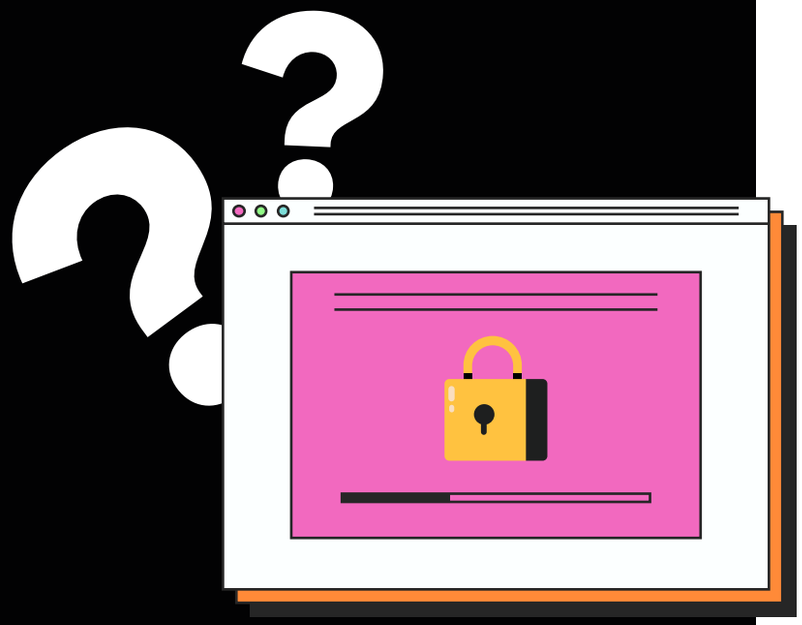


CYBER
BEZPIECZEŃSTWO DLA KAŻDEGO

Jak chronić siebie i swoich bliskich w internecie ?

Celem tej broszury

jest pokazanie, jak rozpoznać zagrożenia
i jak się przed nimi bronić – prosto i praktycznie.



Dlaczego warto dbać o cyberbezpieczeństwo?

Internet to wspaniałe narzędzie – pomaga nam w nauce, pracy, zakupach i kontaktach z bliskimi. Jednak w sieci pojawia się coraz więcej zagrożeń, które mogą dotknąć każdego z nas, niezależnie od wieku.

Na co trzeba uważać w sieci?

Phishing (wyłudzanie danych)

To fałszywe e-maile, SMS-y lub wiadomości, które udają zaufane firmy (np. bank, pocztę, sklep internetowy).
W wiadomości znajduje się link do strony, która wygląda prawdziwie, ale jest pułapką. Po kliknięciu możesz: **ujawnić swoje dane logowania / zainstalować wirusa / stracić pieniądze z konta**

Jak się chronić?

nigdy nie klikaj w linki z nieznanych źródeł	sprawdź adres nadawcy – często różni się jednym znakiem	bank nigdy nie prosi o podanie hasła przez e-mail

Wirusy / złośliwe oprogramowanie

To programy, które mogą kraść dane, blokować komputer lub podsłuchiwać Twoją aktywność.

Jak się chronić?

instaluj program antywirusowy i aktualizuj go	nie pobieraj plików z nieznanych stron	nie instaluj aplikacji spoza oficjalnych sklepów (Google Play, App Store)

Fałszywe sklepy i ogłoszenia

Oszust zakłada stronę, która wygląda jak znany sklep, by wyłudzić pieniądze lub dane kart.

Jak się chronić?

sprawdź opinie o sklepie	zobacz, czy strona ma „https://" i kłódkę w pasku adresu	nie płać przelewem „na konto osoby prywatnej"

Dziecko w internecie – jak zadbać o bezpieczeństwo najmłodszych?

Internet to świetne miejsce do nauki i zabawy, ale dzieci często nie rozumieją ryzyka, ukrytego w sprzestrzeni sieciowej.

Największe zagrożenia dla dzieci:

kontakt z nieznajomymi, którzy podszywają się pod rówieśników;

dostęp do nieodpowiednich treści (przemoc, pornografia, hazard);

cyberprzemoc w grach lub mediach społecznościowych.

Jak chronić dziecko:

ustal zasady korzystania z internetu – ile czasu, jakie strony, kiedy;

zainstaluj kontrolę rodzicielską – np. Family Link, Windows Family Safety;

rozmawiaj o zagrożeniach – tłumacz spokojnie, co może się stać;

zachęcaj do zaufania – jeśli dziecko zobaczy coś niepokojącego, niech przyjdzie do Ciebie.



Dla dzieci:

Nigdy nie podawaj swojego imienia, adresu, numeru telefonu ani szkoły osobom poznanym online.

Bezpieczne korzystanie z internetu na co dzień

Zasady bezpiecznego użytkowania:

używaj silnych haseł – minimum 8 znaków, z literami, cyframi i symbolami;

włącz uwierzytelnianie dwuskładnikowe (2FA) – kod SMS lub aplikacja zabezpieczająca;

aktualizuj system i aplikacje – luki bezpieczeństwa są często naprawiane w aktualizacjach;

nie klikaj w reklamy „Cudowny sposób na zarobek" – to często oszustwo inwestycyjne.

Wskazówka:

Używaj różnych haseł do różnych serwisów. Możesz korzystać z menedżera haseł, który je bezpiecznie przechowuje.

Co robić, gdy ktoś Cię krzywdzi w sieci?

Cyberprzemoc to: obrażanie, poniżanie, rozsyłanie fałszywych informacji lub zdjęć bez zgody.

Jak reagować:

nie odpowiadaj agresją;

zrób zrzuty ekranu (dowody);

zgłoś sprawę administratorowi portalu, nauczycielowi, policji lub rodzicom;

porozmawiaj z kimś zaufanym.

POMOC:

Telefon zaufania dla dzieci i młodzieży: 116 111
Dorośli i rodzice: 800 100 100

Seniorze – internet to Twoja wygoda, ale i odpowiedzialność

Najczęstsze oszustwa wobec seniorów:

fałszywe telefony lub wiadomości „z banku";

„wnuczek w potrzebie" w wersji internetowej;

inwestycje w kryptowaluty i szybki zysk;

oszuści podszywający się pod kuriera lub urzędnika.

Jak się chronić:

- nie otwieraj załączników od nieznanych nadawców;
- nie klikaj w linki w SMS-ach od „banku" – zawsze zaloguj się samodzielnie przez stronę banku;
- nie przekazuj nikomu kodów BLIK ani haseł;
- w razie wątpliwości – zadzwoń do rodziny lub banku.

Kradzież tożsamości

Złodzieje mogą użyć Twojego imienia, zdjęcia lub numeru PESEL, by np. wziąć kredyt lub założyć konto. Najczęściej mogą użyć Twoich danych, do nawiązania kontaktu z blizkimi do Ciebie osobami aby manipulować dla uzyskania korzyści.

Jak się chronić:

- nie udostępniaj dokumentów w internecie (dowodu, prawa jazdy);
- nie publikuj zbyt wielu prywatnych informacji;
- korzystaj z silnych, unikalnych haseł.

Ważne:

Nie ma głupich pytań, jeśli chodzi o bezpieczeństwo. Lepiej zapytać dwa razy niż stracić pieniądze raz.

Nie wszystko warto pokazywać w internecie

Zagrożenia:

złodzieje mogą wykorzystać zdjęcia z wakacji (wiedzą, że nie ma Cię w domu);

ktoś może skopiować Twoje zdjęcia i podszyć się pod Ciebie;

nadmierne udostępnianie danych może ułatwić oszustwa.

Zasady bezpiecznego korzystania:

- nie publikuj adresu, daty urodzenia, numeru telefonu, szkoły dzieci;
- ogranicz widoczność profilu tylko dla znajomych;
- nie klikaj w linki z wiadomości od „znajomych", jeśli wyglądają podejrzanie.

Twoje cyfrowe bezpieczeństwo w praktyce

Narzędzia, które warto mieć:

Antywirus i zapora sieciowa (firewall) – blokują wirusy i ataki.

Kopia zapasowa danych – na dysku zewnętrznym lub w chmurze - dla uniknięcia całkowitej utraty plików w przypadku kradzieży danych cyfrowych.

Menedżer haseł – bezpiecznie przechowuje loginy.

Zasady bezpieczeństwa:

- nie ufaj każdej wiadomości – nawet jeśli wygląda prawdziwie;
- regularnie **ucz się** nowych zasad bezpieczeństwa – **internet się zmienia!**

Sztuczna inteligencja / – nowy typ oszustwa

Sztuczna inteligencja (AI) coraz częściej wykorzystywana jest do tworzenia realistycznych obrazów, głosów i filmów. Niestety, przestępcy również z niej korzystają – podszywają się pod prawdziwe osoby, by wyłudzić pieniądze lub dane.

Na czym to polega?
Oszust, korzystając z AI, potrafi:

stworzyć deepfake – wideo lub nagranie głosowe, w którym ktoś mówi coś, czego nigdy nie powiedział	wygenerować wiadomość głosową, z głosem bliskiej osoby	napisać e-mail, który brzmi jak wiadomość od znajomego lub pracodawcy

Takie działania mają na celu zmylenie ofiary – wywołanie emocji i skłonienie do szybkiej reakcji, np. przelewu pieniędzy.

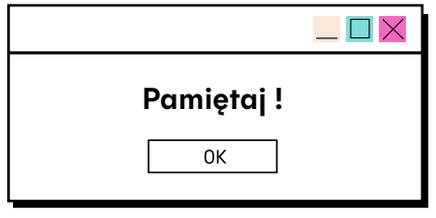
Jak rozpoznać fałszywą tożsamość AI?	głos lub wideo brzmią „dziwnie" – nienaturalny rytm, brak emocji;
	nadawca prosi o natychmiastowe działanie („zrób to teraz, bo stracę konto");
	w treści pojawiają się błędy lub nietypowe zwroty.

Jak się chronić?

- nie działaj impulsywnie. Zawsze zweryfikuj wiadomość, dzwoniąc do tej osoby lub firmy;
- nie publikuj prywatnych nagrań i zdjęć. Mogą zostać wykorzystane do stworzenia deepfake'a;
- nie ufaj wiadomościom, które budzą silne emocje. To typowa taktyka manipulacji;
- nie klikaj w linki i nie przekazuj kodów BLIK.

Bezpieczeństwo zaczyna się od Ciebie

Internet to potężne narzędzie – daje wiedzę, kontakt i rozrywkę, ale wymaga czujności i rozsądku.



- chronisz siebie – chronisz też innych;
- nie ma bezpieczeństwa bez ostrożności;
- dziel się wiedzą – naucz dzieci, rodziców, dziadków, jak być bezpiecznym.

„Klikaj z głową – bo w sieci nie wszystko jest tym, czym się wydaje."

Partner:

Mazowsze. serce Polski

Przedsięwzięcie współfinansowane ze środków Samorządu Województwa Mazowieckiego

Mazowsze dla organizacji pozarządowych

