Ataki socjotechniczne ulubioną metodą cyfrowych oszustów. W pół roku odnotowano dwukrotnie więcej oszukańczych domen niż w całym 2024

Zespół CERT Polska tylko w pierwszej połowie 2025 roku zarejestrował już ponad 100 tys. oszukańczych domen służących cyfrowym przestępcom, w tym kilkadziesiąt tysięcy domen z ofertami fałszywych inwestycji. To więcej niż w całym 2024, kiedy to na Listę Ostrzeżeń trafiło w sumie 92 tysiące domen! Jak przekonuje Ministerstwo Finansów, niezbędne są zakrojone na szeroką skalę działania edukacyjne chroniące społeczeństwo przed cyberzagrożeniami. Przykładem takich działań jest trwająca obecnie kampania społeczna „Bezpieczne Złotówki".

Tak nagły wzrost niebezpiecznych stron internetowych to efekt nie tylko udoskonalenia narzędzi wykrywających cyberzagrożenia, ale i rosnącej popularności phishingu oraz ataków socjotechnicznych. Cyfrowi przestępcy coraz częściej kuszą nas obietnicą pewnych zysków, mnożąc strony internetowe oferujące fałszywe inwestycje.

Odpowiedzią na rosnącą skalę problemu jest kampania edukacyjna „Bezpieczne Złotówki" realizowana przez Ministerstwo Finansów i Fundację THINK!.

– *Bezpieczeństwo finansów obywateli jest jednym z celów określonych w Krajowej Strategii Edukacji Finansowej, której wdrażanie koordynuje Ministerstwo Finansów. Dlatego podejmujemy działania edukacyjne, które towarzyszą rozwiązaniom systemowym podejmowanym przez inne instytucje publiczne. Kampania „Bezpieczne Złotówki" przekłada język techniczny na codzienne decyzje użytkowników. To inwestycja w finansową odporność naszego społeczeństwa* – mówi **Monika Wojciechowska, Pełnomocniczka Ministra Finansów ds. Strategii Edukacji Finansowej.**

Społeczna kampania edukacyjna „Bezpieczne Złotówki", która trwa od czerwca do listopada, w najbliższych tygodniach będzie koncentrowała się na tematach związanych z bezpieczeństwem danych osobowych, do których wycieku często dochodzi właśnie poprzez strony internetowe tworzone przez oszustów.

– *Naszą kampanią pokazujemy, że ochrona przed cyberoszustwami nie wymaga zaawansowanej wiedzy technicznej. Bezpieczeństwo naszych pieniędzy tkwi w sile codziennych nawyków, oraz wzajemnej edukacji. Dlatego nie tylko podpowiadamy, jak upewniać się, że nasza inwestycja nie jest oszustwem ale też jak chronić się przed cyfrowymi przestępcami* – dodaje **Anna Bichta, Prezeska Fundacji THINK!.**

Spojrzenie w statystykę – jak działają cyfrowi oszuści?

Eksperci CERT Polska odnotowują, że w dalszym ciągu do najpowszechniejszych zagrożeń w cyberprzestrzeni należą phishing i ataki socjotechniczne.

– *Przestępcy wciąż bardzo chętnie korzystają ze stron internetowych promujących fałszywe inwestycje, obserwujemy też niezachwianą popularność kampanii opartych na SMS-ach o rzekomo niedostarczonej paczce. To pokazuje, jak ważne są kampanie edukacyjne w zakresie cyberbezpieczeństwa, bo pomimo że świadomość w społeczeństwie rośnie, to cyberprzestępcy dalej zbierają pokaźne żniwo* – wskazuje **Karol Bojke, z działającego w NASK zespołu CERT Polska.**

Czym jest Lista Ostrzeżeń CERT?

Lista Ostrzeżeń CERT Polska to prowadzone od 2020 roku zestawienie niebezpiecznych stron internetowych. Lista jest wykorzystywana przez operatorów telekomunikacyjnych, firmy, organizacje i samych użytkowników do automatycznego blokowania dostępu do złośliwych stron i tym samym ograniczania skutków ataków phishingowych i innych działań cyberprzestępców.

Każdy z nas może zgłosić stronę, która wyłudza dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych, za pomocą formularza dostępnego na https://incydent.cert.pl/phishing.

Korzystając ze strony https://lista.cert.pl/, można z kolei zweryfikować, czy przeglądarka korzysta z Listy Ostrzeżeń przed niebezpiecznymi stronami prowadzonej przez zespół CERT Polska.

Materiał powstał w ramach kampanii społecznej "Bezpieczne Złotówki" sfinansowanej ze środków Funduszu Edukacji Finansowej, którego dysponentem jest Minister Finansów i Gospodarki. Kampanię realizuje Fundacja Think!.