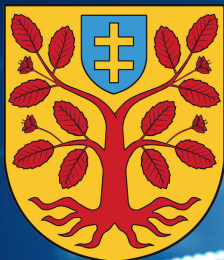


CYBERBEZPIECZEŃSTWO DLA KAŻDEGO

NIE DAJ SIĘ OSZUKAĆ W INTERNECIE!



Internet pomaga nam w codziennym życiu – robimy zakupy, korzystamy z bankowości elektronicznej, kontaktujemy się z rodziną i znajomymi. Jest również miejscem działania cyberprzestępców. Każdy może stać się ofiarą oszustwa, dlatego warto znać najczęstsze zagrożenia i wiedzieć, jak się przed nimi chronić.



PHISHING

Otrzymałem wiadomość z banku lub firmy kurierskiej. Czy powinienem kliknąć w link?



Nie od razu.

Cyberprzestępcy często wysyłają wiadomości wyglądające jak prawdziwe powiadomienia z banku, urzędu, firmy kurierskiej lub dostawcy usług.

Mogą informować o blokadzie konta, niedopłacie za przesyłkę lub konieczności aktualizacji danych.

Co zrobić?

- Sprawdź nadawcę wiadomości.
- Nie klikaj w link pod wpływem emocji.
- Wejdź na stronę instytucji samodzielnie, wpisując jej adres w przeglądarce.



SPOOFING

Dzwoni do mnie ktoś z banku. Skąd mam wiedzieć, że to naprawdę bank?



Nie możesz mieć pewności tylko dlatego, że na ekranie telefonu wyświetla się nazwa lub numer banku. Przestępcy potrafią podszywać się pod zaufane instytucje i wzbudzać poczucie zagrożenia, aby nakłonić do podjęcia szybkiej decyzji.

Co zrobić?

- Nie podawaj przez telefon haseł, PIN-ów ani kodów autoryzacyjnych.
- Jeśli rozmowa budzi wątpliwości, rozłącz się.
- Zadzwoń samodzielnie na oficjalny numer instytucji.



RANSOMWARE

Co może się stać po otwarciu podejrzanego załącznika lub pliku?



Na komputerze lub telefonie może zostać zainstalowane złośliwe oprogramowanie. W niektórych przypadkach przestępcy mogą zablokować dostęp do zdjęć, dokumentów i innych ważnych plików, a następnie żądać pieniędzy za ich odzyskanie.

Co zrobić?

- Nie otwieraj załączników od nieznanych nadawców.
- Aktualizuj system operacyjny i programy.
- Regularnie wykonuj kopie zapasowe ważnych danych.



KRADZIEŻ TOŻSAMOŚCI

Dlaczego moje dane osobowe są cenne dla cyberprzestępców?

Dane osobowe mogą zostać wykorzystane do wyłudzenia pożyczki, założenia konta internetowego, dokonania zakupów lub podszywania się pod inną osobę.

Co zrobić?

- Nie publikuj zdjęć dokumentów w Internecie.
- Ostrożnie udostępniaj swoje dane osobowe.
- Chroń dokumenty tak samo jak pieniądze.



PRZEJĘCIE KONTA

Czy jedno hasło do wszystkich kont to dobry pomysł?

Nie. Jeśli przestępca pozna jedno hasło, może próbować zalogować się na Twoją pocztę elektroniczną, konto społecznościowe a nawet do bankowości elektronicznej.

Co zrobić?

- Używaj różnych haseł do różnych usług.
- Twórz silne i trudne do odgadnięcia hasła.
- Włącz dodatkowe zabezpieczenie logowania (2FA).

OSZUSTWA INTERNETOWE

Jak rozpoznać oszustwo podczas zakupów lub płatności w Internecie?

Przestępcy często kuszą bardzo niskimi cenami, wyjątkowymi promocjami lub obietnicą szybkiego zysku. Mogą również podszywać się pod znajomych i prosić o przekazanie kodu BLIK.

Co zrobić?

- Sprawdzaj opinie o sklepie lub sprzedawcy.
- Nie przekazuj kodów BLIK bez pewności, komu pomagasz.
- Zachowaj ostrożność wobec wyjątkowo atrakcyjnych ofert.

DEEPPAKE I SOCJOTECHNIKA

Czy można podrobić czyjś głos lub wizerunek?

Tak. Dzięki sztucznej inteligencji można stworzyć fałszywe nagranie głosu, zdjęcie lub film przypominające prawdziwą osobę. Przestępcy wykorzystują takie materiały do wyłudzenia pieniędzy lub danych.

Co zrobić?

- Nie działaj pod wpływem emocji i presji czasu.
- Potwierdzaj nietypowe prośby innym sposobem kontaktu.
- Uważaj gdy ktoś prosi o pilny przelew lub przekazanie danych.

PAMIĘTAJ!

Cyberprzestępcy najczęściej wykorzystują pośpiech, strach, ciekawość i zaufanie.

ZATRZYMAJ SIĘ. POMYŚL. SPRAWDŹ.

Zanim klikniesz w link, podasz dane lub wykonasz przelew – zatrzymaj się i sprawdź.

W razie wątpliwości skonsultuj sytuację z rodziną, znajomym lub inną zaufaną osobą.

Cyberprzestępcy liczą na pośpiech i emocje – rozmowa z kimś bliskim może pomóc uniknąć oszustwa.

TWOJA OSTROŻNOŚĆ JEST NAJLEPSZĄ OCHRONĄ PRZED CYBERPRZESTĘPCAMI.

GDZIE ZGŁOSIĆ INCYDENT?

Podjęta wiadomość SMS

Prześlij ją na numer 8080 prowadzony przez CERT Polska

Podjęta strona internetowa?

Zgłoś ją przez formularz na stronie CERT Polska – www.cert.pl

Utrata pieniędzy lub podejrzenie oszustwa?

Niezwłocznie skontaktuj się ze swoim bankiem oraz zgłoś sprawę policji.

Utrata dokumentów?

Jak najszybciej zastrzeż dokumenty i poinformuj odpowiednie instytucje.



TWOJA OSTROŻNOŚĆ JEST NAJLEPSZĄ OCHRONĄ PRZED CYBERPRZESTĘPCAMI



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA