربران پس از وارد کردن اطلاعات بازیابی، تمام دارایی خود را از دست دادند.

مثال ۳: سایت‌های اسکرو جعلی

در سال‌های اخیر، ده‌ها سایت اسکرو جعلی با وعده معاملات سریع و بدون کارمزد در تلگرام فعال شدند و پس از دریافت وجه نقد یا رمزارز، هیچ تراکنشی انجام ندادند.

۸.۵ راه‌های پیشگیری و مقابله با کلاهبرداری صرافی و کیف پول جعلی

۱ .**استفاده از منابع و لینک‌های رسمی:**
آدرس و اپلیکیشن صرافی‌ها و کیف پول‌ها را فقط از سایت اصلی تهیه کنید؛ هرگز به لینک‌های دریافتی از شبکه‌های اجتماعی یا ایمیل اطمینان نکنید.

۲ .**بررسی نام دامنه و صحت آدرس سایت:**
حتی تفاوت یک حرف یا دامنه می‌تواند نشانه جعلی بودن باشد.

۳ .**دانلود اپلیکیشن و نرم‌افزار فقط از فروشگاه‌های معتبر:**
همواره نام توسعه‌دهنده و تعداد نصب و نظرات کاربران را بررسی کنید.

۴ .**خرید کیف پول سخت‌افزاری فقط از نمایندگی و سایت اصلی:**
هرگز از فروشنده‌های دست‌دوم یا ناشناس خرید نکنید.

۵ .**عدم وارد کردن کلید خصوصی یا عبارت بازیابی در سایت‌ها یا اپلیکیشن‌های ناشناس:**
هیچ سرویس معتبری این اطلاعات را از شما نمی‌خواهد.

۶ .**بررسی سوابق و ریویوهای کاربران:**
پیش از استفاده، نظرات کاربران در سایت‌هایی مانند Trustpilot یا Reddit را بخوانید.

۷ .**آزمایش اولیه با مبالغ کم:**
هرگز با مبالغ سنگین شروع نکنید؛ ابتدا عملکرد سایت یا کیف پول را با مقدار کم بسنجید.

پرسش و پاسخ فصل هشتم

۱ .**پرسش:**
چرا نباید کلید خصوصی یا عبارت بازیابی را در هیچ اپلیکیشن یا سایت غیررسمی وارد کنیم؟
پاسخ:
با افشای این اطلاعات، کل دارایی رمزارزی شما در اختیار کلاهبردار قرار می‌گیرد و بازگشت آن تقریباً غیرممکن است.

۲ .**پرسش:**
بهترین راه اطمینان از صحت یک صرافی یا کیف پول چیست؟
پاسخ:
مراجعه به منابع و سایت رسمی، بررسی مجوز و نظرات کاربران، و جستجوی نام پروژه در منابع تخصصی.

۳ .**پرسش:**
آیا صرافی‌های غیرمتمرکز (DEX) هم می‌توانند جعلی باشند؟
پاسخ:
بله؛ رابط کاربری یا سایت جعلی یک DEX می‌تواند کاربر را فریب دهد و دارایی او را سرقت کند.

تمرین عملی فصل هشتم

۱ .**شناسایی سایت و اپلیکیشن جعلی:**
دو نمونه سایت یا اپلیکیشن جعلی صرافی یا کیف پول را جستجو کنید و تفاوت‌های آنها با نسخه اصلی را بنویسید.

۲ .**بررسی تجربه کاربری:**
داستان یک کاربر که قربانی صرافی یا کیف پول جعلی شده است را بخوانید و تحلیل کنید کجا اشتباه کرده است.

۳ .**چک‌لیست پیشگیری:**
یک چک‌لیست ۵ مرحله‌ای برای اطمینان از اعتبار صرافی یا کیف پول بنویسید.

جدول مقایسه‌ای: صرافی و کیف پول معتبر vs جعلی

ویژگی	صرافی/کیف پول معتبر	صرافی/کیف پول جعلی
آدرس و دامنه	رسمی و ثبت‌شده	دامنه عجیب یا مشابه
تیم توسعه‌دهنده	شفاف و قابل پیگیری	ناشناس یا جعلی
اپلیکیشن/سایت	بروزرسانی منظم و ریویوی مثبت	بدون بروزرسانی و ریویوی منفی یا جعلی
درخواست کلید خصوصی	هرگز	معمولاً درخواست می‌کند
مجوز و اطلاعات تماس	معتبر و واقعی	بی‌اطلاع یا جعلی
پشتیبانی	پاسخ‌گو و واقعی	بی‌پاسخ یا اتوماتیک

جمع‌بندی تصویری فصل هشتم

- هرگز اطلاعات حساس خود را در سایت یا اپلیکیشن غیررسمی وارد نکنید؛
- تنها به منابع و لینک‌های اصلی و رسمی مراجعه کنید؛
- خرید کیف پول سخت‌افزاری فقط از نمایندگی رسمی؛
- ریویو و نظرات کاربران و کارشناسان را جدی بگیرید؛
- اگر چیزی بیش از حد خوب به نظر می‌رسد، احتمالاً واقعی نیست!

فصل نهم: کلاهبرداری از طریق شبکه‌های اجتماعی و تبلیغات فریبنده

Social Media & Deceptive Advertising Scams

۹.۱ چرا شبکه‌های اجتماعی بستر محبوب کلاهبرداران است؟

در دنیای امروز، شبکه‌های اجتماعی مانند تلگرام، واتس‌اپ، توییتر، اینستاگرام و حتی یوتیوب، نه‌تنها بستری برای ارتباط، بلکه برای اطلاع‌رسانی و تبلیغات پروژه‌های رمزارزی شده‌اند.
اما همین ویژگی—سرعت انتشار، گستره دسترسی، امکان فعالیت ناشناس و نبود کنترل کافی—بستر مناسبی برای فعالیت کلاهبرداران و انتشار تبلیغات فریبنده ایجاد کرده است. آن‌ها با استفاده از روانشناسی جمعی، القای هیجان، سوءاستفاده از چهره‌های شناخته‌شده و تکنیک‌های نوین تبلیغاتی، میلیون‌ها نفر را هدف قرار می‌دهند.

۹.۲ انواع کلاهبرداری‌های رایج در شبکه‌های اجتماعی

الف (حساب‌های جعلی افراد مشهور(Fake Celebrity Accounts)

کلاهبرداران با ساخت پروفایل جعلی به نام افراد مشهور (مانند مدیران پروژه‌های رمزارزی، اینفلوئنسرها، کارآفرینان، یا حتی شخصیت‌های هنری و ورزشی)، مخاطبان را به سرمایه‌گذاری در پروژه‌ای خاص، شرکت در ایردراپ یا ارسال ارز برای دریافت پاداش دعوت می‌کنند.

مثال:
در سال ۲۰۲۰، هزاران حساب جعلی به نام ایلان ماسک در توییتر وعده ارسال دو برابر بیت‌کوین را در قبال ارسال یک بیت‌کوین به آدرس مشخص دادند و ده‌ها هزار نفر قربانی شدند.

ب (گروه‌ها و کانال‌های پامپ و دامپ(Pump & Dump Groups)

گروه‌هایی که در تلگرام یا دیسکورد با هدف بالا بردن قیمت ناگهانی یک توکن یا کوین بی‌ارزش (پامپ) تشکیل می‌شوند. پس از جذب تعداد زیادی کاربر، ادمین‌ها دارایی خود را می‌فروشند (دامپ) و کاربران عادی با سقوط شدید قیمت مواجه می‌شوند.

ویژگی‌ها:

- وعده سود سریع و مطمئن
- تبلیغ زمان‌بندی دقیق برای خرید و فروش
- ارسال سیگنال‌های جعلی و اطلاعات دروغین درباره پروژه

ج (ایردراپ و جایزه‌های جعلی(Fake Airdrops & Giveaways)

کلاهبرداران با وعده ایردراپ رایگان یا جایزه‌های بزرگ، کاربران را وادار به وارد کردن کلید خصوصی، عبارت بازیابی یا ارسال مقداری رمزارز برای "فعال‌سازی" جایزه می‌کنند.

مثال:
پیام‌هایی با عنوان "شما برنده ۱۰ اتریوم شدید! برای دریافت، عبارت بازیابی خود را وارد کنید" یا "برای فعال‌سازی ایردراپ، ۰.۱ اتریوم ارسال کنید."

د (تبلیغات اسپانسری و صفحات پروژه‌های جعلی

برخی کلاهبرداران با هزینه کردن در تبلیغات اسپانسری شبکه‌های اجتماعی، پروژه‌های اسکم، توکن یا ICOجعلی را به شکل حرفه‌ای معرفی می‌کنند. حتی برخی از این تبلیغات در پلتفرم‌های بزرگ مثل فیسبوک و اینستاگرام نیز دیده می‌شود.

هـ (کامنت‌ها و ریویوهای جعلی(Fake Comments & Reviews)

برای افزایش اعتبار، زیر پست‌های پروژه‌های جعلی یا کانال‌های کلاهبرداری، حجم زیادی کامنت یا ریویوی مثبت توسط ربات‌ها یا حساب‌های جعلی منتشر می‌شود.

و (پیام‌های مستقیم(Direct Message Scams)

کاربرانی با ظاهر مشاور، پشتیبان صرافی یا حتی دوست قدیمی، از طریق پیام خصوصی به قربانی نزدیک می‌شوند و اطلاعات حساس یا انتقال وجه را درخواست می‌کنند.

۹.۳ نشانه‌های هشداردهنده کلاهبرداری در شبکه‌های اجتماعی

- حساب‌هایی با تعداد فالوئر زیاد اما فعالیت کم یا ریویوی تکراری
- پیشنهاد سود سریع، دوبرابر شدن پول، یا ایردراپ رایگان در ازای ارسال دارایی
- پیام‌هایی با اشتباه نگارشی یا ترجمه ضعیف
- لینک‌های کوتاه‌شده یا دامنه‌های مشکوک
- پست‌ها و کامنت‌هایی با مضمون "من سود کردم، شما هم بپیوندید"
- درخواست کلید خصوصی، عبارت بازیابی یا اسکرین‌شات کیف پول
- تشویق به دعوت دوستان و گسترش شبکه به منظور دریافت پاداش

۹.۴ مثال‌های واقعی از کلاهبرداری شبکه‌های اجتماعی

مثال ۱: حمله بزرگ توییتر سال ۲۰۲۰

در حمله‌ای هماهنگ، حساب‌های رسمی ایلان ماسک، بیل گیتس، باراک اوباما و چندین چهره دیگر هک شد و پیام فیشینگ بیت‌کوینی منتشر شد. هزاران نفر مبلغی بیش از ۱۰۰ هزار دلار را در چند ساعت به آدرس مهاجمین واریز کردند.

مثال ۲: گروه‌های پامپ و دامپ ایرانی و خارجی

در سال‌های اخیر، صدها گروه تلگرامی سیگنال پامپ و دامپ راه‌اندازی شده است. در بیشتر موارد، فقط ادمین‌ها سود می‌کنند و کاربران عادی پس از خرید، شاهد سقوط شدید قیمت می‌شوند.

مثال ۳: صفحات اینستاگرامی فروش توکن

صفحات متعدد با تبلیغ پروژه‌های توکن، NFTیا DeFi جعلی، کاربران را به سایت اسکم هدایت کرده و پس از واریز وجه، هیچ خدماتی ارائه نمی‌دهند و حتی صفحه را پاک می‌کنند.

۹.۵ چرا افراد در دام کلاهبرداری شبکه‌های اجتماعی می‌افتند؟

- اثر روانی تبلیغات و فومو :FOMO) ترس از دست دادن فرصت(
- اعتماد به چهره‌های شناخته‌شده یا دنبال‌کنندگان زیاد
- فشار اجتماعی و پیام‌های مثبت فراوان در گروه‌ها
- فقدان دانش و تجربه کافی درباره امنیت رمزارز
- عدم توجه به نشانه‌های ظریف هشدار و عجله برای سود سریع
- نبود مکانیزم کافی برای گزارش و حذف سریع صفحات جعلی

۹.۶ راه‌های پیشگیری و مقابله با کلاهبرداری در شبکه‌های اجتماعی

۱ .**بی‌توجهی به پیام‌های سودآور و وسوسه‌برانگیز:**
هر پیام یا تبلیغ با وعده سود غیرمعمول، باید با تردید جدی مواجه شود.

۲ .**بررسی هویت حساب‌ها و پروفایل‌ها:**
به تعداد پست، تاریخ شروع فعالیت، نوع تعامل و لینک‌های رسمی توجه کنید.

۳ .**عدم ارسال اطلاعات حساس به هیچ فردی یا صفحه‌ای:**
کلید خصوصی، عبارت بازیابی و رمز عبور فقط باید نزد خودتان باشد.

۴ .**عدم کلیک روی لینک‌های ناشناس و کوتاه‌شده:**
ابتدا لینک را بررسی و سپس اقدام به ورود کنید.

۵ .**مشورت با افراد آگاه و جستجوی نام پروژه یا توکن در منابع تخصصی:**
در سایت‌هایی مانندCoinMarketCap ، Reddit، Bitcointalkو Trustpilot نظرات و هشدارها را بخوانید.

۶ .**گزارش حساب‌های مشکوک به پلتفرم مربوطه:**
با گزارش (Report) صفحات و پیام‌های جعلی، به حفاظت از جامعه رمزارز کمک کنید.

۷ .**دوری از گروه‌های پامپ و دامپ، ایردراپ‌های عجیب و سیگنال‌های خرید و فروش ناشناس:**
تنها به منابع معتبر و تحلیل‌های اثبات‌شده اعتماد کنید.

پرسش و پاسخ فصل نهم

۱ .**پرسش:**
چرا حتی صفحات تبلیغ‌شده در اینستاگرام یا فیسبوک هم می‌توانند کلاهبرداری باشند؟
پاسخ:
برخی کلاهبرداران هزینه تبلیغات رسمی را می‌پردازند تا معتبر جلوه کنند، اما هدف نهایی‌شان فقط جذب سرمایه و کلاهبرداری است.

۲ .**پرسش:**
آیا اکانت‌های با تیک آبی (Verified) همیشه واقعی هستند؟
پاسخ:
خیر. حتی حساب‌های تأییدشده نیز ممکن است هک شوند یا جعل شوند؛ تنها منبع رسمی را باید از سایت پروژه یا چهره معتبر دنبال کرد.

۳ .**پرسش:**
بهترین راه مقابله با گروه‌های پامپ و دامپ چیست؟
پاسخ:
اصلاً در این گروه‌ها عضو نشوید؛ در اکثر مواقع فقط گردانندگان سود می‌کنند و بقیه ضرر خواهند کرد.

تمرین عملی فصل نهم

۱. **شناسایی تبلیغات فریبنده:**
سه نمونه تبلیغ، پیام یا پست فریبنده رمزارزی را در شبکه‌های اجتماعی پیدا کنید و نشانه‌های کلاهبرداری در هر کدام را تحلیل کنید.

۲. **مطالعه موردی:**
داستان یک قربانی کلاهبرداری شبکه اجتماعی (مثلاً ایردراپ یا حساب جعلی اینستاگرام) را بررسی و راهکار پیشگیری را بنویسید.

۳. **چک‌لیست عملی:**
یک چک‌لیست پنج‌مرحله‌ای برای بررسی اعتبار یک حساب رمزارزی در شبکه‌های اجتماعی بنویسید.

جدول مقایسه‌ای: کلاهبرداری شبکه اجتماعی، فیشینگ و پامپ/دامپ

ویژگی	کلاهبرداری شبکه اجتماعی	فیشینگ	پامپ و دامپ گروهی
شیوه اجرا	پروفایل جعلی، تبلیغ	ایمیل، سایت یا پیام جعلی	گروه و کانال تلگرامی/دیسکورد
هدف اصلی	سرقت پول، فیشینگ	سرقت اطلاعات/دارایی	فروش ناگهانی و ضرر کاربران
ابزار مورد استفاده	اکانت، گروه، تبلیغ	لینک و سایت جعلی	پیام‌رسان، کانال
نقش کاربر	اعتماد و انتقال وجه	افشای اطلاعات حساس	خرید و فروش توکن
میزان شناسایی	متوسط تا پایین	بالا با آموزش	پایین در لحظه وقوع

جمع‌بندی تصویری فصل نهم

- هر تبلیغ یا پیام با وعده سود سریع و رایگان، احتمالاً دام کلاهبرداران است؛
- به ظاهر حساب‌ها، تعداد دنبال‌کننده و تبلیغ رسمی اعتماد نکنید؛
- کلید خصوصی، رمز و عبارت بازیابی را با هیچ فرد یا صفحه‌ای به اشتراک نگذارید؛
- قبل از سرمایه‌گذاری یا ارسال وجه، حتماً تحقیق کنید و از افراد آگاه مشورت بگیرید؛
- با گزارش حساب‌های مشکوک، نقش فعالی در امنیت جامعه رمزارز داشته باشید.

فصل دهم: بدافزارها و حملات هکری به دارایی‌های رمزارزی

Malware & Hacking Attacks on Crypto Assets

۱۰.۱ مقدمه: تهدیدهای فنی و امنیتی در دنیای رمزارزها

در کنار کلاهبرداری‌های کلاسیک و فریب‌های انسانی، تهدیدات فنی و هک نیز یکی از جدی‌ترین مخاطرات برای دارندگان رمزارز به شمار می‌رود. هرچه ارزش بازار رمزارزها بالاتر می‌رود، هکرها و توسعه‌دهندگان بدافزار انگیزه بیشتری برای حمله به کاربران و پلتفرم‌ها پیدا می‌کنند.
این تهدیدها می‌توانند منجر به سرقت تمام دارایی، از دست رفتن دسترسی، یا حتی از بین رفتن اعتبار یک پروژه رمزارزی شوند.

۱۰.۲ انواع بدافزارها در بازار رمزارز

الف (بدافزار سرقت کیف پول(Wallet Stealer)

برنامه‌های مخربی که پس از نصب روی کامپیوتر یا موبایل، کلید خصوصی، عبارت بازیابی یا اطلاعات دسترسی به کیف پول کاربر را شناسایی و برای مهاجم ارسال می‌کنند.

نمونه:
بدافزارهای شبیه به فایل‌های رایگان یا اپلیکیشن‌های پرکاربرد که بعد از نصب به دنبال فایل‌های مرتبط با کیف پول (MetaMask, Trust Wallet, Electrum و (...می‌گردند.

ب (بدافزارKeylogger

برنامه‌هایی که هر کلیدی را که کاربر روی کیبورد می‌زند، ثبت و برای هکر ارسال می‌کنند. رمز عبور، کلید خصوصی، یا عبارت بازیابی هدف اصلی این بدافزارهاست.

نمونه:
قرار دادن کی‌لاگر در فایل کرک‌شده یک نرم‌افزار، بازی، یا افزونه مرورگر تقلبی.

ج (بدافزارClipBoard Hijacker

این بدافزار آدرس کیف پولی را که کاربر کپی می‌کند، هنگام انتقال وجه با آدرس مهاجم جایگزین می‌کند. کاربر متوجه نمی‌شود و دارایی خود را به آدرس هکر ارسال می‌کند.

نمونه:
هنگام انتقال بیت‌کوین، آدرس مقصد را از سایت کیف پول خود کپی کرده‌اید، اما با جای‌گذاری (Paste)آدرس، بدافزار آن را تغییر داده است.

د (بدافزار استخراج رمزارز(Crypto Mining Malware)

برخی بدافزارها از منابع سخت‌افزاری سیستم قربانی برای استخراج رمزارز (معمولاً مونرو یا بیت‌کوین) بدون اطلاع کاربر استفاده می‌کنند.

نمونه:
تبلیغات سایت‌های ناشناس یا نصب افزونه‌های عجیب، باعث می‌شود CPU یا GPU سیستم شما همیشه مشغول استخراج برای مهاجم باشد.

هـ (فیشینگ با بدافزار ترکیبی

بدافزارها گاهی به صورت لینک در پیام یا ایمیل فیشینگ منتشر می‌شوند. پس از دانلود و اجرا، بدافزار اطلاعات حساس شما را به سرقت می‌برد یا به سایت‌های جعلی هدایتتان می‌کند.

۱۰.۳ انواع حملات هکری به دارایی‌ها و پلتفرم‌های رمزارزی

الف (حملات به صرافی‌ها و پلتفرم‌هایDeFi

صرافی‌ها و پلتفرم‌های دیفای، به دلیل حجم بالای دارایی، همواره هدف اصلی هکرها هستند.

- **هک قرارداد هوشمند :**استفاده از آسیب‌پذیری در کد قرارداد برای سرقت یا قفل‌کردن دارایی کاربران.
- **هک صرافی متمرکز :**نفوذ به سرورهای صرافی، سرقت اطلاعات کاربران یا انتقال دارایی‌ها به کیف پول هکر.

مثال:

- **Mt.Gox:**در سال ۲۰۱۴، صرافی Mt.Gox بزرگ‌ترین هک تاریخ رمزارز را تجربه کرد و ۸۵۰ هزار بیت‌کوین سرقت شد.
- **Poly Network:**در ۲۰۲۱، بیش از ۶۰۰ میلیون دلار از پلتفرم دیفای Poly Network به سرقت رفت.

ب (حملات به کاربران فردی

هکرها با استفاده از بدافزار، مهندسی اجتماعی یا فیشینگ، مستقیماً کاربران عادی را هدف می‌گیرند و با دسترسی به کلید خصوصی یا اطلاعات ورود، دارایی‌ها را تخلیه می‌کنند.

ج (حملات ۵۱ درصد(51% Attack

در برخی بلاکچین‌ها، اگر یک مهاجم بیش از ٪۵۱ قدرت پردازش شبکه را در اختیار بگیرد، می‌تواند تراکنش‌های جعلی ثبت یا تایید کند و حتی دارایی‌های کاربران را خرج دوباره (Double Spend) کند.

مثال:
در برخی کوین‌های کوچک، هکرها با اجاره موقت قدرت پردازشی از این روش سوءاستفاده کردند.

د (حملاتSybil ، DDoSو سایر تهدیدهای فنی

حملات DDoS (ازدحام سرور) یا Sybil (ساخت حساب‌های متعدد برای تاثیرگذاری در رأی‌گیری‌های شبکه) می‌تواند به اختلال در عملکرد شبکه یا سرقت اطلاعات منجر شود.

۱۰.۴ نشانه‌ها و پیامدهای حمله هکری یا بدافزاری

- کاهش ناگهانی موجودی کیف پول بدون انجام تراکنش توسط کاربر
- عدم دسترسی به حساب یا بلاک شدن آن
- کندی غیرعادی سیستم یا مصرف بالای پردازنده و رم
- مشاهده تراکنش‌هایی که کاربر انجام نداده است
- دریافت ایمیل، پیامک یا نوتیفیکیشن عجیب از صرافی‌ها یا کیف پول‌ها
- نصب یا وجود نرم‌افزارهای ناشناس روی سیستم

۱۰.۵ مثال‌های واقعی حمله و بدافزار

- **Mt.Gox:** نابودی بزرگ‌ترین صرافی بیت‌کوین و هزاران قربانی
- **ژاپن Coincheck):** هک صرافی و سرقت ۵۰۰ میلیون دلار NEM
- **Ledger Hack:** سرقت اطلاعات مشتریان کیف پول سخت‌افزاری Ledger و حمله فیشینگ گسترده به ایمیل قربانیان
- **Cryptojacking:** ده‌ها میلیون کامپیوتر قربانی بدافزار استخراج مخفی مونرو
- **Clipboard Malware:** در ایران و جهان نمونه‌های بسیاری وجود داشته که کاربران به اشتباه رمزارز خود را به آدرس هکر منتقل کرده‌اند.

۱۰.۶ راه‌های پیشگیری و مقابله با بدافزار و حمله هکری

۱ .**استفاده از آنتی‌ویروس و بروزرسانی سیستم عامل:**
همیشه از آنتی‌ویروس به‌روز و سیستم عامل و نرم‌افزارهای آپدیت‌شده استفاده کنید.

۲ .**دانلود فقط از منابع معتبر:**
هرگز نرم‌افزار، کیف پول یا افزونه را از سایت یا کانال غیررسمی دریافت نکنید.

۳ .**فعال‌سازی احراز هویت دومرحله‌ای:(2FA)**
حتی در صورت افشای رمز عبور، لایه امنیتی اضافه‌تری خواهید داشت.

۴ .**عدم نگهداری کل دارایی در صرافی‌ها:**
دارایی رمزارزی خود را در کیف پول‌های امن، به ویژه سخت‌افزاری یا کاغذی، نگهداری کنید.

۵ .**بررسی آدرس قبل از انتقال وجه:**
هر بار قبل از ارسال رمزارز، آدرس مقصد را چند بار چک کنید و آن را تایپ کنید.

۶ .**عدم باز کردن لینک‌ها یا فایل‌های مشکوک:**
به پیام‌ها و ایمیل‌های ناشناس پاسخ ندهید و فایل‌های پیوست را باز نکنید.

۷ .**پشتیبان‌گیری (Backup) منظم از کیف پول و عبارت بازیابی:**
همیشه از اطلاعات مهم نسخه پشتیبان تهیه کنید و آن را به صورت آفلاین و امن نگه دارید.

۸ .**استفاده از مرورگر و سیستم مجزا برای تراکنش‌های رمزارزی:**
برای افزایش امنیت، انجام تراکنش‌ها را در سیستم یا مرورگر اختصاصی و با پلاگین‌های محدود انجام دهید.

پرسش و پاسخ فصل دهم

۱ .**پرسش:**
مهم‌ترین راه نفوذ بدافزار به سیستم کاربران چیست؟
پاسخ:
دانلود و نصب نرم‌افزار، افزونه یا فایل‌های ناشناس و آلوده از اینترنت یا کانال‌های غیررسمی.

۲ .**پرسش:**

آیا آنتی‌ویروس به تنهایی برای جلوگیری از هک کافی است؟

پاسخ:

خیر؛ آنتی‌ویروس یک لایه امنیتی مهم است، اما عادات کاربری صحیح، بروزرسانی و رعایت امنیت رمز و اطلاعات نیز ضروری‌اند.

۳ .**پرسش:**

بهترین روش نگهداری دارایی رمزارزی با امنیت بالا چیست؟

پاسخ:

استفاده از کیف پول سخت‌افزاری معتبر و نگهداری عبارت بازیابی به صورت آفلاین و امن.

تمرین عملی فصل دهم

۱ .**تحلیل یک حمله واقعی:**

یکی از حملات هکری مشهور به صرافی یا پلتفرم رمزارزی را جستجو و علل موفقیت هکرها را تحلیل کنید.

۲ .**شناسایی بدافزار:**

نمونه یک بدافزار رمزارزی) مانند کیف پول تقلبی، ClipBoard Hijackerیا (Keylogger را بررسی و نشانه‌های آن را فهرست کنید.

۳ .**چک‌لیست پیشگیری:**

یک چک‌لیست پنج‌مرحله‌ای برای افزایش امنیت دارایی‌های رمزارزی بنویسید.

جدول مقایسه‌ای: بدافزار، حمله هکری و فیشینگ

فیشینگ	حمله هکری	بدافزار	ویژگی
جعل سایت/ایمیل و فریب	نفوذ مستقیم به سیستم یا پلتفرم	نصب نرم‌افزار مخرب	شیوه اجرا
سرقت اطلاعات حساس	سرقت دارایی یا تخریب سیستم	سرقت اطلاعات، استخراج رمزارز	هدف اصلی
وارد کردن اطلاعات	معمولاً بی‌خبر از حمله	دانلود/نصب/اجرا	نقش کاربر
بله	تا حدی	بله	قابل پیشگیری با آموزش
عدم افشای اطلاعات	امنیت سرور و کدنویسی	آنتی‌ویروس، مراقبت دانلود	راه مقابله

جمع‌بندی تصویری فصل دهم

- دانلود نرم‌افزار فقط از منابع رسمی و معتبر؛
- آنتی‌ویروس به‌روز، سیستم عامل آپدیت و رعایت نکات امنیتی الزامی است؛
- نگهداری رمزارز در کیف پول امن و استفاده از FA2؛
- هرگز لینک و فایل مشکوک را باز نکنید؛
- امنیت رمزارز، ترکیبی از ابزار، آموزش و عادت درست است.

فصل یازدهم: نشانه‌های پروژه‌های مشکوک و راه‌های شناسایی آن‌ها

How to Spot Suspicious Crypto Projects

۱۱.۱ چرا شناسایی پروژه‌های مشکوک اهمیت دارد؟

بازار رمزارز، به‌ویژه با ماهیت غیرمتمرکز و جهانی خود، محیطی بسیار جذاب برای نوآوری و سرمایه‌گذاری است؛ اما این محیط به همان اندازه برای کلاهبرداران، پروژه‌های جعلی و تیم‌های بی‌نام‌ونشان نیز وسوسه‌کننده است.
در بسیاری از موارد، نشانه‌های هشداردهنده از همان ابتدا قابل شناسایی است؛ اما طمع سود بالا، جو هیجان یا تبلیغات فریبنده باعث می‌شود سرمایه‌گذاران چشم خود را بر این نشانه‌ها ببندند.
شناسایی و بررسی دقیق پروژه‌ها، مهم‌ترین گام در کاهش ریسک و جلوگیری از ضررهای مالی و اعتباری است.

۱۱.۲ مهم‌ترین نشانه‌های یک پروژه مشکوک رمزارزی

الف (تیم ناشناس یا بدون سابقه معتبر

- اسامی افراد تیم فقط نام کوچک یا مستعار است؛ عکس‌ها یا پروفایل‌ها جعلی یا با عکس‌های استوک.
- جستجوی نام اعضا در لینکدین یا شبکه‌های حرفه‌ای نتیجه خاصی ندارد یا پروفایل‌ها تازه ساخته شده‌اند.
- عدم ارائه اطلاعات تماس معتبر و شفاف) ایمیل‌های عمومی مثل gmail یا بدون دامنه رسمی.(

ب (وایت‌پیپر یا اسناد پروژه غیرحرفه‌ای یا مبهم

- وایت‌پیپر کلی، کپی از سایر پروژه‌ها، بدون جزییات فنی، نقشه راه یا مدل اقتصادی شفاف.
- وعده‌های مبهم مانند "انقلابی در بلاکچین" بدون توضیح مکانیزم اجرایی و فنی.

- نبود شفافیت درباره نحوه توزیع توکن، تأمین مالی و درآمدزایی پروژه.

ج (تبلیغات اغراق‌آمیز و وعده سود قطعی

- وعده رشد چند صد یا چند هزار درصدی در مدت کوتاه.
- تضمین سود بدون ریسک یا وعده بازگشت اصل سرمایه در هر شرایطی.
- استفاده از واژه‌هایی مثل "فرصت استثنایی"، "بدون ضرر"، "دریافت سود مطمئن" و...

د (تاریخچه نامشخص و نبود محصول واقعی

- پروژه فقط وعده می‌دهد و هیچ نسخه دموی محصول یا سرویس قابل آزمایش ارائه نمی‌کند.
- هیچ ویدیوی عملیاتی از کارکرد پروژه، تست‌نت یا Proof of Concept منتشر نشده است.
- تمام فعالیت‌ها فقط در حد برنامه‌ریزی و طرح گرافیکی است.

هـ (ساختار پانزی یا هرمی پنهان

- تأکید مداوم بر جذب زیرمجموعه یا ارائه پاداش برای دعوت دیگران.
- سوددهی صرفاً وابسته به ورود افراد جدید و نه توسعه واقعی یا فروش محصول.
- شبکه‌سازی اجباری یا معرفی "سیستم بازاریابی پاداشی" برای رشد سریع.

و (عدم شفافیت در قرارداد هوشمند، کد یاAudit

- کد منبع پروژه یا قرارداد هوشمند غیرقابل دسترسی یا مخفی است.
- نبود گزارش Audit معتبر از شرکت‌های امنیتی شناخته‌شده.

- قراردادها فقط روی سایت خود پروژه یا گیت‌هاب ناشناس آپلود شده‌اند.

ز (حجم مشکوک معاملات یا پامپ مصنوعی قیمت

- رشد ناگهانی قیمت توکن در بازه زمانی کوتاه بدون دلیل مشخص.
- حجم معاملات غیرواقعی یا شواهدی از معاملات ساختگی.(Wash Trading)
- نبود نقدینگی کافی یا عدم امکان فروش آزادانه توکن در صرافی‌های معتبر.

ح (اطلاعات تماس و آدرس فیزیکی نامعتبر

- آدرس دفتر پروژه قابل ردیابی نیست یا مربوط به مکان‌های عمومی (مثلاً کافی‌شاپ، دفتر کار اشتراکی).
- شماره تماس و ایمیل پاسخ‌گو نیستند.
- نبود حضور در رویدادها، کنفرانس‌ها یا اخبار رسمی.

ط (پوشش خبری جعلی یا پرداخت‌شده

- پوشش رسانه‌ای فقط در سایت‌های تبلیغاتی، بلاگ‌های بی‌نام یا کانال‌های تلگرامی.
- استفاده از رتبه‌بندی جعلی، جایزه‌های ساختگی یا رپورتاژ آگهی.
- نبود تاییدیه یا نظر مثبت از سوی کارشناسان مستقل و منابع معتبر جهانی.

۱۱.۳ مثال‌های واقعی از پروژه‌های مشکوک

مثال ۱BitConnect :

پروژه‌ای که با وعده سود ثابت و روزانه، میلیون‌ها دلار جذب کرد؛ اما تیم توسعه، ناشناس و محصول فقط یک پلتفرم ویدئویی تبلیغاتی بود. پس از فروپاشی، تمام نشانه‌های فوق آشکار شد.

مثال ۲: پروژه Pincoin وiFan

با تبلیغات شدید و پوشش خبری ساختگی، بدون ارائه محصول و شفافیت تیم، سرمایه‌گذاران زیادی را فریب داد و در نهایت، سایت‌ها و تیم پروژه ناپدید شدند.

مثال ۳Scam Token :ها

توکن‌هایی که در صرافی‌های غیرمعتبر لیست می‌شوند و پس از پامپ ناگهانی، امکان فروش وجود ندارد یا قیمت به صفر می‌رسد.

۱۱.۴ راه‌های عملی شناسایی پروژه‌های مشکوک و افزایش امنیت

۱ .**تحقیق عمیق درباره تیم و سوابق:**
اسامی، پروفایل‌ها و سابقه تیم را در سایت‌های حرفه‌ای و پروژه‌های قبلی جستجو کنید.

۲ .**بررسی اسناد و وایت‌پیپر:**
به جزئیات، مدل درآمدی، نقشه راه، توزیع توکن و فناوری پروژه توجه کنید.

3. **مطالعه ریویو و نظرات کاربران:**
   سایت‌هایی مانندReddit ، Bitcointalk، Trustpilotو انجمن‌های تخصصی پر از نظرات و هشدار کاربران با تجربه است.

4. **بررسی کد و گزارش:Audit**
   اگر پروژه قرارداد هوشمند دارد، کد را روی گیت‌هاب و Audit شرکت‌های معتبر بررسی کنید.

5. **آزمایش محصول یا پلتفرم:**
   نسخه دموی واقعی یا تست‌نت را بررسی کنید. فقط عکس و فیلم تبلیغاتی ملاک نیست.

6. **پرهیز از پروژه‌هایی با تبلیغات وسوسه‌برانگیز و وعده سود قطعی:**
در بازار رمزارز، هیچ تضمینی برای سود سریع و بدون ریسک وجود ندارد.

7. **سوال کردن و ارتباط با تیم پروژه:**
از تیم پروژه سوال‌های تخصصی بپرسید و واکنش و پاسخگویی آنان را ارزیابی کنید.

8. **دوری از پروژه‌هایی که اطلاعات تماس، آدرس یا پشتیبانی شفاف ندارند.**

9. **بررسی حضور پروژه در رویدادها و رسانه‌های معتبر:**
پروژه‌های جدی معمولاً در کنفرانس‌ها و رسانه‌های تخصصی حضور دارند.

پرسش و پاسخ فصل یازدهم

۱ .**پرسش:**
آیا می‌توان به‌تنهایی بر اساس وایت‌پیپر درباره اعتبار پروژه تصمیم گرفت؟
پاسخ:
خیر؛ باید تیم، محصول، کد، نظرات کاربران و فعالیت پروژه را نیز بررسی کرد.

۲ .**پرسش:**
نشانه‌های کلیدی یک تیم جعلی یا ناشناس چیست؟
پاسخ:
اسامی بدون پروفایل معتبر، عکس‌های استوک، نبود سوابق شغلی و حضور آنلاین مشکوک.

۳ .**پرسش:**
بهترین راه تست عملی یک پروژه چیست؟
پاسخ:
استفاده از نسخه دموی محصول، تست‌نت یا امکاناتی که نیاز به افشای اطلاعات حساس یا واریز مبالغ سنگین نداشته باشد.

تمرین عملی فصل یازدهم

۱ .**شناسایی پروژه مشکوک:**
یک پروژه جدید رمزارزی را انتخاب و تمام نشانه‌های مشکوک فوق را در آن بررسی کنید. نتایج را تحلیل و جمع‌بندی کنید.

۲ .**مطالعه موردی:**
داستان یک پروژه اسکم) مانند BitConnect یا (Pincoin را بخوانید و فهرستی از نشانه‌های هشداردهنده آن تهیه کنید.

۳ .**چک‌لیست عملی:**
یک چک‌لیست پنج‌مرحله‌ای برای شناسایی پروژه‌های مشکوک و اسکم بنویسید.

جدول مقایسه‌ای: پروژه معتبر، پروژه مشکوک و پروژه اسکم

ویژگی	پروژه معتبر	پروژه مشکوک	پروژه اسکم
تیم توسعه‌دهنده	شفاف، پروفایل کامل	ناقص، گاهی ناشناس	ناشناس یا جعلی
وایت‌پیپر و مستندات	دقیق، شفاف، فنی	مبهم یا تکراری	تبلیغاتی، کپی یا بی‌ارزش
محصول/نسخه دمو	نسخه واقعی و عملیاتی	نسخه آزمایشی مشکوک	صرفاً وعده یا تصویرسازی
کد و گزارشAudit	عمومی و معتبر	ناقص یا نامشخص	مخفی یا تقلبی
تبلیغات	معقول و علمی	پرحجم و اغراق‌آمیز	فریبنده و وسوسه‌برانگیز
وعده سود	منطقی و شفاف	نیمه‌شفاف، گاهی غیرواقعی	قطعی، غیرواقعی و تضمینی

جمع‌بندی تصویری فصل یازدهم

- تیم شفاف، محصول واقعی و مدل اقتصادی روشن، سه رکن پروژه معتبر است.
- وعده سود قطعی، تبلیغات پرهیجان و اسناد مبهم، زنگ خطر جدی هستند.
- هیچ پروژه‌ای بدون تحقیق، تست عملی و بررسی جامعه کاربران، قابل اعتماد نیست.
- طمع و عجله، بزرگ‌ترین دشمنان امنیت مالی شما هستند.

فصل دوازدهم: استانداردها و ابزارهای امنیتی برای مقابله با کلاهبرداری

Security Standards & Tools to Combat Crypto Scams

۱۲.۱ چرا امنیت در بازار رمزارز حیاتی است؟

رمزارزها با وجود پتانسیل بالای سودآوری، به دلیل ماهیت غیرمتمرکز، برگشت‌ناپذیری تراکنش‌ها، و نبود نهاد نظارتی مرکزی، نیازمند رعایت استانداردهای ویژه امنیتی هستند.
یک اشتباه ساده یا سهل‌انگاری کوچک می‌تواند منجر به از دست رفتن تمام دارایی دیجیتال شود.
بنابراین، شناخت ابزارها و استانداردهای امنیتی و به‌کارگیری آن‌ها برای تمام فعالان بازار ضروری است.

۱۲.۲ مهم‌ترین استانداردها و اصول امنیت فردی

الف (مدیریت رمز عبور و عبارت بازیابی

- استفاده از رمز عبور قوی، ترکیبی از حروف بزرگ و کوچک، اعداد و نمادها
- عدم استفاده مجدد از یک رمز برای چند سرویس
- ذخیره آفلاین و امن عبارات بازیابی (Seed Phrase) و کلید خصوصی
- خودداری از ارسال یا ذخیره رمزها و Seed در ایمیل، پیام‌رسان یا فضای ابری
- استفاده از نرم‌افزارهای مدیریت رمز عبور معتبر) مانند Bitwarden یا 1 (Passwordتنها با رعایت ملاحظات امنیتی

ب (احراز هویت دومرحله‌ای(Two-Factor Authentication - 2FA

- فعال‌سازی 2 FAدر تمام صرافی‌ها و کیف پول‌های آنلاین
- استفاده از اپلیکیشن‌های تولیدکننده کد(Google Authenticator) ، (Authyبه‌جایSMS
- پشتیبان‌گیری از کدهای بازیابی 2 FAو نگهداری آن‌ها در محل امن

ج (تقسیم و توزیع دارایی‌ها

- عدم نگهداری کل دارایی در یک صرافی یا کیف پول
- استفاده از کیف پول سخت‌افزاری برای دارایی‌های اصلی
- انتقال مبالغ سنگین به کیف پول‌های آفلاین(cold wallet)
- نگهداری مقادیر کم برای ترید روزانه در کیف پول یا صرافی آنلاین

د (بروزرسانی مستمر نرم‌افزار و سیستم‌عامل

- آپدیت منظم سیستم‌عامل، مرورگر، کیف پول و اپلیکیشن‌های رمزارزی
- حذف نرم‌افزارها و افزونه‌های غیرضروری یا مشکوک
- استفاده از آنتی‌ویروس به‌روز و اسکن منظم سیستم

هـ (بررسی لینک و منابع دانلود

- دانلود کیف پول و نرم‌افزار فقط از سایت رسمی یا فروشگاه معتبر
- بررسی دامنه و نام توسعه‌دهنده قبل از نصب
- پرهیز از کلیک روی لینک‌های کوتاه‌شده یا ناشناس

و (پشتیبان‌گیری منظم

- یادداشت و نگهداری آفلاین کلیدهای خصوصی، Seed Phraseو کدهای بازیابی
- نگهداری نسخه پشتیبان در محل امن و غیرقابل دسترسی برای دیگران (مثلاً گاوصندوق)

۱۲.۳ ابزارها و راهکارهای امنیتی کاربردی

الف (کیف پول سخت‌افزاری(Hardware Wallets)

ابزاری فیزیکی برای ذخیره امن کلید خصوصی که حتی در صورت آلودگی سیستم، امکان سرقت کلید وجود ندارد.
نمونه‌ها: Ledger Nano S/X ،. Trezor One/Model T، SafePal

ب (اپلیکیشن‌های مدیریت رمز عبور

برای ساخت، نگهداری و استفاده امن از رمزها وSeed Phrase
نمونه‌ها: Bitwarden ،. Password1، Keepass

ج (افزونه و اپلیکیشن احراز هویت(2FA)

تولید کدهای یکبار مصرف برای ورود امن به سایت‌ها
نمونه‌ها: Google Authenticator ،. Authy، Microsoft Authenticator

---

د (سرویس‌های شناسایی پروژه‌های اسکم و امنیت قرارداد هوشمند

- **سایت‌هایی برای شناسایی پروژه اسکم**: Scamsniper ،. TokenSniffer، RugDoc
- **بررسی گزارش Audit قرارداد هوشمند**: CertiK ،. SlowMist، PeckShield
- **بررسی وضعیت توکن و نقدینگی**: Dextools ،. Etherscan، BscScan

---

هـ (آنتی‌ویروس و امنیت سیستم

استفاده از نرم‌افزار آنتی‌ویروس قوی و قابلیت ضدفیشینگ و ضدبدافزار
نمونه‌ها Kaspersky :، Bitdefender، ESET، Windows Defender

و (ابزارهای مشاهده و تحلیل تراکنش‌ها

امکان رهگیری و تحلیل تراکنش‌های مشکوک، کیف پول‌های مشکوک و آدرس‌های بلک‌لیست
نمونه‌ها Etherscan :، Blockchair،) Chainalysisبرای کاربران حرفه‌ای(

۱۲.۴ توصیه‌های عملی برای ارتقای امنیت در بازار رمزارز

۱ .**تردید در برابر هر وعده سود عجیب، تبلیغ فریبنده یا پروژه ناشناس**
۲ .**چندلایه کردن امنیت) رمز قوی + 2 + FAکیف پول سخت‌افزاری(**
۳ .**آموزش مستمر درباره تهدیدها، بدافزارها و روش‌های نوین کلاهبرداری**
۴ .**استفاده از ابزارهای اعتبارسنجی پروژه قبل از هر سرمایه‌گذاری**
۵ .**تست پروژه با مبلغ کم قبل از هر انتقال سنگین**
۶ .**پرهیز از به‌اشتراک‌گذاری اسکرین‌شات، Seed Phraseیا اطلاعات حساس در شبکه‌های اجتماعی**
۷ .**پرهیز از نگهداری کلید خصوصی در ایمیل یا فضای ابری حتی با رمزگذاری**

۱۲.۵ مثال‌های کاربردی

- **کیف پول سخت‌افزاری :**کاربری که برای دارایی‌های اصلی خود از Ledger استفاده می‌کند و عبارت بازیابی را روی کاغذ و در محل فیزیکی جداگانه نگهداری می‌کند، احتمالاً قربانی بدافزار یا هک آنلاین نمی‌شود.
- **2FAو مدیریت رمز :**فردی که برای همه حساب‌هایش رمزهای متفاوت، قوی و 2 FAفعال دارد، حتی در صورت افشای یکی از رمزها یا هک یک ایمیل، دارایی رمزارزی او امن می‌ماند.

- **بررسی پروژه قبل از سرمایه‌گذاری :**استفاده از سایت‌هایی مثلTokenSniffer ، RugDocو بررسی گزارشAudit ، بسیاری از اسکم‌ها را پیش از سرمایه‌گذاری آشکار می‌کند.

پرسش و پاسخ فصل دوازدهم

۱ .**پرسش:**
آیا نگهداری کل دارایی در صرافی‌های متمرکز، کار امنی است؟
پاسخ:
خیر؛ صرافی‌های متمرکز بارها هک شده‌اند و بهتر است دارایی اصلی را در کیف پول امن نگهداری کنید.

۲ .**پرسش:**
بهترین روش نگهداری عبارت بازیابی چیست؟
پاسخ:
نگهداری آفلاین، یادداشت روی کاغذ و قرار دادن آن در محل امن (مثلاً گاوصندوق)، دور از دسترس دیگران.

۳ .**پرسش:**
چگونه از اسکم بودن یک پروژه مطمئن شویم؟
پاسخ:
تحقیق درباره تیم، وایت‌پیپر، گزارشAudit ، ریویو کاربران، ابزارهای اعتبارسنجی و آزمودن پروژه با مبلغ کم پیش از هر سرمایه‌گذاری جدی.

تمرین عملی فصل دوازدهم

۱ .**لیست ابزارهای امنیتی:**
یک کیف پول سخت‌افزاری، یک اپلیکیشن مدیریت رمز و یک سایت اعتبارسنجی پروژه اسکم معرفی کنید و کاربرد هر کدام را توضیح دهید.

۲ .**تحلیل پروژه:**
یک پروژه رمزارزی جدید را با ابزارهای امنیتی بررسی کنید و نتایج را خلاصه کنید.

۳ .**چک‌لیست عملی:**
یک چک‌لیست ۵ مرحله‌ای برای رعایت امنیت کامل در فعالیت‌های رمزارزی خود بنویسید.

جدول مقایسه‌ای: ابزارهای امنیتی رمزارز

نمونه/توضیح	معایب	مزایا	ابزار / راهکار
Ledger, Trezor	هزینه خرید، نیاز به نگهداری فیزیکی	امنیت بالا، آفلاین، غیرقابل هک آنلاین	کیف پول سخت‌افزاری
Bitwarden, 1Password	وابستگی به یک اپ، نیاز به بکاپ	ساخت رمز قوی، نگهداری امن، ذخیره متعدد	اپلیکیشن مدیریت رمز
Authy, Google Auth	گم شدن گوشی یا کدها، نیاز به پشتیبان	لایه امنیتی اضافی، مقابله با هک ساده	2FA
Kaspersky, Bitdefender	هزینه سالانه، امکان تشخیص کاذب	مقابله با بدافزار و فیشینگ	آنتی‌ویروس
TokenSniffer, RugDoc	همیشه کامل نیستند، نیاز به تحقیق بیشتر	شناسایی سریع اسکم و ضعف امنیتی	سایت‌های اعتبارسنجی پروژه

جمع‌بندی تصویری فصل دوازدهم

- رمز عبور قوی، FA2، کیف پول سخت‌افزاری و مدیریت رمزها چهار اصل امنیت هستند.
- ابزارهای اعتبارسنجی پروژه و گزارشAudit ، ضامن پیشگیری از اسکم و پروژه‌های خطرناک‌اند.

- امنیت رمزارز مسئولیت شخصی شماست؛ آموزش، ابزار مناسب و عادت‌های صحیح، ضامن بقای دارایی دیجیتال شماست.

فصل سیزدهم: قوانین، مقررات و نقش نهادهای نظارتی در پیشگیری از کلاهبرداری رمزارزی

Regulation, Law & The Role of Regulatory Bodies in Crypto Scam Prevention

۱۳.۱ چرا قوانین و مقررات در بازار رمزارز اهمیت دارد؟

بازار رمزارزها به دلیل ماهیت غیرمتمرکز، جهانی و نوآورانه خود، اغلب خارج از حوزه نظارت سنتی نهادهای مالی قرار می‌گیرد. همین مسئله فرصت مناسبی برای رشد فناوری و سرمایه‌گذاری فراهم آورده، اما همزمان بستری مناسب برای فعالیت کلاهبرداران و متخلفین ایجاد کرده است.
قوانین و مقررات روشن، نقش حیاتی در حمایت از حقوق سرمایه‌گذاران، شفافیت بازار و کاهش جرایم مالی دارند.
همچنین وجود نهادهای نظارتی فعال، امکان پیگیری حقوقی و کاهش ریسک کلاهبرداری را افزایش می‌دهد.

۱۳.۲ وضعیت مقررات رمزارزها در جهان

الف (کشورهای با رویکرد حمایتی و قانون‌گذاری شفاف

کشورهایی مانند سوئیس، سنگاپور، ژاپن و امارات، با ایجاد چارچوب‌های قانونی روشن، صرافی‌ها و پروژه‌های رمزارزی را ملزم به رعایت استانداردهای ضدپولشویی (AML) و شناخت مشتری (KYC) می‌کنند. این کشورها با صدور مجوز، ثبت شرکت و کنترل تراکنش‌ها، بستر نسبتا امن و قانونی برای فعالیت ایجاد کرده‌اند.

ب (کشورهای با محدودیت یا ممنوعیت کامل

در برخی کشورها مانند چین، هند، مراکش یا الجزایر، خرید و فروش یا نگهداری رمزارز ممنوع یا با محدودیت شدید همراه است. هدف این کشورها جلوگیری از جرایم مالی و پولشویی است اما ممنوعیت مطلق معمولاً منجر به بازارهای زیرزمینی و افزایش ریسک می‌شود.

ج (کشورهای خاکستری (فاقد مقررات مشخص)

در بسیاری از کشورها (از جمله ایران)، قوانین جامع و شفافی برای رمزارزها وجود ندارد یا در حال تدوین است. همین خلأ قانونی، فضا را برای فعالیت اسکم‌ها و کلاهبرداری‌ها باز گذاشته است.

۱۳.۳ مهم‌ترین قوانین و مقررات رایج در حوزه رمزارز

الف (ضدپولشویی(AML: Anti-Money Laundering)

صرافی‌ها، پروژه‌ها و نهادهای رمزارزی موظفند تراکنش‌های مشکوک را شناسایی، ثبت و به مراجع قانونی گزارش کنند.

ب (شناخت مشتری(KYC: Know Your Customer)

فرایندی برای تایید هویت کاربران و جلوگیری از استفاده مجرمانه از پلتفرم‌ها. شامل احراز هویت با مدارک شناسایی و بررسی سوابق مالی است.

ج (گزارش‌دهی تراکنش‌های بزرگ

در بسیاری کشورها، تراکنش‌های رمزارزی با مبلغ بالا باید به نهادهای دولتی گزارش داده شود.

د (مجوز فعالیت و ثبت شرکت

پروژه‌ها و صرافی‌ها برای فعالیت رسمی ملزم به ثبت قانونی و اخذ مجوز از مراجع ذی‌ربط هستند.

هـ (حمایت از مصرف‌کننده و شفافیت اطلاعات

ارائه اطلاعات شفاف به کاربران، هشدار درباره ریسک سرمایه‌گذاری و آموزش عمومی از وظایف صرافی‌ها و پلتفرم‌هاست.

۱۳.۴ نقش نهادهای نظارتی، پلیس و دستگاه قضایی

الف (نهادهای بین‌المللی

- **گروه ویژه اقدام مالی (FATF):** تدوین استانداردهای جهانی برای مبارزه با پولشویی و تامین مالی تروریسم
- **سوئیس (FINMA)، سنگاپور (MAS)، انگلستان (FCA)، آمریکا (FinCEN):** نمونه‌هایی از نهادهای مالی نظارتی

ب (پلیس سایبری و پلیس بین‌الملل (اینترپل)

بررسی جرایم پیچیده، ردیابی تراکنش‌های مشکوک و پیگیری کلاهبرداران فرامرزی.

ج (دادگاه‌ها و سازوکارهای حل اختلاف

برخی کشورها دادگاه‌های تخصصی یا داوری رمزارزی برای حل اختلافات و جبران خسارت دارند.

۱۳.۵ مثال‌های واقعی از نقش قانون و نظارت در مبارزه با کلاهبرداری رمزارزی

- **پرونده BitConnect:** پیگرد بین‌المللی مدیران پروژه، بازگرداندن بخشی از سرمایه قربانیان و صدور احکام زندان
- **تعطیلی صرافی Mt.Gox:** پیگیری قضایی گسترده در ژاپن برای رسیدگی به مطالبات قربانیان
- **بررسی ICO ها و پرونده‌های SEC آمریکا:** جریمه یا تعطیلی پروژه‌های فاقد مجوز یا فریبکار، احضار چهره‌های تبلیغ‌کننده اسکم‌ها

۱۳.۶ چالش‌ها و محدودیت‌های قانونی در مقابله با کلاهبرداری رمزارزی

۱. **ماهیت فرامرزی و غیرمتمرکز رمزارزها**
بسیاری از پروژه‌ها و کلاهبرداران در کشورهای فاقد مقررات مستقرند و پیگیری حقوقی را دشوار می‌کند.

۲. **فقدان قوانین جامع و هماهنگ جهانی**
اختلاف قوانین و سیاست‌های کشورها، ریسک فعالیت در بازار رمزارز را افزایش می‌دهد.

۳ .**عدم آموزش عمومی کافی**
نبود آموزش کافی درباره مقررات، ریسک و حقوق کاربران، آگاهی جامعه را پایین نگه می‌دارد.

۴ .**شکل‌گیری بازارهای زیرزمینی و ابزارهای مخفی‌کاری**
فناوری‌هایی مانند کوین‌های پرایوسی یا سرویس‌های میکسینگ ردیابی مجرمان را سخت‌تر می‌کند.

۱۳.۷ راهکارها و توصیه‌ها برای کاربران و فعالان بازار

۱ .**آگاهی از وضعیت قانونی رمزارزها در کشور خود**
همیشه مقررات و هشدارهای مراجع قانونی را پیگیری کنید.

۲ .**فعالیت در پلتفرم‌های دارای مجوز و ثبت‌شده**
استفاده از صرافی‌ها و پروژه‌هایی که تحت نظارت یا ثبت رسمی هستند، امنیت شما را افزایش می‌دهد.

۳ .**گزارش کلاهبرداری به مراجع رسمی**
هرگونه سوءاستفاده، سایت یا پروژه مشکوک را به پلیس فتا (در ایران) یا نهادهای سایبری اطلاع دهید.

۴ .**مطالعه قراردادهای کاربری و شرایط خدمات قبل از سرمایه‌گذاری**
آگاهی از حقوق و تعهدات قانونی پیش از هر فعالیت مهم است.

۵ .**مشورت با وکیل یا کارشناس حقوقی در صورت وقوع مشکل یا ضرر**

پرسش و پاسخ فصل سیزدهم

۱ .**پرسش:**
چرا مقررات رمزارزها در برخی کشورها سختگیرانه و در برخی دیگر آزادانه است؟
پاسخ:
سیاست‌های اقتصادی، نگرانی از پولشویی، کنترل سرمایه و رویکرد کشورها نسبت به نوآوری مالی، تعیین‌کننده قوانین است.

۲ .**پرسش:**

در صورت قربانی شدن اسکم رمزارزی، چه باید کرد؟

پاسخ:

مستندسازی کامل، گزارش سریع به پلیس سایبری و در صورت امکان پیگیری قضایی یا ثبت در پلتفرم‌های هشداردهنده بین‌المللی.

۳ .**پرسش:**

آیا قوانین کافی است که از همه اسکم‌ها جلوگیری شود؟

پاسخ:

خیر؛ قوانین مهم‌اند اما بدون آموزش، آگاهی و رعایت نکات امنیتی فردی، باز هم امکان قربانی شدن وجود دارد.

تمرین عملی فصل سیزدهم

۱ .**بررسی وضعیت مقررات رمزارزها در کشور خود:**

اطلاعات مربوط به مجوز صرافی‌ها، ممنوعیت‌ها و هشدارهای بانک مرکزی یا پلیس را گردآوری کنید.

۲ .**مطالعه یک پرونده کلاهبرداری رمزارزی:**

روند پیگیری، بازگرداندن دارایی و نقش نهادهای نظارتی را تحلیل کنید.

۳ .**چک‌لیست عملی:**

یک چک‌لیست ۵ مرحله‌ای برای فعالیت امن و قانونی در بازار رمزارز کشور خود تهیه کنید.

جدول مقایسه‌ای: وضعیت مقررات رمزارز در جهان

معایب	مزایا	وضعیت مقررات	کشور/منطقه
فرایند ثبت و نظارت پیچیده	جذب سرمایه، کاهش اسکم، حمایت کاربر	قانون‌گذاری شفاف	سوئیس، سنگاپور
رشد بازار سیاه، فرار سرمایه	کنترل جرایم مالی، شفافیت دولت	ممنوعیت یا محدودیت	چین، هند
دشواری ورود پروژه‌های نوپا	حمایت کاربر، پیگرد حقوقی	مقررات پویا و سختگیرانه	آمریکا، اتحادیه اروپا
افزایش ریسک، رشد اسکم‌ها	آزادی عمل اولیه، نوآوری تکنولوژیک	فاقد مقررات روشن	ایران و کشورهای فاقد قانون

جمع‌بندی تصویری فصل سیزدهم

- وجود قوانین شفاف، مجوز و نظارت، ریسک کلاهبرداری را کاهش می‌دهد؛
- انتخاب پلتفرم دارای مجوز و ثبت‌شده، نخستین گام برای سرمایه‌گذاری امن است؛
- آموزش و آگاهی فردی مکمل مقررات است؛
- پیگیری حقوقی و گزارش سریع به مراجع ذی‌ربط در صورت بروز مشکل ضروری است؛
- آینده بازار رمزارز نیازمند تعامل هوشمندانه میان قانون‌گذاری، فناوری و آموزش است.

فصل چهاردهم: آینده امنیت و روندهای جدید کلاهبرداری در بازار رمزارز

The Future of Security & Emerging Crypto Scam Trends

۱۴.۱ مقدمه: بازار رمزارز، همیشه یک گام جلوتر؟

تاریخچه بازار رمزارز نشان می‌دهد که فناوری و نوآوری مالی همیشه دو رو دارد: فرصت برای رشد و خلق ثروت، و فرصتی همیشگی برای کلاهبرداران. همان‌گونه که امنیت کیف پول‌ها و قراردادهای هوشمند رشد کرده، روش‌های کلاهبرداری نیز روزبه‌روز پیچیده‌تر و خلاقانه‌تر شده است.
در این فصل، به مهم‌ترین روندهای آینده امنیت و تهدیدهای جدید دنیای رمزارز پرداخته می‌شود تا خواننده همیشه یک گام جلوتر باشد.

۱۴.۲ روندهای نوین کلاهبرداری در بازار رمزارز

الف (کلاهبرداری‌های هوش مصنوعی(AI-powered Scams)

با گسترش ابزارهای هوش مصنوعی، کلاهبرداران از چت‌بات‌های هوشمند برای فریب کاربران، تولید محتوای جعلی(Deepfake) ، ساخت پروفایل‌های اجتماعی پیچیده و حتی شبیه‌سازی صدای افراد مشهور جهت فریب کاربران استفاده می‌کنند.

نمونه:
ایجاد ویدیوهای جعلی از چهره‌های مشهور رمزارزی که یک پروژه را تأیید می‌کنند یا تماس‌های صوتی خودکار با صدای مدیران پروژه‌ها برای درخواست اطلاعات حساس.

ب (کلاهبرداری‌های چندزنجیره‌ای و بین‌پلتفرمی(Cross-chain & Multi-platform Scams)

با رشد پروژه‌های مولتی‌چین و پل‌های بین بلاکچینی(Bridge) ، حملات و کلاهبرداری‌ها دیگر محدود به یک بلاکچین یا صرافی خاص نیست. مهاجمان با جابه‌جایی سریع دارایی‌ها بین شبکه‌ها یا سو استفاده از ضعف امنیتی پل‌ها، ردیابی و مقابله را بسیار سخت می‌کنند.

نمونه:
هک پل Wormhole بین اتریوم و سولانا که بیش از ۳۲۰ میلیون دلار سرقت شد.

ج (حملات به قراردادهای هوشمند پیچیده

کدهای قرارداد هوشمند هر روز پیشرفته‌تر می‌شوند، اما با افزایش پیچیدگی، نقاط ضعف امنیتی جدید پدیدار می‌شود. حملات مانندFlash Loan Attack ، حمله به اوراکل‌ها یا دستکاری قیمت‌ها، تهدیدهای جدی برای دیفای و کاربران عادی است.

نمونه:
حمله Flash Loan به پروتکل‌های دیفای که میلیون‌ها دلار فقط در چند ثانیه منتقل می‌شود.

د Social Engineering (پیشرفته و حملات روانشناسی

فیشینگ کلاسیک جای خود را به حملات چندلایه داده است: ترکیب تماس تلفنی، پیامک، ایمیل و شبکه اجتماعی، همه برای جلب اعتماد کاربر. مهاجمان با تحقیق درباره زندگی و فعالیت کاربران، حملات شخصی‌سازی‌شده طراحی می‌کنند.

هـ (اسکم‌های مبتنی بر NFT و متاورس

با رشد توکن‌های غیرقابل تعویض (NFT) و جهان‌های متاورس، فروشNFT های جعلی، پروژه‌های متاورس بدون پشتوانه و حملات به بازارهای NFT به شدت گسترش یافته است.

نمونه:
ایجاد بازار جعلیNFT ، پروژه‌های هنری بدون اصالت و کلاهبرداری‌های مرتبط با زمین مجازی و دارایی‌های متاورس.

و (کلاهبرداری مبتنی بر اپلیکیشن‌های غیرمتمرکز(dApp Scams

دپ‌های جعلی با ظاهر و کدنویسی مشابه پروژه‌های معتبر اما با کد مخرب یا پشت‌درهایی (Backdoor)برای سرقت دارایی‌ها ساخته می‌شوند. تشخیص این پروژه‌ها برای کاربر عادی بسیار دشوار است.

ز (کلاهبرداری با توکن‌های اجتماعی (Social Tokens) و DAO جعلی

پروژه‌هایی با شعار دموکراسی مالی و سرمایه‌گذاری جمعی (DAO) و توکن‌های اجتماعی، گاهی بدون شفافیت و حسابرسی، صرفاً برای جذب سرمایه ایجاد می‌شوند.

۱۴.۳ آینده ابزارها و راهکارهای امنیتی

۱ .گسترش ابزارهای هوشمند اعتبارسنجی و مانیتورینگ

- استفاده از هوش مصنوعی برای شناسایی رفتارهای مشکوک و هشدار سریع به کاربران
- اپلیکیشن‌ها و سایت‌های تحلیل قرارداد هوشمند و شناسایی پروژه‌های اسکم) مانندRugDoc ، ScamSniper)
- سامانه‌های اطلاع‌رسانی ریسک به‌صورت بلادرنگ

۲ .گسترش خدمات بیمه رمزارز و دیفای

- شرکت‌های بیمه‌گر، محصولات بیمه کیف پول و سرمایه‌گذاری روی پروژه‌های رمزارزی را توسعه خواهند داد تا ریسک سرقت و اسکم را کاهش دهند.

۳ .بهبود فرآیندهای احراز هویت (KYC) و اعتبارسنجی پروژه‌ها

- ادغام فناوری‌های بیومتریک، امضای دیجیتال و تایید هویت غیرمتمرکز (DID) در پلتفرم‌های رمزارزی

4. **آموزش مستمر و هوشمندسازی اطلاع‌رسانی عمومی**
    - ایجاد پلتفرم‌های آموزش امنیت، کمپین‌های جهانی هشدار اسکم و همکاری پروژه‌ها برای مبارزه با کلاهبرداری

۱۴.۴ نقش دولت‌ها و نهادهای جهانی در آینده بازار

- **ایجاد چارچوب‌های قانونی هوشمند و بین‌المللی:**
  کشورهای پیشرو به سمت ایجاد استانداردهای جهانی برای دیفای، NFT، متاورس و شناسایی سریع کلاهبرداران حرکت می‌کنند.
- **همکاری بین‌المللی برای ردیابی دارایی‌ها:**
  استفاده از فناوری بلاکچین برای همکاری پلیس‌ها و مراجع قضایی جهان در پیگیری جرایم مالی
- **توسعه رگولاتوری انعطاف‌پذیر:**
  قوانین باید با سرعت نوآوری فناوری حرکت کند و زمینه رشد، بدون ایجاد فضای مناسب برای کلاهبرداران، فراهم شود.

۱۴.۵ تهدیدها و فرصت‌های امنیتی آینده رمزارز

فرصت‌ها:

- افزایش شفافیت و دسترسی به اطلاعات با ابزارهای بلاکچین
- رشد آموزش و فرهنگ‌سازی درباره امنیت دیجیتال
- توسعه سرویس‌های بیمه و حمایت حقوقی از سرمایه‌گذاران
- ورود نهادهای معتبر جهانی برای استانداردسازی

تهدیدها:

- رشد حملات مبتنی بر هوش مصنوعی و مهندسی اجتماعی پیشرفته
- کلاهبرداری با پروژه‌های چندزنجیره‌ای و غیرمتمرکز
- حملات به قراردادهای هوشمند پیشرفته و پل‌های بلاکچینی
- ظهور بازارهای زیرزمینی پیچیده‌تر و اپلیکیشن‌های مخرب جدید

۱۴.۶ توصیه‌های حیاتی برای آینده

۱. **همیشه آموزش ببینید و به‌روز باشید.**
دانش و آگاهی کلید بقا در دنیای پرریسک رمزارز است.

۲. **قبل از هر سرمایه‌گذاری، ابزارها و ریسک‌ها را بشناسید.**
صرفاً بر اساس تبلیغات و توصیه اینفلوئنسرها وارد نشوید.

۳. **ابزارهای اعتبارسنجی، Auditو گزارش‌دهی اسکم را جدی بگیرید.**
از پلتفرم‌هایی با امنیت، شفافیت و اعتبار بالا استفاده کنید.

۴. **هوشمندانه از دارایی دیجیتال خود حفاظت کنید.**
تقسیم دارایی‌ها، کیف پول‌های امن و فعال‌سازی همه لایه‌های امنیتی

۵. **در صورت مشاهده یا تجربه اسکم، به سرعت اطلاع‌رسانی و گزارش کنید.**
این کار علاوه بر کمک به خودتان، امنیت کل جامعه را ارتقا می‌دهد.

پرسش و پاسخ فصل چهاردهم

۱. **پرسش:**
آیا هوش مصنوعی می‌تواند راهکار نهایی برای مقابله با اسکم‌های رمزارزی باشد؟
پاسخ:

هوش مصنوعی ابزار مهمی برای تشخیص رفتارهای مشکوک است، اما کلاهبرداران هم از آن استفاده می‌کنند. آموزش و فرهنگ‌سازی، مکمل فناوری است.

۲ .**پرسش:**
بزرگ‌ترین تهدید امنیتی آینده بازار رمزارز چیست؟
پاسخ:
ترکیب حملات هوش مصنوعی، پروژه‌های چندزنجیره‌ای و ضعف امنیت قراردادهای هوشمند پیچیده، مهم‌ترین تهدیدها هستند.

۳ .**پرسش:**
آیا پروژه‌های بیمه رمزارز می‌توانند همه ریسک‌ها را پوشش دهند؟
پاسخ:
بیمه می‌تواند خسارت‌های بخشی از ریسک‌ها را جبران کند اما جایگزین احتیاط و امنیت فردی نیست.

تمرین عملی فصل چهاردهم

۱ .**تحلیل یک روند کلاهبرداری جدید:**
یک نوع اسکم نوظهور) مثل Flash Loan Attack یا اسکم (NFT را جستجو و مراحل آن را تحلیل کنید.

۲ .**بررسی یک ابزار امنیتی آینده‌نگر:**
یک ابزار یا سرویس امنیتی جدید (مثلاً پلتفرم تحلیل رفتار بلاکچینی یا بیمه رمزارز) را معرفی و نقاط قوت و ضعف آن را شرح دهید.

۳ .**چک‌لیست آمادگی برای آینده:**
یک چک‌لیست پنج‌مرحله‌ای برای حفاظت دارایی در برابر اسکم‌های آینده تهیه کنید.

جدول مقایسه‌ای: اسکم‌های گذشته، حال و آینده بازار رمزارز

ویژگی	اسکم‌های گذشته	اسکم‌های فعلی	اسکم‌های آینده
ابزار اصلی	فیشینگ، هرمی، پانزی	دیفای اسکم، راگ‌پول، NFT	هوش مصنوعی، مولتی‌چین، متاورس
سطح پیچیدگی	پایین تا متوسط	متوسط تا بالا	بسیار بالا و چندلایه
سرعت گسترش	کند (شبکه‌ای)	سریع (شبکه‌های اجتماعی)	آنی، بین‌زنجیره‌ای و اتوماتیک
راه مقابله	آموزش، احتیاط	ابزارهای اعتبارسنجی، Audit	فناوری‌های هوشمند، همکاری جهانی
نقش کاربر	فریب سنتی	فریب تکنولوژیک و اجتماعی	هدف شخصی‌سازی‌شده و مبتنی بر داده

جمع‌بندی تصویری فصل چهاردهم

- آینده امنیت رمزارز، تلفیقی از نوآوری، ابزارهای هوشمند و آموزش مستمر خواهد بود.
- کلاهبرداران با فناوری حرکت می‌کنند؛ کاربر باید همیشه یک گام جلوتر باشد.
- تعامل میان فناوری، مقررات، بیمه و آگاهی اجتماعی، کلید سلامت آینده بازار است.
- دنیای رمزارز فرصت بی‌پایانی برای ثروت و کلاهبرداری است؛ انتخاب شماست که در کدام سمت بایستید.

جمع‌بندی نهایی و نتیجه‌گیری

Final Summary & Conclusion

نگاهی دوباره به مسیر طی‌شده

بازار رمزارز، دنیایی سرشار از نوآوری، فرصت و تحول است؛ اما این سرزمین جدید، همچون غرب وحشیِ دوران طلا، محل جولان ماجراجویان و سودجویان نیز هست. همان‌قدر که رمزارز می‌تواند به آزادی مالی و قدرت فردی منجر شود، در صورت غفلت و بی‌توجهی، می‌تواند موجب از دست رفتن دارایی، اعتماد و حتی آرامش زندگی شود.

در طول این کتاب، با انواع کلاهبرداری‌های رایج، از طرح پانزی و هرمی تا راگ‌پول، اسکمICO ، فیشینگ، بدافزار، کیف پول و صرافی جعلی، اسکم‌های شبکه اجتماعی، پروژه‌های مشکوک و... آشنا شدیم.
ابزارها و استانداردهای امنیتی، نقش نهادهای نظارتی و روندهای آینده کلاهبرداری را بررسی کردیم و یاد گرفتیم که امنیت در دنیای رمزارز، هرگز یک نقطه پایان ندارد.

کلیدهای بقا و موفقیت در دنیای رمزارز

۱ .**آگاهی و آموزش مستمر:**
دنیای رمزارزها با سرعتی حیرت‌انگیز تغییر می‌کند. تنها کاربری که همیشه در حال یادگیری است، می‌تواند در این بازار بقا یابد و از فرصت‌ها بهره‌مند شود.

۲ .**احتیاط و تردید سالم:**
هیچ سود سریعی بدون ریسک نیست. هر وعده سود عجیب، پیام‌های وسوسه‌برانگیز، یا تبلیغات پرزرق و برق باید با تردید جدی بررسی شود.

۳ .**استفاده از ابزارهای امنیتی و اعتبارسنجی:**
کیف پول سخت‌افزاری، FA2، رمز عبور قوی، بررسی گزارش Audit و استفاده از سایت‌های اعتبارسنجی، باید عادت همیشگی شما باشد.

4. **پرهیز از طمع و تصمیمات عجولانه:**
   بزرگ‌ترین قربانیان کلاهبرداری، کسانی بوده‌اند که با طمع سود سریع و بدون تحقیق کافی، سرمایه خود را در اختیار افراد ناشناس قرار دادند.
5. **همکاری و گزارش‌دهی برای افزایش امنیت جمعی:**
   با اطلاع‌رسانی و گزارش سریع پروژه‌ها و افراد مشکوک، به ارتقای امنیت کل جامعه رمزارز کمک کنید.

یک جمله کلیدی برای تمام فعالان بازار رمزارز

در بازار رمزارز، امنیت یک انتخاب روزانه است؛ نه یک حادثه تصادفی.

پیشنهاد پایانی به خواننده

- همیشه پیش از هر سرمایه‌گذاری یا انتقال دارایی، حتی برای کوچک‌ترین مبلغ، تحقیق و بررسی کن.
- از تجربه‌های دیگران درس بگیر؛ بسیاری پیش از تو مسیر را رفته‌اند و شکست خورده‌اند.
- آینده بازار رمزارز، متعلق به کسانی است که هوشمندانه، با احتیاط و مسئولیت‌پذیری حرکت می‌کنند.

کلاهبرداری با تتر از طریق اسمارت کانترکت(Smart Contract USDT Scam)

مکانیزم کار چگونه است؟

۱ .**ارسال توکن تتر به کیف پول کاربر**

- کلاهبردار توکن‌های تتر (USDT) را به ولت قربانی ارسال می‌کند.
- قربانی موجودی را در ولت خود می‌بیند و تصور می‌کند این تتر واقعی است و توسط شخص/سایت معتبری به او پرداخت شده است.

۲ .**تترها قابل برداشت به نظر می‌رسند، اما...**

- قربانی، چه به‌عنوان جایزه یا دریافت پول، وسوسه می‌شود تا این تترها را جابه‌جا کند یا خرج نماید.

۳ .**تترها در واقع تحت کنترل یک اسمارت کانترکت مخرب هستند**

- کلاهبردار، یک **قرارداد هوشمند سفارشی** طراحی کرده که به محض دریافت تتر در ولت قربانی، یا با هر تراکنش خاص) مثلاًSwap ، ارسال یا تایید تراکنش(، اجازه برداشت یا انتقال توکن را از ولت قربانی می‌گیرد.
- این قرارداد هوشمند به گونه‌ای طراحی شده که معمولاً با «Approve» یا «Allow» توکن، کاربر ناآگاهانه به قرارداد اجازه می‌دهد تترهایش را هر زمان دلخواه خارج کند.

۴ .**خروج دارایی پس از مدتی یا در یک تراکنش**

- پس از مدتی (مثلاً چند ساعت یا روز) یا با رخ دادن یک تراکنش خاص (مانند سواپ یا فروش)، تمام یا بخشی از تترهای ولت توسط قرارداد هوشمند به آدرس کلاهبردار منتقل می‌شود.
- حتی اگر کاربر قصد برداشت یا تبدیل این تترها را داشته باشد، تراکنش موفق نمی‌شود یا تترها بلافاصله به آدرس دیگری ارسال می‌شود.

چرا این اتفاق می‌افتد؟

- **Approveمخرب:**
  بسیاری از ولت‌ها برای استفاده از توکن (مثلاً در دیفای یا تبدیل)، ابتدا نیاز به تأیید (Approve) دارند. برخی قراردادهای مخرب طوری طراحی می‌شوند که در مرحلهApprove ، مجوز دسترسی کامل به تمام موجودی را از کاربر می‌گیرند.
- **کد مخفی در قرارداد هوشمند:**
  برخی توکن‌ها یا قراردادهای سفارشی، دستور خروج خودکار دارایی را در خود دارند) به نام Hidden Backdoor).
- **ایردراپ‌های جعلی:**
  کاربر به خیال دریافت ایردراپ رایگان یا جایزه، با کلیک روی لینک یا امضای تراکنش، مجوز کنترل دارایی خود را به قرارداد می‌دهد.

نشانه‌های هشداردهنده

- دریافت ناگهانی تتر یا توکن ناشناس در ولت (خصوصاً بدون دلیل یا اطلاع قبلی)
- مشاهده پیام Approve یا Allow با درخواست مجوز برای مقدار بسیار زیاد) مثلاً(Unlimited
- درخواست امضای تراکنش ناشناس یا لینک از منابع غیررسمی
- عدم امکان انتقال یا Swap تترها در صرافی‌های معتبر
- سابقه فعالیت عجیب یا نامشخص در بخش) Contract Explorer مثلاًEtherscan ، Tronscan)

راه‌های پیشگیری و مقابله

۱ .**هرگز به قرارداد ناشناس Approve ندهید:**
هر بار که پیامی با مضمون Approve Token دریافت کردید، نام قرارداد و سایت را بررسی کنید و فقط به سایت‌های کاملاً معتبر اعتماد کنید.

۲ .**تراکنش‌ها و مجوزهای فعال ولت را چک کنید:**
با ابزارهایی مثل Revoke.cashیا Etherscan Token Approvals، همهApprove های فعال را ببینید و مجوزهای غیرضروری را لغو کنید.

3. **از ایردراپ و توکن‌های ناشناس استفاده نکنید:**
به هیچ توکن یا تتر ناخواسته‌ای دست نزنید، Swapیا Approve انجام ندهید.
4. **فقط با صرافی‌های معتبر و کیف پول رسمی کار کنید.**
5. **همیشه هشدارها و تراکنش‌ها را با دقت مطالعه کنید.**

جمع‌بندی و توصیه

- توکن‌هایی که بدون دلیل به ولت شما واریز می‌شوند، بسیار مشکوک هستند و ممکن است تله کلاهبرداری باشند.
- هیچ‌گاه مجوز انتقال نامحدود (Unlimited Allowance) به هیچ قرارداد یا توکن ناشناس ندهید.
- برای اطمینان از وضعیت Approve ولت، به‌طور دوره‌ای آن را چک و مجوزهای غیرضروری را Revokeکنید.

کلاهبرداری تتر با استفاده از قرارداد هوشمند (Smart Contract) چطور انجام می‌شود؟

اصل ماجرا چیست؟

کلاهبرداران با استفاده از ترفندهای برنامه‌نویسی در بلاکچین (مثل شبکه ترون، اتریوم و ...) کاری می‌کنند که توکن تتر (یا هر توکن دیگری) وارد کیف پول شما شود، اما در واقع شما هیچ کنترلی روی آن ندارید و این تترها همیشه می‌تواند توسط کلاهبردار خارج شود. ممکن است چند روز، چند ساعت یا تا زمانی که شما تراکنشی بزنید، تترها در کیف پول باقی بماند اما ناگهان همه آنها خارج شود!

مکانیزم دقیق به زبان ساده

۱. کلاهبردار توکن یا تتر را به کیف پول شما می‌فرستد

- شما در والت خود تتر (USDT) یا یک توکن خاص مشاهده می‌کنید و خوشحال می‌شوید، شاید فکر می‌کنید پولی برای شما واریز شده، هدیه یا سود پروژه‌ای است.

۲. ولی این تترها "واقعی" نیستند و تحت کنترل یک قرارداد هوشمند هستند

- کلاهبردار با نوشتن یک قرارداد هوشمند سفارشی (سمی/مخرب) کاری می‌کند که با اولین اقدام شما (مثلاً وقتی بخواهید تتر را جابجا یا تبدیل کنید یا حتی فقط بخواهید مقدارش را ببینید)، اجازه برداشت تترهای داخل کیف پول را به قرارداد خودش بدهید.

۳. مجوز انتقال (Approve) مشکل‌ساز است

- وقتی شما بخواهید تتر را تبدیل یا جابه‌جا کنید، معمولاً نرم‌افزار از شما می‌خواهد تا به یک قرارداد هوشمند "اجازه (Approve) "بدهید. در این لحظه شما ناخواسته به قرارداد کلاهبردار مجوز می‌دهید تا هر مقدار تتر از کیف پول شما برداشت کند.

۴. کلاهبردار می‌تواند هر زمانی پول شما را خارج کند

- بعد از این که شما مجوز (Approve) دادید، قرارداد هوشمند اجازه دارد هر زمان که کلاهبردار اراده کند، کل تترهای شما را از کیف پولتان به آدرس خودش منتقل کند—حتی اگر شما در خواب باشید!

چرا این اتفاق می‌افتد؟

- **ولتاژ امنیت پایین در بلاکچین :**بلاکچین ذاتاً غیرمتمرکز و برگشت‌ناپذیر است، پس هرکسی بتواند مجوز دسترسی بگیرد، می‌تواند هر کاری با دارایی شما بکند.
- **عدم آگاهی کاربران :**خیلی از کاربران وقتی Approve می‌کنند، نمی‌دانند که اجازه برداشت "نامحدود" یا "هر زمان" به قرارداد هوشمند می‌دهند.
- **ظاهر عادی تترها :**تترها کاملاً واقعی به نظر می‌رسند و مثل یک واریزی عادی دیده می‌شوند، اما پشت پرده همه چیز در کنترل کلاهبردار است.

مثال واقعی

فرض کنید شما در کیف پولتان ناگهان 1000 تتر جدید می‌بینید که انتظارش را نداشتید. خوشحال می‌شوید و سعی می‌کنید آن را به ریال یا ارز دیگری تبدیل کنید. کیف پول (یا صرافی غیرمتمرکز) از شما می‌خواهد که "Approve" را انجام دهید تا تتر را بفروشد. شما هم بدون دقت، تایید می‌کنید. حالا عملاً مجوز انتقال هر مقدار تتر در کیف پولتان را به قرارداد کلاهبردار داده‌اید و او هر لحظه می‌تواند تترهای شما را خالی کند.

چطور جلوی این نوع کلاهبرداری را بگیریم؟

1. **به هیچ وجه توکن یا تتر ناشناس را لمس نکنید، تبدیل یا ارسال نکنید.**

2. اگر نیاز به Approve پیدا کردید، فقط به قراردادهای معتبر (مانند صرافی‌های شناخته‌شده) مجوز دهید.
3. از سایت‌هایی مثل revoke.cash یا etherscan.io/tokenapprovalchecker استفاده کنید و هر از چندگاهی مجوزهای غیرضروری را لغو (Revoke) کنید.
4. اگر تتر ناخواسته دریافت کردید، آن را رها کنید و هیچ اقدامی انجام ندهید.
5. در پروژه‌های مشکوک، ایردراپ، یا پیام‌هایی با وعده سود و پاداش شرکت نکنید.

جمع‌بندی

هرگز فریب واریز تتر یا توکن ناشناس را نخورید و هرگز به قرارداد یا سایتی که نمی‌شناسید، مجوز دسترسی به کیف پول ندهید. امنیت دارایی رمزارزی، اول از همه به عادت‌ها و دقت شما بستگی دارد.

مرحله‌به‌مرحله لغو مجوز (Approve) توکن‌ها در کیف پول

۱ .بررسی Approve های فعال روی کیف پول

الف (استفاده از سایت Revoke.cash

1. **ورود به سایت**
   - به سایت revoke.cash بروید.
   - سایت کاملاً امن و بین‌المللی است (در مرورگر کروم، فایرفاکس یا موبایل باز کنید).
2. **اتصال کیف پول**
   - روی دکمه Connect Wallet کلیک کنید.
   - نوع کیف پول خود را انتخاب کنید) مثلاًMetaMask ، Trust Walletیا WalletConnect).

- پیام اتصال را در کیف پول تأیید کنید.

3. **مشاهده لیست Approve ها**

- بعد از اتصال، تمام توکن‌هایی که قبلاً به قراردادهای مختلف اجازه برداشت داده‌اید، نمایش داده می‌شود.
- این لیست معمولاً شامل نام توکن) مثل(USDT ، آدرس قرارداد، و مقدار مجوز داده‌شده است.

---

۲ .لغو (Revoke) مجوز قراردادهای مشکوک یا غیرضروری

1. **شناسایی مجوزهای مشکوک**

- در لیست، هر Approve که مربوط به پروژه، قرارداد یا سایتی است که نمی‌شناسید یا به آن اعتماد ندارید، پیدا کنید.
- اگر قبلاً به پروژه‌ای نامعتبر یا ناشناس مجوز داده‌اید، آن را در لیست خواهید دید.

2. **لغو دسترسی**

- کنار هر مجوز، گزینه‌ای به نام **Revoke**وجود دارد (دکمه قرمز یا آبی).
- روی Revoke کلیک کنید.
- یک تراکنش برای کیف پول شما ارسال می‌شود (مانند انتقال معمولی).
- در کیف پول تراکنش را تأیید (Confirm) کنید) ممکن است هزینه کمی بابت Gas پرداخت کنید.(

3. **منتظر تایید تراکنش بمانید**

- چند ثانیه یا دقیقه صبر کنید تا تراکنش در بلاکچین تایید شود.

- بعد از تایید، دسترسی آن قرارداد به کیف پول شما قطع می‌شود و دیگر نمی‌تواند هیچ تتر یا توکنی برداشت کند.

---

۳ .(اختیاری) بررسی با Etherscan یاBSCScan

اگر کیف پول شما روی شبکه اتریوم یا BSC (بایننس اسمارت چین) است، می‌توانید با استفاده از سایت‌های Etherscan Token Approval Checkerیا BSCScan Token Approvalsهم مجوزها را مشاهده و لغو کنید.
روند کار دقیقاً مثل Revoke.cash است:

- آدرس کیف پول را وارد کنید
- لیستApprove ها را ببینید
- مجوزهای مشکوک را Revoke کنید

---

۴ .نکته مهم در همه مراحل

- **فقط مجوز پروژه‌ها و قراردادهایی را که نمی‌شناسید یا دیگر لازم ندارید لغو کنید.**
- هر Approve که به سایت‌های مشکوک یا ایردراپ‌های ناشناس داده‌اید، حتماً لغو شود.
- برای لغو هر Approve باید هزینه بسیار کمی (Gas Fee) بپردازید.

---

۵ .پس از لغوApprove ، امنیت دارایی برقرار می‌شود؟

بله!
تا زمانی که مجوز (Approve) یک قرارداد یا سایت به کیف پول شما فعال باشد، آن قرارداد هر لحظه می‌تواند توکن یا تتر را خارج کند.
اما به محض Revoke کردن، این دسترسی قطع شده و دیگر هیچ خطری شما را تهدید نمی‌کند.

حتی اگر بعداً توکن جدیدی به کیف پولتان بیاید، تا وقتی Approve نداده‌اید، قابل برداشت توسط کسی نیست.

جمع‌بندی سریع و چک‌لیست عملی:

1. به سایت revoke.cash بروید.
2. کیف پول را وصل کنید.
3. لیستApprove ها را ببینید.
4. مجوزهای ناشناس/مشکوک را Revoke کنید و تراکنش را تایید نمایید.
5. همیشه مراقب باشید به قرارداد یا سایتی که نمی‌شناسید، Approveندهید.

جادوی فکر یک شرکت پیشرو در زمینه توسعه راهکارهای نوآورانه‌ی دیجیتال، هوش مصنوعی و تحول سازمانی است. ما با تمرکز بر آموزش، تحقیق، و مشاوره، به سازمان‌ها کمک می‌کنیم تا از فناوری‌های نوظهور برای رشد، کارایی بیشتر و تصمیم‌گیری هوشمندانه بهره‌مند شوند.

تیم ما متشکل از متخصصان فناوری، تحلیل‌گران کسب‌وکار و مشاوران تحول دیجیتال است که با ترکیبی از دانش فنی و درک عمیق از نیازهای بازار، راهکارهایی جامع و عملی ارائه می‌دهند.

این کتاب با هدف ارائه‌ی بینش‌های کاربردی و آینده‌نگر درباره‌ی هوش مصنوعی عاملی گردآوری و تألیف شده است تا راهنمایی مؤثر برای مدیران، کارآفرینان، و علاقه‌مندان به فناوری باشد.

برای آشنایی بیشتر با خدمات ما، به وب‌سایت جادوی فکر سر بزنید:

www.jadoosoft.com

ساری-خیابان پیروزی- نبش پیروزی ۱۴ -ساختمان پارک علم و فناوری استان مازندران- طبقه سوم

کد پستی:۴۸۱۸۷۶۵۷۶۷

۰۱۱۳۳۲۵۹۶۵۹ – ۰۲۱۸۸۱۷۸۶۰۵ (پشتیبانی عصرها از ساعت ۱۶ تا ۲۰، ۰۹۱۰۱۰۰۹۰۰۷)

این کتاب به بررسی جامع و عمیق انواع کلاهبرداری‌های رایج در بازار رمزارزها می‌پردازد و با ارائه مثال‌های واقعی، نشانه‌های هشداردهنده، و راهکارهای عملی، خواننده را برای شناسایی و مقابله با این تهدیدها آماده می‌کند. در دنیای غیرمتمرکز و پرریسک رمزارزها، کلاهبرداران از روش‌های متنوعی مانند طرح‌های پانزی و هرمی، پروژه‌های اسکم و راگ‌پول، فیشینگ، کیف پول‌ها و صرافی‌های جعلی، سوءاستفاده از شبکه‌های اجتماعی، و حملات هکری استفاده می‌کنند. این کتاب با تحلیل هر یک از این روش‌ها و ارائه راهکارهای پیشگیرانه، به خوانندگان کمک می‌کند تا سرمایه‌گذاری ایمن و آگاهانه‌ای داشته باشند.

شرکت نرم افزاری جادوی فکر - (مجری پروژه نرم افزاری حوزه هوش مصنوعی و بلاکچین)

www.jadoosoft.com