Warszawa, 22.05.2026 r.

Jesteś świadkiem phishingu? Zgłoś incydent

Każdego dnia do naszych skrzynek e-mail, telefonów i komunikatorów trafiają tysiące prób wyłudzeń danych lub pieniędzy. Jedne wiadomości phishingowe są mniej, inne bardziej wyrafinowane. Potrafią do złudzenia przypominać prawdziwe wiadomości z banku, od kuriera czy nawet od przełożonego. O tym, jak rozpoznać próbę wyłudzenia danych i się przed nią bronić, pisała niedawno na Blogu iSecure Katarzyna Ułasiuk-Delamare.
Dziś chcielibyśmy pokazać nie tylko, jak się chronić, ale również jak każdy z nas może pomóc innym uniknąć phishingu i sprawić, że kolejna osoba nie stanie się ofiarą cyberoszustów.

Zgłoś incydent

Każda osoba, która zidentyfikuje zagrożenie phishingowe lub inne cyberzagrożenie, może zgłosić je do CERT Polska za pośrednictwem strony: incydent.cert.pl
Proces zgłoszenia jest krótki i intuicyjny. Formularz prowadzi użytkownika krok po kroku przez klasyfikację incydentu:

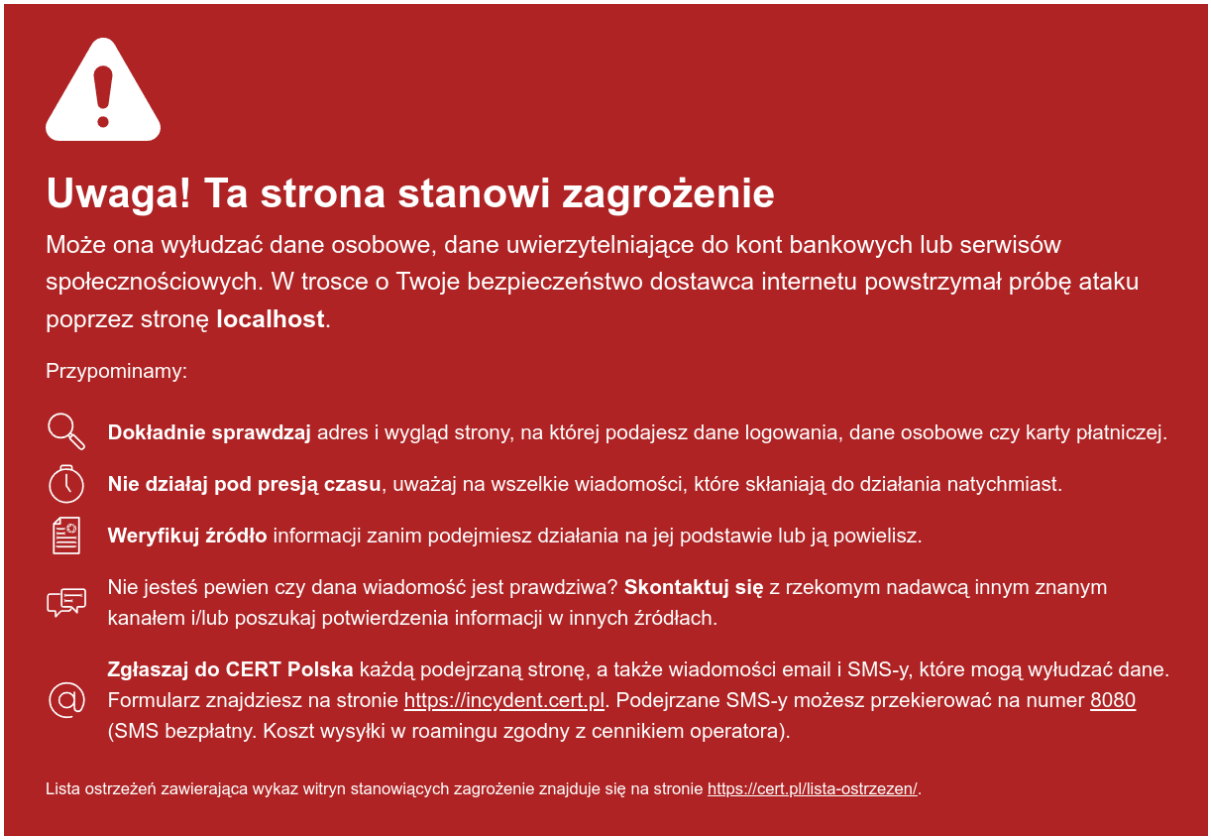
1. **Kto zgłasza incydent?**
   Nasza instrukcja skierowana jest do osób lub podmiotów, które nie podlegają ustawie o krajowym systemie cyberbezpieczeństwa, zatem należy wybrać opcję „Osoba fizyczna / inne podmioty".
2. **Czy zgłaszane zdarzenie doprowadziło do negatywnych skutków?**
   Jeżeli udało się uniknąć oszustwa, wybieramy „Nie - zgłaszam inne zagrożenie".
3. **Czy zdarzenie wystąpiło?**
   To pytanie nie dotyczy rzeczywistych skutków, a samego faktu wystąpienia zagrożenia. Jeśli rzeczywiście otrzymaliśmy phishingowy e-mail, SMS lub link, wybieramy: „Zgłaszam cyberzagrożenie".
4. **Powaga zagrożenia**
   Warto podejść do tej opcji rozsądnie i adekwatnie ocenić sytuację. Nie każde podejrzane zdarzenie powinno otrzymywać najwyższy priorytet. Klasyfikujmy w ten sposób wyłącznie poważne zagrożenia, aby rzeczywiście istotne incydenty nie musiały czekać w niepotrzebnej kolejce.
5. **Rodzaj zagrożenia**
   W ostatnim kroku wybieramy kategorię odpowiadającą zaobserwowanemu incydentowi, np.:
   - złośliwa domena,
   - podejrzany SMS,
   - podejrzany e-mail,
   - podejrzany telefon.

Pozostaje już tylko opisać zagrożenie, wkleić adres potencjalnie złośliwej strony, potwierdzić, że nie jesteśmy robotem, i kliknąć „Wyślij zgłoszenie". Co ważne, jeżeli nie oczekujemy kontaktu zwrotnego, nie musimy podawać swoich danych. Możliwe jest przesłanie zgłoszenia wyłącznie informacyjnie.

Dlaczego zgłaszanie incydentów jest w interesie nas wszystkich?

Wiele oszustw działa skutecznie dlatego, że są nowe i jeszcze nierozpoznane. Mając świadomość schematu działania przestępców, dużo łatwiej się przed nimi ustrzec. Dzięki zgłoszeniom możliwe jest szybsze ostrzeganie innych użytkowników oraz systemowe ograniczanie skali zagrożenia.

Jeżeli np. strona internetowa służy do wyłudzania danych osobowych lub środków finansowych (np. danych kart płatniczych), może zostać dodana przez NASK do Listy Ostrzeżeń CERT Polska (https://cert.pl/lista-ostrzezen/). Może to się stać właśnie na podstawie naszego zgłoszenia. Po wpisaniu domeny na listę, dostęp do podejrzanej witryny zostanie błyskawicznie zablokowany przez wiodących operatorów telekomunikacyjnych. Dzięki temu kolejna osoba, która kliknęłaby w fałszywy link, może uniknąć utraty danych lub pieniędzy. Zamiast strony oszustów zobaczy co najwyżej wielkie, czerwone ostrzeżenie:



Podsumowanie

Cyberoszustwa stały się codziennością Internetu i trudno oczekiwać, że szybko z niego znikną. Niestety, są skuteczne i przynoszą obfite plony. Skala problemu jest ogromna. W 2025 roku CERT Polska zarejestrował około 250 000 incydentów, z czego aż 97% z nich stanowiły oszustwa komputerowe, w tym phishing, oszustwa inwestycyjne i inne formy wyłudzania danych lub pieniędzy[1]. Nie sposób policzyć, ilu oszustw udało się uniknąć właśnie dzięki zgłoszeniom „zwykłych" użytkowników Internetu.

Nowoczesne technologie, operatorzy telekomunikacyjni oraz organizacje zajmujące się cyberbezpieczeństwem stale pracują nad ochroną użytkowników. Jednak ogromną rolę nadal odgrywa zwykła czujność Internautów, czyli każdego z nas. Czasem jedno zgłoszenie podejrzanego e-maila lub fałszywej strony może sprawić, że ktoś inny nie stanie się ofiarą oszustwa. W dzisiejszym

[1] RAPORT ROCZNY 2025 z działalności CERT Polska" - https://cert.pl/uploads/docs/Raport_CP_2025.pdf

świecie nawet niewielka reakcja pojedynczej osoby może mieć znaczenie dla bezpieczeństwa wszystkich innych użytkowników.

Marcin Stryszko – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.