# Poradnik cyberbezpieczeństwa Enei

# Spis treści

**Spis treści**

# Wstęp

Nieustanny rozwój sieci Internet i oferowanych w niej usług sprawił, iż stała się ona nieodzowną częścią życia codziennego. Niestety proces integracji z wirtualnym światem niesie również szereg zagrożeń, których nie można bagatelizować.

Bezpieczeństwo w sieci to nie tylko kwestia ochrony danych osobowych, danych wrażliwych, danych poufnych itp., ale też ochrony prywatności.

Metody działań w obszarze cyberprzestępczości stają się coraz bardziej zaawansowane (rozwiązania technologiczne, metody socjotechniczne). Kluczową kwestią jest zrozumienie, co naprawdę oznacza „bycie bezpiecznym w sieci" i jakie kroki należy podjąć, aby chronić siebie, swoich bliskich i przeciwdziałać potencjalnym zagrożeniom oraz ich następstwom. Istotna jest też wiedza, jak należy postępować w sytuacji, gdy nastąpi udany atak cybernetyczny, w wyniku którego traci się dostęp do swoich danych, środki finansowe czy też informacje, które powinny być poufne, a zostają upublicznione.

Ze względu na występujące coraz częściej w sferze cyberprzestrzeni zagrożenia, wynikające z różnych przyczyn (zysk finansowy, cyberterroryzm, dezinformacja itp.), stałe podnoszenie kompetencji w obszarze tzw. cyberhigieny, we współczesnych realiach geopolitycznych jest kluczowe dla cyberbezpieczeństwa.

# Podstawowe definicje

1. **CERT ENEA** to zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet, działający w Grupie Enea.

2. **CERT Polska** to zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet, działający w strukturach NASK – Państwowego Instytutu Badawczego.

3. **Cyberatak** jest to każdy rodzaj ofensywnego działania osób lub organizacji w sieci Internet, którego celem mogą być systemy informatyczne, sieci komputerowe, komputery lub inne urządzenia elektroniczne z dostępem do sieci.

4. **Cyberbezpieczeństwo** to ochrona danych i systemów informatycznych przed zagrożeniami, jakie niosą za sobą cyberataki. Najważniejszym celem zapewnienia bezpieczeństwa w sieci jest zmniejszenie ryzyka ataków cybernetycznych oraz skuteczna ochrona przed nieuprawnionym wykorzystaniem danych i programów.

5. **Deepfake** jest to technika obróbki obrazu i dźwięku, która tworzy łudząco prawdopodobny, jednak zmanipulowany materiał. Takie materiały działają zwykle na niekorzyść rzekomo występujących w nich osób, mogą być zatem wykorzystywane, np. jako element walki politycznej.

# Podstawowe definicje

6. **Fake news** to rozpowszechniana nieprawdziwa informacja, często o sensacyjnym i szokującym charakterze, przyciągająca uwagę krzykliwym nagłówkiem i opisana emocjonalnym językiem, co sprawia, że czyta się ją chętnie i dalej rozpowszechnia. Fake news jest też narzędziem do przeprowadzania ataków phishingowych. Zawarte w nich linki mogą przekierowywać do fałszywych witryn internetowych, których celem jest wyłudzenie danych lub kradzież środków finansowych.

7. **Dezinformacja** jest to celowe działanie, którego celem jest sfabrykowanie lub zaburzenie przekazu informacyjnego, by osiągnąć własne korzyści polityczne, społeczne, finansowe, militarne, itp.

8. **Incydent bezpieczeństwa** jest to nieautoryzowane, nieakceptowalne lub bezprawne działanie w systemie komputerowym lub innym urządzeniu elektronicznym (np. smartfonie, tablecie, telefonie etc.), którego efektem jest naruszenie integralności, poufności, czy też dostępności do systemu lub danych.

# Podstawowe definicje

9. **Phishing** jest to najbardziej popularna metoda cyberataku. Polega na tym, że przestępcy podszywają się pod rozpoznawalne pomioty i instytucje, takie jak koncerny energetyczne, banki, urzędy, sklepy internetowe, dostawców usług czy portale aukcyjne. Użytkownik otrzymuje e-maila z linkiem lub załącznikiem i informacją o konieczności podjęcia natychmiastowych działań. Po wejściu w link ofiara przekierowywana jest na stronę łudząco podobną do strony zaufanego podmiotu i proszona jest o podanie swoich danych. Oprócz phishingu e-mailowego, istnieje również phishing telefoniczny, gdzie przestępca może podszyć się np. pod firmę kurierską, aby zażądać od ofiary symbolicznej opłaty za dostarczą przesyłkę.

# Phishing

## 1. Czym jest phishing?

Phishing to metoda oszustwa polegająca na podszyciu się pod podmiot gospodarczy, instytucję, osobę, która cieszy się powszechnym zaufaniem i dobrą reputacją, w celu:

1. wyłudzenia cennych informacji (np. danych do logowania do serwisów internetowych);
2. zainfekowania urządzenia, z którego korzysta użytkownik złośliwym oprogramowaniem;
3. nakłonienia do podjęcia określonych działań.

Do przeprowadzania ataków typu phising przestępcy wykorzystują różne kanały komunikacji, takie jak: wiadomość e-mail, wiadomość SMS, rozmowa telefoniczna i media społecznościowe.

# Phishing

## 2. Jak rozpoznać phishing?

Dobrze przygotowany atak typu phishing trudno rozpoznać. Jednak większość masowych ataków ma kilka cech, które powinny wzbudzić czujność i szczególną uwagę.

Gdy zachodzi podejrzenie próby ataku typu phishing, nie należy działać pod wpływem emocji. Żadna instytucja (bank, organy ścigania, urzędy) nigdy nie zgłasza potrzeby przekazywania poufnych informacji za pośrednictwem elektronicznych kanałów komunikacji czy poprzez telefon (np. dane do logowania do serwisów internetowych). Przestępcy mają na celu nakłonienie do niezwłocznego podjęcia działania, a ich kreatywność jest w tym zakresie niemal nieograniczona. Dlatego zachowanie spokoju jest kluczowe dla bezpieczeństwa w sieci. Poniżej lista cech, które mogą świadczyć o próbie ataku typu phishing:

- zazwyczaj wiadomości zmuszają do pilnego i szybkiego działania (np. konieczna jest zmiana hasła ze względów bezpieczeństwa) lub grożą nieprzyjemnymi konsekwencjami (zablokowania konta, odłączeniem od mediów czy usługi itd.);

- wiadomości często zawierają błędy językowe, gramatyczne i nie są pisane poprawną polszczyzną.

# Phishing

## 2. Jak rozpoznać phishing?

- wiadomości zawierają link do adresu łudząco podobnego do prawdziwego adresu w sieci;
- wiadomości mogą zawierać dziwny numer telefonu, adres lub nazwę nadawcy (adres nadawcy e-maila, nazwa nadawcy SMS-a, nazwę konta na serwisie społecznościowym czy komunikatorze);
- wiadomości zawierają załączniki w niestandardowym formacie jak na to, co powinno się w nich znajdować (np. .zip, ,.xls, .xlsx, .rar, .iso czy .doc zamiast zwykłej faktury w PDF)

# Phishing

## 3. Obrona przed phishingiem

Istnieje kilka podstawowych zasad, które pozwolą zapobiec próbie ataku typu phishing:

- należy zweryfikować poprawność domeny, np.:
  Prawdziwa domena (adres): poczta-polska.pl
  Fałszywa domena (adres): poczta-poiska.pl (litera „i" zamiast „l)
  Fałszywa domena (adres): poczta-polskas-pl.word („polskas-pl.word")
  Fałszywa domena (adres): poczta-poIska.pl (zastosowano literę duże „i" w miejsce małej litery „l")

- należy stosować zasadę ograniczonego zaufania wobec informacji otrzymywanych za pośrednictwem poczty elektronicznej i innych elektronicznych kanałów komunikacji;

- nie należy otwierać linków z niespodziewanych wiadomości dotyczących np.: blokady konta, konieczności ustalenia nowego hasła ze względów bezpieczeństwa, autoryzacji płatności itp.

# Phishing

## 3. Obrona przed phishingiem

- nie należy pobierać ani otwierać załączników do maili, których nie oczekujemy, np.: nieoczekiwana faktura, wezwanie do zapłaty itp. Wzmożona aktywność w tym obszarze pojawia się w okresach okołoświątecznych (rzekoma konieczność dopłaty do przesyłki) lub w miesiącach letnich (rzekomo niezapłacone faktury);

- w przypadku wątpliwości w zakresie autentyczności wiadomości e-mail, należy dokonać weryfikacji poprzez inny kanał komunikacyjny, np. poprzez oficjalną infolinię, ale nie korzystając z danych teleadresowych umieszczonych np. w stopce adresowej otrzymanej wiadomości;

- tam gdzie jest to możliwe, należy zabezpieczać dostęp do kont za pomocą weryfikacji dwuetapowej (2FA).

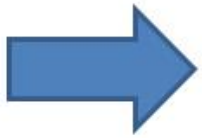
# Phishing

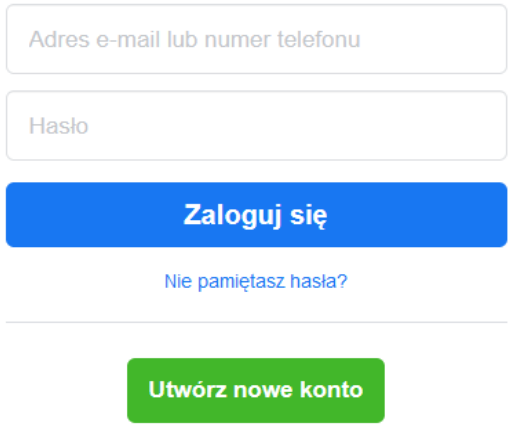
## 3. Przykład ataku typu phishing

1. Publikacja sensacyjnej, emocjonalnej wiadomości w portalu cieszącym się zaufaniem

2. Kliknięcie w link wymusza podanie w formularzu danych do logowania (w tym przypadku jest to fałszywa strona do logowania, pozyskująca prawdziwe poświadczenia do konta)

3. Utrata dostępu do konta systemowego




# Phishing

## 4. Gdzie zgłosić phishing?

Jeśli pomimo zachowania szczególnej ostrożności i środków bezpieczeństwa, doszło do udanego ataku typu phishing, należy skupić się na podjęciu działań w dwóch obszarach:

1. **ograniczenia szkód poprzez:**
   - zmianę haseł do posiadanych kont w serwisach internetowych, w posiadanych urządzeniach elektronicznych (komputer, tablet, telefon, ruter, hasło do WIFI itp.),
   - wykonanie aktualizacji oprogramowania,
   - jeśli sprawa dotyczy kradzieży danych związanych z bankowością, należy bezzwłocznie skontaktować się z infolinią banku, aby podjąć dalsze kroki rekomendowane przez bank,

2. **zgłoszenia oszustwa odpowiednim organom i instytucjom:**
   - przede wszystkim należy złożyć doniesienie na Policję o popełnieniu przestępstwa,
   - wszelkie zdarzenia mające znamiona cyberprzestępstwa należy również zgłosić do zespołów CERT, np. CERT ENEA , CERT Polska (NASK) itp., w celu maksymalnego ograniczania rozpowszechniania się zagrożenia.

## 4. Gdzie zgłosić phishing?

**Dane kontaktowe CERT ENEA**
ul. Pastelowa 8, 60-198 Poznań POLAND

Adres poczty elektronicznej: cert(at)enea(dot)pl

Telefon : +48 61 884 88 00
Telefon alarmowy: +48 785 888 080

Funkcja skrótu klucza PGP: 0x760B060A6C2FA2DB

4. Gdzie zgłosić phishing?

**Dane kontaktowe CERT NASK**

https://incydent.cert.pl/

# Zasady bezpieczeństwa w sieci

## ZASADY BEZPIECZEŃSTWA TECHNICZNEGO

- należy systematycznie aktualizować system operacyjny i przeglądarkę internetową, zarówno w komputerze osobistym, tablecie czy telefonie;
- należy systematycznie tworzyć kopie zapasowe istotnych danych przechowywanych w postaci elektronicznej;
- należy zabezpieczać urządzenia mobilne bezpiecznymi hasłami/ kodami PIN;
- należy zawsze blokować komputer lub urządzenie mobilne, gdy się z niego nie korzysta;
- znaleziony nośnik pamięci, np. pendrive lub ładowarka, czy kabel USB może być wzbogacony o dodatki, powalające zainfekować komputer lub telefon i w rezultacie wykraść dane;

# Zasady bezpieczeństwa w sieci

## ZASADY BEZPIECZEŃSTWA TECHNICZNEGO

- nie należy ignorować komunikatów w przeglądarkach internetowych oraz ostrzeżeń o szkodliwości danej witryny;
- należy zwracać uwagę na adres witryny internetowej, literówka w adresie strony WWW może oznaczać próbę kradzieży danych (phishing);
- należy zwracać uwagę na obecność „zielonej kłódki" i/lub adresu strony WWW rozpoczynającego się od wyrażenia „https://" w przeglądarce; jeżeli adres witryny jest prawidłowy, a kłódka zielona – jest większa pewność, że dane wymieniane są w bezpieczny, zaszyfrowany sposób z tą witryną, w innym przypadku dane mogą być przekazywane w formie niezaszyfrowanej poprzez sieć Internet;
- nie należy instalować żadnego oprogramowania z linków zawartych w SMS lub w wiadomościach e-mail od nieznanych nadawców;
- nie należy pobierać z Internetu danych i oprogramowania, do którego nie posiada się praw autorskich;

# Zasady bezpieczeństwa w sieci

## ZASADY BEZPIECZEŃSTWA TECHNICZNEGO

- należy używać oprogramowania antywirusowego i systematycznie je aktualizować;
- należy stosować bezpieczne hasła dostępu do kont systemowych;
- nie należy stosować jednego hasła do wielu kont systemowych/ kont internetowych;
- jeśli dany system lub serwis internetowy oferuje uwierzytelnienie dwuskładnikowe, należy z niego korzystać;

# Zasady bezpieczeństwa w sieci

## ZASADY BEZPIECZNEGO POSTĘPOWANIA

- zawsze należy kierować się zasadą ograniczonego zaufania i wzmożonej ostrożności;
- nie należy ufać wiadomościom e-mail od nieznanych osób, w szczególności dokumentom jakie przysyłają oraz linkom zawartym w otrzymanych wiadomościach; zawierający „sensacyjne treści" link lub dokument może prowadzić wprost do pobrania oprogramowania, które zaszyfruje lub wykradnie dane, albo wyrządzi inne szkody;
- nie należy zamieszczać w sieci Internet treści, których nie chciałoby się udostępnić publicznie w sieci ;
- nie należy zamieszczać w sieci Internet treści, które mogłyby dla osób o złych intencjach stanowić źródło informacji. Fotorelacja z wakacji umieszczona w mediach społecznościowych może oznaczać, że dom lub mieszkanie jest chwilowo puste;
- należy zachowywać szczególną ostrożność w nawiązywaniu kontaktów przez Internet;

# Zasady bezpieczeństwa w sieci

## ZASADY BEZPIECZNEGO POSTĘPOWANIA

- należy uważać na nietypowe prośby od znajomych, przesłane przez Internet (np. prośba o szybki przelew określonej kwoty); zawsze należy zweryfikować takie prośby przez osobisty lub telefoniczny kontakt (nie SMS) z daną osobą;

- należy uważać na wiadomości SMS/e-mail wzywające do dopłaty niewielkiej nawet kwoty za niedawno zakupiony poprzez Internet towar lub usługę; zawsze należy zweryfikować takie sytuacje, kontaktując się innymi kanałami ze sprzedawcą;

- robiąc zakupy w Internecie, należy wystrzegać się niezwykłych promocji; jeżeli sklep internetowy jest znacznie tańszy od konkurencji, należy zweryfikować, kim jest jego właściciel, gdzie ta firma ma swoją siedzibę i jakie sposoby płatności preferuje, brak płatności kartą czy płatności przy odbiorze, brak lub tylko jeden numer telefonu, adres sklepu wskazujący na lokalizację w egzotycznym kraju, wyłącznie doskonałe opinie i praktycznie brak śladu historii tego sklepu w opiniach na innych witrynach to wskazówki, że można mieć do czynienia z próbą wyłudzenia;

- każde podejrzenie naruszenia cyberbezpieczeństwa należy zgłaszać do odpowiednich służb;

# Zasady bezpieczeństwa w sieci

## ZASADY BEZPIECZNEGO POSTĘPOWANIA

- należy chronić dzieci przed niebezpieczeństwem w Internecie;
- czytając wiadomości SMS z banków, zawsze bardzo dokładnie należy porównać numer konta i kwotę;
- nie należy ufać publicznym sieciom Wi-fi, w szczególności na lotniskach, w hotelach czy restauracjach;
- należy szanować prywatność innych; w przypadku omyłkowego otrzymania wiadomości kierowanej do kogoś innego, należy powiadomić nadawcę o pomyłce i skasować wiadomość.

# Bezpieczne hasło

## 1. Wprowadzenie

Hasła do kont systemowych, urządzeń elektronicznych, portali internetowych to powszechnie stosowany sposób chronienia dostępu do poufnych danych i usług. Jednak skuteczność tej ochrony jest uwarunkowana od sposobu utworzenia hasła, jego stosowania w sposób prawidłowy, w tym dostosowany do aktualnych wymogów technicznych i organizacyjnych.

Hasła są jednym z podstawowych sposobów, za pośrednictwem których można udowodnić swoją tożsamość. Używanie silnych haseł jest niezbędne, by chronić dostęp do swoich danych.

# Bezpieczne hasło

## 2. Jak zadbać o bezpieczne hasła?

Nie istnieje jedna uniwersalna metoda tworzenia bezpiecznego hasła. Jednym z rekomendowanych sposobów jest opracowanie hasła z trzech losowych słów, które należy ze sobą połączyć, na przykład „herbataautobuspies" lub „ścianagrubakoszula".

Można również wybrać słowa, które łatwo zapadają w pamięć, ale należy unikać takich zwrotów, które mogą być łatwe do odgadnięcia, np. „jedendwatrzy" lub są ściśle związane z konkretną osobą, jak: imiona i nazwiska członków rodziny lub zwierząt domowych.

# Bezpieczne hasło

## 2. Jak zadbać o bezpieczne hasła?

Należy pamiętać o kilku prostych zasadach:

- ✓ **należy stosować hasło o długości co najmniej 14 znaków**
  Rekomenduje się kombinację kilku słów z użyciem DUŻYCH, małych liter, cyfr i znaków specjalnych (np. !@#$%&).

- ✓ **nie należy używać jednego hasła do różnych usług**
  Hasła dostępowe do poszczególnych usług powinny być unikatowe, w szczególności do serwisów bankowych, systemu poczty elektronicznej i kont w domenie GOV (np. profil zaufany, mObywatel itp.)

- ✓ **należy włączyć weryfikację dwuetapową (2FA)**
  Jeśli dana usługa (bank, konto pocztowe itp.) w sieci Internet umożliwia stosowanie weryfikacji dwuetapowej, to należy z niej korzystać. Weryfikacja dwuetapowa polega na uwierzytelnieniu hasłem (w pierwszym kroku) oraz w drugim kroku za pomocą jednorazowego kodu lub potwierdzenia w aplikacji zainstalowanej na urządzeniu mobilnym.

# Bezpieczne hasło

## 2. Jak zadbać o bezpieczne hasła?

- ✓ **należy dbać o poufność hasła**
  Nikomu nie należy ujawniać swojego hasła.

- ✓ **należy stosować zasady tzw. cyberhigieny**
  Należy unikać wprowadzenia hasła w urządzeniach, nad którymi nie posiada się kontroli, np. kioski internetowe.

- ✓ **należy zachować ostrożność**
  Jeśli zachodzi podejrzenie, iż hasło mogło zostać ujawnione lub podejrzane przez osoby postronne w trakcie jego wprowadzania, bez zbędnej zwłoki należy hasło zmienić na nowe.

- ✓ **zmiana hasła**
  Hasło powinno być zmieniane nie rzadziej niż co 90 dni, to pozwoli na zminimalizowanie ryzyka przeprowadzenia udanego ataku na hasło użytkownika.

- ✓ **nie należy zapamiętywać haseł w przeglądarkach internetowych**
  Korzystanie z funkcji zapamiętywania haseł w przeglądarce internetowej nie jest bezpiecznym rozwiązaniem. Zamiast tego rekomenduje się stosowanie menadżerów haseł.



**Dane kontaktowe CERT**

ul. Pastelowa 8, 60-198 Poznań POLAND

Adres poczty elektronicznej: cert(at)enea(dot)pl

Telefon : +48 61 884 88 00
Telefon alarmowy: +48 785 888 080

Funkcja skrótu klucza PGP: 0x760B060A6C2FA2DB