# PORADNIK

## BEZPIECZEŃSTWA CYBERNETYCZNEGO

### WSPÓLNA ODPOWIEDZIALNOŚĆ

FERMENTATION. UNLIMITED.

LESAFFRE

# Szanowni Partnerzy i Klienci!

*W dobie postępującej cyfryzacji, bezpieczeństwo informacji staje się kluczowym elementem prowadzenia działalności.*

*Niniejszy poradnik ma na celu podniesienie świadomości na temat zagrożeń cybernetycznych oraz przedstawienie praktycznych wskazówek, jak skutecznie chronić dane Państwa firm i Klientów.*

## Z naszego poradnika dowiesz się:

1. **Jak rozpoznawać zagrożenia i oszustwa w sieci?**
2. **Jak dbać o swoje bezpieczeństwo?**
3. **Jak reagować, gdy padniesz ofiarą oszustwa?**

# Zagrożenia i oszustwa w sieci!

# Phishing

To jedna z najczęściej stosowanych metod oszustwa w internecie, która polega na podszywaniu się pod zaufaną osobę, instytucję lub usługę, w celu wyłudzenia poufnych danych, takich jak: loginy, hasła, numery kart kredytowych, czy inne informacje wrażliwe.

Nazwa „phishing" pochodzi od angielskiego słowa „fishing" (*tłum. wędkowanie*), ponieważ atakujący zarzuca przynętę w nadziei, że nieostrożna osoba ją złapie.

Coraz częściej e-maile pisane są idealną polszczyzną.
W większości przypadków przestępcy chcą przekonać ofiarę do działania psychologicznymi sztuczkami:

*„Nadpłacił pan rachunek"*
*„Proszę o natychmiastowy zwrot pieniędzy"*
*„Zostanie zablokowany dostęp do internetu".*

# Złośliwe oprogramowanie

Za pomocą poczty elektronicznej cyberprzestępcy mogą wysyłać różnego rodzaju złośliwe oprogramowanie, ukryte w załącznikach lub ukierunkowane na wykorzystanie luk bezpieczeństwa, w komputerze odbiorcy.

Poniżej przedstawiamy najczęściej spotykane typy złośliwego oprogramowania, które mogą zostać rozprzestrzenione tą drogą:

## Ransomware

to oprogramowanie, które szyfruje pliki użytkownika, uniemożliwiając dostęp do nich. Cyberprzestępcy żądają zapłaty okupu (najczęściej w kryptowalutach), za dostarczenie klucza do odszyfrowania danych. Oprogramowanie to rozprzestrzenia się najczęściej w zainfekowanych załącznikach (np. plikach PDF, Word, Excel) lub po kliknięciu w podejrzany link.

## Trojan (Koń trojański)

to złośliwe oprogramowanie, które podszywa się pod legalny plik lub aplikację, aby uzyskać nieautoryzowany dostęp do systemu ofiary. Nie działa ono samo – musi zostać uruchomione przez użytkownika.

## Worm (Robak)

to rodzaj złośliwego oprogramowania, które rozprzestrzenia się samoistnie – nie wymaga uruchomienia przez użytkownika. Może infekować systemy przez luki w oprogramowaniu i rozsyłać się do kontaktów w skrzynce e-mail ofiary. E-maile z robakami mogą zawierać linki lub załączniki, które po otwarciu automatycznie zarażają system i rozsyłają kopie siebie do kolejnych ofiar.

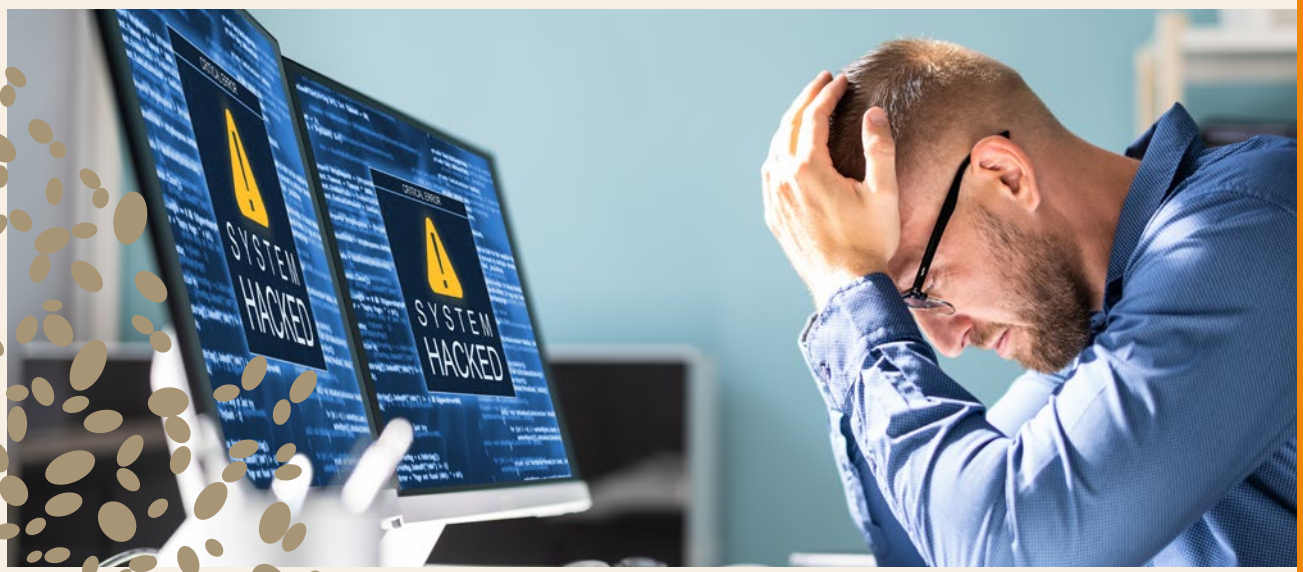
# Złośliwe oprogramowanie

## Spyware (Oprogramowanie szpiegujące)

to oprogramowanie zaprojektowane do potajemnego zbierania danych o użytkowniku, takich jak: dane logowania, historie przeglądania, dane osobowe czy numery kart płatniczych. Często jest dołączane do załączników e-mail lub instalowane przez użytkownika, który zostaje wprowadzony w błąd, na przykład proszony o „instalację aktualizacji" lub „aktywację dokumentu". Spyware działa w tle i jest trudne do wykrycia.

## Malware

ukierunkowany na dane płatnicze. Ten typ złośliwego oprogramowania jest projektowany specjalnie w celu wykradania danych bankowych, informacji o kartach płatniczych i innych cennych informacji finansowych. Może być dostarczany w fałszywych e-mailach od banków lub innej instytucji finansowej, w których prosi się o kliknięcie w link lub otwarcie rzekomo ważnego dokumentu.



# Jak rozpoznać potencjalnie niebezpieczny e-mail?

## 1. Podejrzany nadawca

Sprawdzaj dokładnie adres e-mail nadawcy, a nie tylko wyświetlaną nazwę. Cyberprzestępcy często używają podobnych do prawdziwych adresów e-mail (np. zamiast „firma@example.com” używają „firma1@example.com” lub „firm@example.co”).

Jeśli nadawca jest nieznany lub adres wygląda nietypowo, zachowaj szczególną ostrożność.

## 2. Pilne wezwanie do działania

Czy wiadomość wymaga szybkiej reakcji, np. kliknięcia w link, podania danych osobowych lub finansowych? To charakterystyczna metoda stosowana w atakach phishingowych.

## 3. Nieoczekiwane załączniki

Nigdy nie otwieraj załączników w e-mailach od nieznanych nadawców. Mogą one zawierać złośliwe oprogramowanie. Nawet załączniki od znanych nadawców, które są nieoczekiwane lub dziwnie wyglądają, mogą być podejrzane (np. nazwy plików typu „Faktura+1234.zip” albo „Dokument.pdf.exe”).

## 4. Linki do podejrzanych stron

Przed kliknięciem w link, najedź na niego kursorem, aby zobaczyć pełny adres URL. Upewnij się, że prowadzi do wiarygodnej strony. Cyberprzestępcy często podmieniają linki, aby przekierowywały do fałszywych stron.

## 5. Błędy gramatyczne i ortograficzne

Fałszywe e-maile często zawierają rażące błędy, literówki lub niespójności w treści, co może świadczyć o niskiej jakości fałszerstwa.

# Zasady bezpieczeństwa w sieci!

# Pamiętaj!

## Silne hasła – Twoja linia obrony

**Twórz** hasła składające się z co najmniej 12 znaków, w tym małych i wielkich liter, cyfr i znaków specjalnych.
**Unikaj** używania oczywistych haseł, takich jak „123456” lub „qwerty”.
**Nigdy** nie używaj tego samego hasła do różnych kont i usług.
**Regularnie** zmieniaj swoje hasła.
**Korzystaj** z menedżerów haseł do bezpiecznego przechowywania i generowania unikalnych haseł.

## Dwuetapowa weryfikacja (2FA)

**Włącz** dwuetapową weryfikację tam gdzie to możliwe. Nawet jeśli ktoś pozna Twoje hasło, nie zaloguje się bez dodatkowego kodu wysłanego na Twój telefon.

## Nie klikaj podejrzanych linków

**Nawet jeśli** e-mail wygląda profesjonalnie, nie klikaj w linki prowadzące do logowania, zanim nie upewnisz się, że pochodzą z zaufanego źródła.
W razie wątpliwości otwórz stronę ręcznie, wpisując jej URL w przeglądarce.

## Uważaj na załączniki

**Otwieraj** załączniki tylko od zaufanych nadawców i wyłącznie wtedy, kiedy są oczekiwane. Pliki z rozszerzeniami typu *.exe, *.zip, *.scr lub *.js mogą być szczególnie niebezpieczne.

*Zasady bezpieczeństwa w sieci.*

## Aktualizacja oprogramowania

**Regularnie** aktualizuj system operacyjny, aplikacje, przeglądarki i wtyczki.
Aktualizacje zawierają poprawki zabezpieczeń chroniące przed nowymi zagrożeniami.
**Włącz** automatyczne aktualizacje, gdy tylko jest to możliwe.
**Unikaj** nielegalnego oprogramowania – może zawierać złośliwy kod.

## Korzystaj z Oprogramowania Antywirusowego

**Zainstaluj** renomowany program antywirusowy.
**Włącz** ochronę w czasie rzeczywistym.
**Regularnie** aktualizuj bazy wirusów.


## Bezpieczne połączenia internetowe

**Unikaj** korzystania z publicznych sieci Wi-Fi, szczególnie do logowania się do kont bankowych i innych wrażliwych systemów. Jeśli musisz, korzystaj z połączenia VPN.
**Upewnij się**, że każda strona, z której korzystasz, używa https://.
W przeglądarce oznaczane jest to często jako zamknięta kłódka obok adresu URL.

## Uważaj na urządzenia zewnętrzne

**Nie podłączaj** do swoich urządzeń nieznanych pendrive'ów czy innych nośników danych – mogą zawierać złośliwe oprogramowanie.
**Skanuj** zewnętrzne nośniki za pomocą oprogramowania antywirusowego przed użyciem.

## Ochrona urządzeń mobilnych

**Zabezpiecz** urządzenia mobilne kodem PIN, wzorem lub biometrią.
**Włącz** możliwość zdalnego wymazania danych w przypadku zgubienia urządzenia.
**Instaluj** aplikacje wyłącznie z oficjalnych sklepów.

# Jak reagować,
# gdy padniesz ofiarą oszustwa?

**Pomimo zachowania ostrożności i środków bezpieczeństwa może się zdarzyć, że padniesz ofiarą oszustwa. Co wtedy? Musisz skupić się na dwóch kwestiach:**

## Ograniczeniu szkód

**Zmień hasła** na kontach, z których korzystasz.
**Zaktualizuj oprogramowanie,** które ma zabezpieczać sprzęt i sieć.
**Skontaktuj się z bankiem,** jeśli sprawa dotyczy kradzieży danych bankowych, aby zablokować konta oraz karty płatnicze.

## Zgłoszeniu oszustwa odpowiednim organom i instytucjom

**Złóż na policji** doniesienie o popełnieniu przestępstwa. Zachowaj dowody, mogą nimi być np. zrzuty ekranu czy wiadomości.
**Zgłoś oszustwo do CERT Polska** – to instytucja, która zajmuje się tematem bezpieczeństwa w internecie. Dzięki przekazaniu jej informacji o oszustwach przyczyniasz się do ograniczenia tego szkodliwego procederu w sieci.
**Zgłoś oszustwo instytucji / firmie**, pod którą podszywa się oszust.

# WAŻNE KONTAKTY:

1. **Zespół ds. bezpieczeństwa** Lesaffre Polska SA
   pomocIT@lesaffre.com | +48 77 40 72 424

2. **CERT Polska**
   https://cert.pl

3. **Pilne zgłoszenia incydentów**
   numer 997 (policja)
   lub 112

# Razem budujemy bezpieczną przyszłość!


Cyberbezpieczeństwo to ciągły proces. Dzięki tym praktykom minimalizujesz ryzyko i chronisz siebie oraz naszą współpracę.

**Pamiętaj:** Twoja czujność to pierwsza linia obrony!