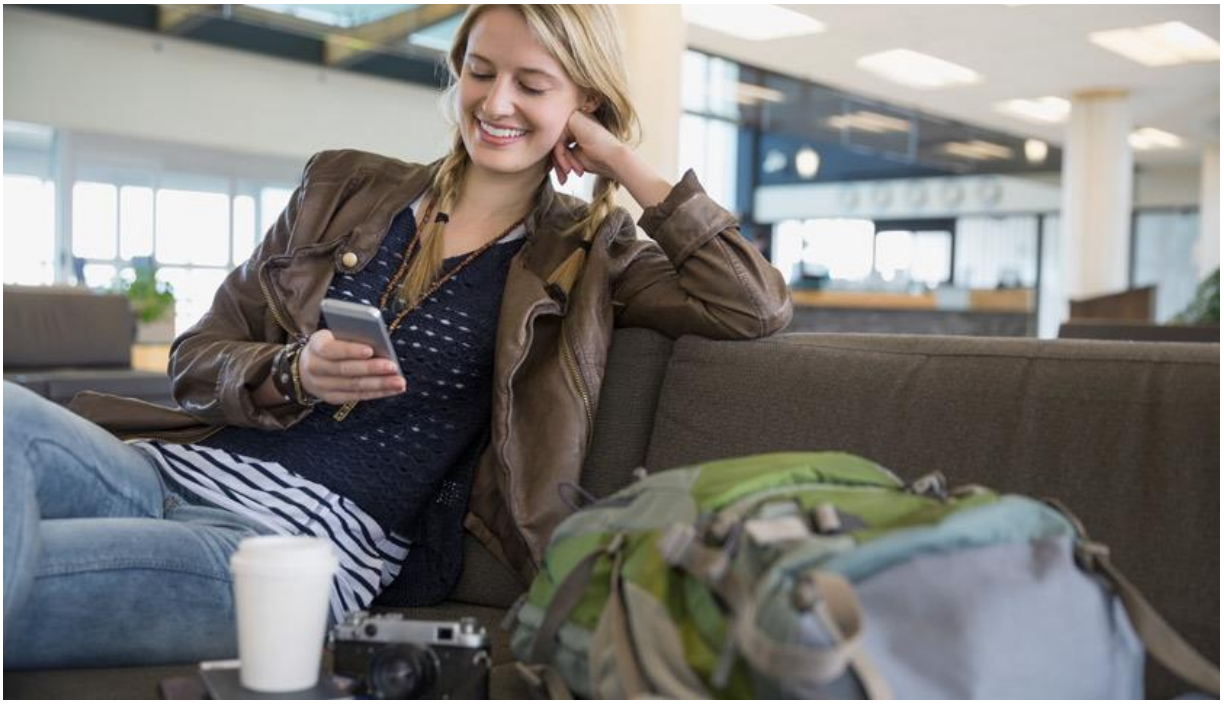
CERT Orange Polska podsumował wakacje w sieci: fałszywe inwestycje numerem jeden wśród oszustw.

Informacja prasowa, 17 września 2025



W ciągu dwóch wakacyjnych miesięcy CERT Orange Polska zablokował dostęp do ponad 140 tys. fałszywych domen internetowych – ponad trzykrotnie więcej niż w tym samym okresie ubiegłego roku. Niemal 70% spośród wykrytych i zablokowanych adresów prowadziło do fałszywych inwestycji. Działająca w sieci operatora CyberTarcza ochroniła ponad 1,6 miliona użytkowników, którzy kliknęli w zablokowane wcześniej niebezpieczne linki.

Oszustwa na fałszywe inwestycje utrzymują się w czołówce zagrożeń już od kilku lat, a w ostatnim roku przybrały na sile. Dla porównania, w poprzednie wakacje stanowiły one 45% blokowanych przez CERT Orange Polska fałszywych domen używanych do wyłudzeń danych lub pieniędzy.

– *Widać mniejszą różnorodność fałszywych kampanii, ale liczba domen używanych do oszustw lawinowo się zwiększa. Oszuści sprawnie wykorzystują najnowsze techniki, sztuczną inteligencję do tworzenia grafik z wizerunkiem znanych osób umieszczonych w sensacyjnym kontekście czy wideo z podłożonym głosem. Wpływają na nasze emocje, liczą na szybką reakcję. Apeluję o rozwagę w reagowaniu na te treści. Widzimy także coraz większą automatyzację działań cyberprzestępców by przeciwdziałać naszym blokadom, jednak nasza skuteczność w wykrywaniu i blokowaniu zagrożeń także rośnie* – mówi Robert Grabowski, szef CERT Orange Polska.

W czasie wakacji kolejną istotną grupą zagrożeń były oszustwa związane z płatnościami, w tym „na kupującego”, które stanowiły niemal 20% zablokowanych domen. W tym przypadku linki kierujące do fałszywych stron z płatnościami tworzone są zwykle pod konkretnych użytkowników.

Chroń swoją cyfrową tożsamość

Internauci mogą liczyć na wsparcie ekspertów CERT Orange Polska. Podejrzane wiadomości można przesłać na adres cert.opl@orange.com lub SMS-em na nr 508 700 900. To tylko chwila, a może przyspieszyć blokadę potwierdzonych stron phishingowych i pomóc ochronić także inne osoby. Aby lepiej zadbać o swoją cyfrową tożsamość, na stronie Hasło Alert można sprawdzić, czy nasze hasło lub login nie wyciekły. Można to także zrobić w Centrum Bezpieczeństwa w aplikacji Mój Orange.

Warto śledzić także bieżące ostrzeżenia na stronie cert.orange.pl, na platformie X @CERT_OPL, a także cotygodniowe materiały dotyczące bezpieczeństwa na blogu Orange Polska.

Źródło: blog Orange Polska https://biuroprasowe.orange.pl