**Prezenty czy przynęty? Jak uchronić się przed cyberoszustwami w okresie świątecznym**

**Święta Bożego Narodzenia to czas wzmożonych wydatków i poszukiwania okazji – zarówno na wymarzone prezenty, jak i dodatkowe źródła dochodu, które mają pomóc domknąć świąteczny budżet. Pod presją czasu i rosnących świątecznych zobowiązań, wiele osób działa nieostrożnie. To niestety sprzyja oszustom. Próbując złapać ostatnie promocje lub znaleźć szybki sposób na dodatkowy zarobek, łatwo o chwilę nieuwagi, którą coraz częściej wykorzystują cyberprzestępcy – dla nich święta to prawdziwy czas żniw.**

Święta Bożego Narodzenia to czas wzmożonych wydatków i poszukiwania okazji – zarówno na wymarzone prezenty, jak i dodatkowe źródła dochodu, które mają pomóc domknąć świąteczny budżet. Pod presją czasu i rosnących świątecznych zobowiązań, wiele osób działa nieostrożnie. To niestety sprzyja oszustom. Próbując złapać ostatnie promocje lub znaleźć szybki sposób na dodatkowy zarobek, łatwo o chwilę nieuwagi, którą coraz częściej wykorzystują cyberprzestępcy – dla nich święta to prawdziwy czas żniw.

„*Okres bożonarodzeniowy to czas, w którym wiele osób traci głowę w zakupowym szaleństwie. Pośpiech i brak uwagi to sprzymierzeńcy oszustów, którzy obiecują szybki zysk, a w zamian zostawiają swoje ofiary z pustymi rękami*” – ostrzega Jakub Bartoszek, CEO ogólnopolskiej sieci kantorów kryptowalut Cashify.

Jak wynika z raportu CSIRT KNF (Computer Security Incident Response Team) za 2023 r., liczba zgłoszonych incydentów związanych

z oszustwami w Polsce wyniosła 22 tysiące, z czego znacząca część dotyczyła wyłudzeń finansowych online. Szczególnie na celowniku znajdują się osoby, które inwestują w kryptowaluty lub korzystają z nowych technologii i dopiero rozpoczynają swoją przygodę z nimi,

co podkreślają eksperci ds. cyberbezpieczeństwa.

„*Cyberprzestępcy wykorzystują każdą okazję, by żerować na niewiedzy lub nieostrożności ludzi. Kryptowaluty stały się szczególnie atrakcyjnym obszarem dla oszustów, ponieważ wiele osób widzi w nich szansę na szybki zarobek, ale jednocześnie nie zna zasad działania tego rynku. Słyszeli gdzieś, że można dużo i łatwo zarobić. To idealne pole do nadużyć*” – tłumaczy Jakub Bartoszek. - “*Jako firma z wieloletnim doświadczeniem w branży, jesteśmy świadomi skali zagrożeń, jakie niosą ze sobą oszustwa kryptowalutowe, dlatego chętnie i bezpłatnie dzielimy się wiedzą na naszej stronie internetowej* [www.cashify.eu/kryptoscamy](https://www.cashify.eu/kryptoscamy)*, gdzie prowadzimy szereg działań edukacyjnych w tym obszarze”* - dodaje.

**Jak działają oszuści w obszarze kryptowalut?**

W okresie przedświątecznym cyberprzestępcy dostosowują swoje metody do emocji i potrzeb, które są szczególnie silne w tym czasie. Osoby, które szukają oszczędności lub chcą szybko zarobić dodatkowe pieniądze, stają się łatwiejszymi celami. W obszarze kryptowalut oszustwa mogą przyjmować różne formy:

l **Fałszywe platformy inwestycyjne** – przestępcy oferują szybki zysk z inwestycji w kryptowaluty, prowadząc ofiary na fałszywe strony internetowe, które imitują prawdziwe giełdy. Ofiary wpłacają środki, które potem znikają bez śladu.

l **Phishing i fałszywe portfele kryptowalutowe** – oszuści wysyłają fałszywe e-maile lub SMS-y, podszywając się pod znane giełdy kryptowalutowe, aby nakłonić ofiary do kliknięcia w linki, które prowadzą do stron wyłudzających dane lub fałszywych portfeli.

l **Nieistniejące ICO (Initial Coin Offerings)** – przestępcy organizują fikcyjne oferty nowych kryptowalut, oferując „ekskluzywne inwestycje” w rzekomo obiecujące projekty. Osoby, które się zdecydują, przekazują swoje pieniądze na fałszywe adresy, tracąc je bezpowrotnie.

l **Fałszywe konkursy i loterie kryptowalutowe** – oszuści obiecują „wielką wygraną” w zamian za drobną wpłatę, wymagając przy tym podania danych osobowych, w tym danych dostępów do portfeli kryptowalutowych.

Jak wskazano w raporcie CSIRT KNF, jednym z kluczowych elementów sukcesu oszustów jest brak wiedzy ofiar na temat mechanizmów działania tych ataków. Szczególnie narażone są osoby starsze, ale także młodsze pokolenia, które często ma ograniczone doświadczenie w zarządzaniu finansami online.

**Jak się chronić?**

Aby nie paść ofiarą oszustwa, szczególnie w obszarze kryptowalut, warto stosować się do poniższych zasad:

1. **Sprawdzaj wiarygodność platform inwestycyjnych** – zawsze weryfikuj opinie o giełdach kryptowalutowych oraz projektach ICO (Initial Coin Offering). Można odwiedzić strony takie jak CoinMarketCap czy CoinGecko, które oferują informacje o popularnych giełdach i projektach kryptowalutowych.

2. **Unikaj ofert obiecujących nierealistycznie wysokie zyski** – żaden legalny projekt kryptowalutowy nie gwarantuje zysku. Jeśli ktoś obiecuje szybki i łatwy zysk bez ryzyka, to bardzo prawdopodobnie jest to oszustwo.

3. **Zachowaj ostrożność w przypadku presji czasu** – oszuści często stosują techniki wywierania presji, jak np. konieczność natychmiastowej decyzji, ponieważ „oferta wygasa za chwilę”. Tego rodzaju ponaglanie jest bardzo charakterystyczne dla oszustów..

4. **Obcojęzyczny akcent w rozmowach telefonicznych** – jeśli kontaktuje się z nami osoba z obcojęzycznym akcentem, powinniśmy zachować szczególną ostrożność. Często takie osoby są powiązane z oszustwami międzynarodowymi, zwłaszcza w przypadku ofert inwestycji w kryptowaluty.

5. **Reklamy z wykorzystaniem wizerunków znanych osób** – oszuści często wykorzystują wizerunki celebrytów, polityków czy sportowców w reklamach, które pojawiają się w mediach społecznościowych lub na różnych stronach internetowych. Nigdy nie klikaj na takie reklamy, szczególnie te, które oferują szybki zysk.

6. **Nie zgadzaj się na zdalny dostęp do swojego komputera** – oszuści mogą poprosić o dostępu do komputera np. w celu „pomocy” przy zakładaniu portfela kryptowalutowego. Najczęściej proszą o użycie oprogramowania AnyDesk lub TeamViewer.

7. **Nie angażuj się w projekty, które wymagają wpłat przed udzieleniem dostępu do inwestycji** – każda wiarygodna giełda lub projekt inwestycyjny powinien umożliwić dostęp do swoich usług bez konieczności wcześniejszej wpłaty. Wszelkie prośby o przedpłatę są wyraźnym sygnałem ostrzegawczym.

8. **Nie klikaj w podejrzane linki** – cyberprzestępcy często wysyłają wiadomości e-mail lub SMS-y, podszywając się pod zaufane platformy. Zamiast klikać w linki, odwiedzaj strony giełd bezpośrednio przez przeglądarkę, upewniając się, że adres URL jest poprawny.

9. **Sprawdzaj terminy ważności domen -** to również jeden ze sposobów na zidentyfikowanie oszustwa. Czasem zdarza się, że domena wygasa “za 24 godziny” - wówczas wygasa również projekt i nasze pieniądze.

10. **Zabezpiecz swoje urządzenia** – korzystaj z programów antywirusowych, dbaj o aktualizacje systemu operacyjnego oraz aplikacji,

a także włącz dwuskładnikowe uwierzytelnianie (2FA) na wszystkich kontach związanych z kryptowalutami.

11. **Nie zgadzaj się na kontakt z nieznanymi osobami** – jeśli ktoś sam zgłasza się do Ciebie z propozycją inwestycji, to wyraźny sygnał ostrzegawczy. Legalni brokerzy nigdy nie dzwonią ani nie wysyłają nieproszonych wiadomości jako pierwsi. Oszuści często używają numerów telefonicznych zaczynających się na +44 (międzynarodowy numer kierunkowy Wielkiej Brytanii) lub kontaktują się przez aplikację WhatsApp.

12. **Uważaj na „oferty szyte na miarę”** – jeśli ktoś twierdzi, że ma ofertę, przygotowaną specjalnie dla ciebie, to również może to być oszustwo. Takie propozycje są jednym z najczęstszych elementów scamów.

„*Jeśli masz wątpliwości, skontaktuj się z ekspertem i zasięgnij informacji w Google lub na grupach związanych z kryptowalutami. Jeśli nie masz doświadczenia w kryptowalutach, warto skorzystać z pomocy specjalistów, np. w takich miejscach jak nasze kantory*” – radzi Jakub Bartoszek. „*W Cashify uratowaliśmy już dla naszych klientów blisko 31 250 000 zł, przez co nie zarobiliśmy 937 500 zł prowizji. Ale takie jest nasze podejście – pomagamy ludziom, bo ich bezpieczeństwo jest dla nas najważniejsze*.”

**Kryptowaluty a bezpieczeństwo: wyzwania i nadzieje**

Chociaż rynek kryptowalut jest jednym z obszarów najbardziej podatnych na oszustwa, edukacja może znacząco zmniejszyć skalę tego problemu. Kryptowaluty jako technologia są solidnie zabezpieczone. Najsłabszym ich ogniwem jest człowiek i jego nieuważność. Jak czytamy w raporcie Polskiego Instytutu Ekonomicznego, 66% Polaków przyznaje, że brakuje im podstawowej wiedzy o kryptowalutach.

To pokazuje, jak ważne są działania edukacyjne i jak dużo jest jeszcze do zrobienia w tym obszarze.

W tym kontekście szczególnie istotne będą zmiany prawne. Wprowadzenie regulacji MiCA (Markets in Crypto-Assets), które wejdą w życie w Polsce pod koniec 2024 r., ma na celu uregulowanie rynku aktywów cyfrowych, zwiększenie przejrzystości oraz poprawę ochrony konsumentów. Jednak eksperci podkreślają, że choć regulacje są istotne, to najważniejsza jest świadomość i odpowiednia wiedza użytkowników.

„*Żadna regulacja nie zastąpi czujności i zdrowego rozsądku, dlatego edukacja jest podstawą, by zminimalizować ryzyko stania się ofiarą oszustwa*” – kończy Jakub Bartoszek.