

Interreg



Współfinansowany przez
UNIĘ EUROPEJSKĄ
Kofinansiert von
der EUROPÄISCHEN UNION

Polska – Sachsen

PORADNIK SENIORA

Cyberbezpieczeństwo – najczęstsze zagrożenia oraz sposoby, jak się przed nimi chronić



RATGEBER

FÜR SENIORINNEN UND SENIOREN

Cybersicherheit – die häufigsten Bedrohungen und wie man sich davor schützen kann

Poradnik stanowi materiał informacyjny dla seniorów zrealizowany w ramach projektu „Seniorzy – ambasadorzy na rzecz zrównoważonego rozwoju regionu”.
Der Ratgeber ist ein Informationsmaterial für Seniorenw/-innen, umgesetzt im Rahmen des Projekts „Seniorenbotschafterinnen und Seniorenbotschafter für nachhaltige Entwicklung der Region”.

Phishing (wyłudzenie danych)

To technika, w której oszuści podszywają się pod znane instytucje np. banki, i wysyłają fałszywe e-maile lub SMS-y z prośbą o podanie danych logowania.

Jak się chronić? Nigdy nie klikaj w podejrzaną linki. Zawsze sprawdzaj adres nadawcy. Bank nigdy nie prosi o hasło e-mailem!

Vishing (oszustwo telefoniczne)

Oszuści dzwonią, podając się za pracowników banku lub urzędu i proszą o dane osobowe albo dostęp do konta.

Jak się chronić? Nie podawaj danych przez telefon. Rozłącz się i samodzielnie zadzwoń na oficjalny numer banku.

SPAM (niechciane wiadomości)

Mogą zawierać reklamy, ale także złośliwą zawartość.

Jak się chronić? Nie otwieraj wiadomości od nieznanego nadawcy. Użyj programu antyspamowego.

Phishing

Bei dieser Technik geben sich Betrüger/-innen als bekannte Institutionen, z. B. Banken, aus und versenden gefälschte E-Mails oder SMS-Nachrichten, in denen sie nach Login-Daten fragen.

Wie können Sie sich schützen? Klicken Sie niemals auf verdächtige Links. Überprüfen Sie immer die Adresse des Absenders. Die Bank fragt Sie niemals per E-Mail nach Ihrem Passwort!

Vishing (Telefonbetrug)

Betrüger rufen an und geben sich als Bank – oder Behördenmitarbeiter/-innen aus und bitten um persönliche Daten oder den Zugang zu einem Konto.

Wie können Sie sich schützen? Geben Sie Ihre Daten nicht per Telefon heraus. Legen Sie auf und rufen Sie selbst die offizielle Nummer der Bank an.

SPAM (unerwünschte Nachrichten)

Sie können Werbung, aber auch böartige Inhalte enthalten.

Wie können Sie sich schützen? Öffnen Sie keine Nachrichten von unbekanntem Absender. Verwenden Sie ein Antispam-Programm.

Spooftng (podszywanie się pod numery lub adresy)

Oszuści podszywają się pod znane numery telefonów lub adresy e-mail.

Jak się chronić? Nie ufaj tylko numerowi czy adresowi. Jeśli rozmówca prosi o dane, zakończ rozmowę i zweryfikuj kontakt samodzielnie.

Oszustwo na kod BLIK

Osoba podszywa się pod znajomego i prosi o kod BLIK, którym potem wypłaca pieniądze z bankomatu.

Jak się chronić? Zawsze zadzwoń do osoby, która prosi o kod BLIK, zanim go przekażesz.



Spooftng (Nachahmung von Nummern oder Adressen)

Betrüger/-innen geben sich als bekannte Telefonnummern oder E-Mail-Adressen aus.

Wie können Sie sich schützen? Vertrauen Sie nicht einfach auf die Nummer oder Adresse. Wenn der Anrufer nach Details fragt, beenden Sie das Gespräch und überprüfen Sie den Kontakt selbst.

Vorsicht vor digitalen Betrügereien

Wenn Sie jemand über einen Messenger kontaktiert und Sie bittet, Geld über einen Dienst wie Paypal zu überweisen, überprüfen Sie immer die Identität dieser Person.

Geben Sie niemals Bestätigungs-codes für Überweisungen oder Ihre Zugangsdaten für das Online-Banking weiter.

Denken Sie daran: Banken und Behörden fragen niemals per E-Mail oder Telefon nach persönlichen Daten.

Fałszywe sklepy internetowe

Sklepy wyglądają wiarygodnie, ale po dokonaniu płatności towar nie dociera.

Jak się chronić? Sprawdzaj opinie o sklepie, upewnij się, że adres strony zaczyna się od „https://”. Nie płać z góry nieznanym sprzedawcom.

Fałszywe wiadomości z banku (e-mail lub SMS)

Informują o rzekomych problemach z kontem i nakłaniają do kliknięcia w link.

Jak się chronić? Banki nie wysyłają linków do logowania. Lepiej zalogować się samodzielnie przez znaną stronę banku.

Fałszywe SMS-y ze złośliwym oprogramowaniem

Zawierają link do rzekomej przesyłki lub wiadomości. Kliknięcie instaluje wirusa.

Jak się chronić? Nie klikaj w podejrzane linki. Zainstaluj oprogramowanie antywirusowe na telefonie.

Falsche Online-Shops

Die Shops sehen glaubwürdig aus, aber nach der Zahlung kommt die Ware nicht an.

Wie können Sie sich schützen? Überprüfen Sie die Bewertungen des Shops und vergewissern Sie sich, dass die Adresse der Website mit „https://“ beginnt. Zahlen Sie nicht im Voraus an unbekannte Verkäufer.

Falsche Nachrichten von der Bank (E-Mail oder SMS)

Sie informieren über angebliche Probleme mit dem Konto und fordern Sie auf, auf einen Link zu klicken.

Wie können Sie sich schützen? Banken versenden keine Links zum Einloggen. Es ist besser, sich selbst über die bekannte Website der Bank einzuloggen.

Falsche SMS mit Schadsoftware

Sie enthalten einen Link zu einer angeblichen Sendung oder Nachricht. Durch Anklicken wird ein Virus installiert.

Wie können Sie sich schützen? Klicken Sie nicht auf verdächtige Links. Installieren Sie Antivirensoftware auf Ihrem Smartphone.

Fałszywe panele logowania do instytucji

Oszuści tworzyli strony łudzaco podobne do stron urzędów i banków.

Jak się chronić? Upewnij się, że adres strony jest poprawny.

Nie wpisuj danych logowania na podejrzanych stronach.

Fake newsy w sieci

Fałszywe informacje mające wpływ na emocje i decyzje.

Jak się chronić? Sprawdzaj informacje w wiarygodnych źródłach, np. w serwisach informacyjnych lub na stronach rządowych.



Falsche Einloggsseiten von Institutionen

Betrüger haben Websites erstellt, die den Websites von Behörden und Banken zum Verwechseln ähnlich sehen.

Wie können Sie sich schützen? Vergewissern Sie sich, dass die Adresse der Website korrekt ist. Geben Sie keine Anmeldedaten auf verdächtigen Websites ein.

Fake News im Internet

Falsche Informationen, die Emotionen und Entscheidungen beeinflussen.

Wie können Sie sich schützen? Überprüfen Sie Informationen in zuverlässigen Quellen, z. B. in Nachrichtendiensten oder auf Regierungswebsites.

Podstawowe zasady bezpieczeństwa w sieci:

- ◆ Korzystaj z silnych, różnych haseł do różnych serwisów.
- ◆ Aktualizuj system i programy.
- ◆ Użyj dwuskładnikowego uwierzytelniania (2FA).
- ◆ Nigdy nie udostępniaj danych osobowych przez telefon ani e-mail.
- ◆ Miej ograniczone zaufanie do nieznanym osobom w Internecie.

Pamiętaj: jeśli coś wydaje się podejrzane, lepiej to sprawdzić niż dać się oszukać. Rozmawiaj z rodziną i znajomymi o bezpieczeństwie w sieci. W razie wątpliwości skontaktuj się z zaufaną osobą lub instytucją.

Zadbajmy wspólnie o bezpieczeństwo w sieci!

WIĘCEJ INFORMACJI NA STRONACH:

<https://www.gov.pl/web/cyberbezpieczenstwo>

<https://www.cert.pl>

<https://www.zaufanatrzeciastrona.pl>

<https://www.niebezpiecznik.pl>

Grundlegende Sicherheitsregeln im Internet:

- ◆ Verwenden Sie starke, unterschiedliche Passwörter für verschiedene Dienste.
- ◆ Aktualisieren Sie Ihr System und Ihre Programme.
- ◆ Verwenden Sie eine Zwei-Faktor-Authentifizierung (2FA).
- ◆ Geben Sie niemals persönliche Daten per Telefon oder E-Mail weiter.
- ◆ Seien Sie vorsichtig im Umgang mit unbekanntem Personen im Internet.

Denken Sie daran: wenn Ihnen etwas verdächtig vorkommt, überprüfen Sie es lieber, als sich täuschen zu lassen. Sprechen Sie mit Ihrer Familie und Ihren Freunden über Sicherheit im Internet. Wenden Sie sich im Zweifelsfall an eine vertrauenswürdige Person oder Institution.

Sorgen wir gemeinsam für Sicherheit im Internet!

<https://www.bsi.bund.de> (Bundesamt für Sicherheit in der Informationstechnik – BSI)

<https://www.polizei-beratung.de> (Polizeiliche Kriminalprävention der Länder und des Bundes)

<https://www.verbraucherzentrale.de> (Verbraucherzentrale – Verbraucherberatung zum Thema Internet und Sicherheit)

<https://www.bundespolizei.de> (Bundespolizei – Hinweise zu Cyberkriminalität)