WSPÓŁCZESNE ZAGROŻENIA CYBERNETYCZNE METODY OSZUSTW I SKUTECZNE STRATEGIE OCHRONY

OCHRONA OSÓB I MIENIA

MARCIN NIEDOPYTALSKI

WSB SECURITY

CYBER SECURITY

W dobie globalnej cyfryzacji i rosnącej roli technologii telekomunikacyjnych coraz więcej osób pada ofiarą oszustw związanych z fałszywymi połączeniami telefonicznymi, wiadomościami SMS oraz oszustwami internetowymi. Przestępcy posługują się zaawansowanymi metodami socjotechnicznymi, a wraz z rozwojem sztucznej inteligencji (AI) ich techniki stają się coraz bardziej wyrafinowane i trudniejsze do wykrycia. Niniejszy artykuł przedstawia szczegółową analizę najczęstszych oszustw stosowanych we współczesnym świecie, ze szczególnym uwzględnieniem zagrożeń wynikających z wykorzystania AI, oraz skutecznych strategii obronnych, pozwalających na ochronę zarówno dorosłych, jak i dzieci przed zagrożeniami w cyberprzestrzeni.

1. Typologia współczesnych oszustw telekomunikacyjnych

1.1 Oszustwa „na policjanta"

Oszuści podszywają się pod funkcjonariuszy organów ścigania, informując ofiary o rzekomym zagrożeniu finansowym lub konieczności współpracy w tajnym śledztwie. W celu zapewnienia „bezpieczeństwa" nakłaniają do przekazania środków pieniężnych lub ujawnienia danych wrażliwych.

Jak się chronić?

- Policja nigdy nie prosi o przekazanie pieniędzy ani danych osobowych.
- Należy weryfikować tożsamość rozmówcy poprzez kontakt z oficjalną placówką.

1.2 Oszustwa „na lekarza"

Przestępcy informują o nagłym zagrożeniu zdrowotnym bliskiej osoby i proszą o natychmiastowy przelew pieniędzy na kosztowne leczenie.

Jak się chronić?

- Weryfikować informacje, kontaktując się z placówkami medycznymi.
- Nie podejmować pochopnych decyzji pod wpływem presji emocjonalnej.

1.3 Oszustwa „na bankowca"

Oszuści podszywają się pod przedstawicieli instytucji finansowych, informując o rzekomym zagrożeniu dla konta bankowego ofiary. Często nakłaniają do

zainstalowania aplikacji do zdalnej kontroli lub dokonania przelewu na „bezpieczne konto".

Jak się chronić?

- Banki nigdy nie proszą o podanie haseł ani kodów dostępu.
- Nie instalować aplikacji z linków przesyłanych przez telefon.
- Kontaktować się bezpośrednio z bankiem poprzez oficjalny numer.

1.4 Oszustwa związane z wynajmem mieszkań

Przestępcy zamieszczają fałszywe ogłoszenia dotyczące wynajmu mieszkań i żądają przedpłaty przed obejrzeniem lokalu.

Jak się chronić?

- Nie dokonywać przedpłat przed obejrzeniem nieruchomości.
- Weryfikować tożsamość wynajmującego oraz dokumentację lokalu.

1.5 Oszustwa związane z biurami podróży

Oszuści oferują fałszywe wycieczki i bilety lotnicze po atrakcyjnych cenach.

Jak się chronić?

- Sprawdzać rejestrację biura podróży w oficjalnych bazach danych.
- Unikać płatności na prywatne konta bankowe.

2. Wykorzystanie sztucznej inteligencji do oszustw

Rozwój AI otworzył nowe możliwości dla przestępców. Przykłady wykorzystania sztucznej inteligencji w cyberprzestępczości obejmują:

- Deepfake głosowy – oszuści mogą naśladować głos członka rodziny lub przedstawiciela instytucji.
- Generowanie fałszywych wiadomości e-mail i SMS – AI może automatycznie generować treści dopasowane do ofiary.
- Automatyzacja oszustw – chatboty i algorytmy AI mogą prowadzić wielowątkowe rozmowy, imitując realnych ludzi.

Jak się chronić?

- Nie ufać nagłym telefonicznym prośbom o pomoc finansową.
- Weryfikować głosy poprzez pytania kontrolne, które tylko bliska osoba zna.
- Nie klikać w podejrzane linki w wiadomościach.

3. Ochrona dzieci w sieci

Dzieci są szczególnie narażone na cyberzagrożenia, takie jak oszustwa, cyberprzemoc i nieodpowiednie treści. Zagrożenia obejmują:

- Manipulacje w mediach społecznościowych – oszuści mogą podszywać się pod rówieśników.
- Fałszywe konkursy i promocje – wyłudzanie danych logowania do kont w grach.
- Kontakt z nieznajomymi – ryzyko nawiązania niebezpiecznych znajomości.

Jak zabezpieczyć dzieci?

- Edukować dzieci o zagrożeniach w sieci.
- Instalować kontrolę rodzicielską na urządzeniach.
- Monitorować aktywność online dzieci i uczyć zasad cyberbezpieczeństwa.

4. Jak skutecznie zgłaszać oszustwa?

W przypadku podejrzenia próby oszustwa należy podjąć odpowiednie kroki:

- Policja – zgłaszanie oszustw na numer 112 lub lokalny komisariat.
- CERT Polska – zgłaszanie zagrożeń internetowych na stronie https://incydent.cert.pl/.
- UOKiK – zgłaszanie oszustw konsumenckich na stronie https://www.uokik.gov.pl/.

5. Wnioski i rekomendacje

Oszustwa w świecie cyfrowym stają się coraz bardziej zaawansowane i trudne do wykrycia. Kluczowe strategie ochrony obejmują:

✅ Świadomość zagrożeń – edukacja na temat współczesnych metod oszustw. ✅ Weryfikacja rozmówców – kontakt z instytucjami na oficjalnych numerach. ✅ Nieklikanie w podejrzane linki – ochrona przed zainfekowaniem urządzeń. ✅ Zabezpieczenie dzieci w sieci – edukacja i kontrola rodzicielska. ✅ Zgłaszanie oszustw do odpowiednich organów – szybka reakcja na zagrożenia.

Współczesne technologie ułatwiają życie, ale niosą ze sobą także nowe zagrożenia. Tylko poprzez świadome i odpowiedzialne korzystanie z Internetu możemy skutecznie chronić siebie i naszych bliskich przed cyberprzestępcami.

Poradnik: Jak zabezpieczyć się przed podejrzanymi SMS-ami i połączeniami telefonicznymi

W dobie cyfryzacji i powszechnego dostępu do telefonii komórkowej coraz częściej spotykamy się z różnymi formami oszustw. Ataki telefoniczne i SMS-owe stały się popularnym sposobem na wyłudzanie danych osobowych oraz pieniędzy. Fałszywe wiadomości często podszywają się pod banki, operatorów komórkowych, instytucje rządowe czy znane stacje radiowe, jak RMF FM. W tym poradniku dowiesz się, jak skutecznie chronić się przed tego typu zagrożeniami, jakie kroki podjąć w przypadku podejrzanego SMS-a lub połączenia oraz jak zgłaszać oszustwa do odpowiednich instytucji.

1. Jak rozpoznać oszukańczy SMS?

Podejrzane wiadomości SMS często mają następujące cechy:

- **Zawierają linki do podejrzanych stron** – oszuści próbują nakłonić Cię do kliknięcia w link prowadzący do fałszywej strony.
- **Informują o wygranej, której nie oczekiwałeś** – np. w loterii RMF FM lub innym konkursie, w którym nigdy nie brałeś udziału.
- **Straszą konsekwencjami** – np. blokadą konta bankowego, przeterminowaną płatnością.
- **Pochodzą od nieznanego nadawcy** – numer nadawcy może wyglądać na losowy lub przypominać numer premium (np. 7474).

- **Zawierają błędy językowe i stylistyczne** – wiele oszustw pochodzi od osób spoza Polski, co skutkuje niepoprawnym językiem w wiadomościach.

Przykładowy fałszywy SMS:

"Gratulacje! Wygrałeś 5000 zł w konkursie RMF FM. Kliknij tutaj, aby odebrać nagrodę: [podejrzany link]".

WAŻNE! Nie klikaj w podejrzane linki i nie podawaj swoich danych.

2. Jak rozpoznać oszukańcze połączenie telefoniczne?

Nie tylko SMS-y są wykorzystywane przez oszustów. Mogą oni również dzwonić, udając przedstawicieli banku, operatora czy instytucji rządowej.

Charakterystyczne cechy podejrzanych połączeń:

- **Rozmówca prosi o dane osobowe lub finansowe** – np. numer PESEL, hasło do banku, kod BLIK.
- **Dzwoni z nieznanego numeru lub numeru zagranicznego**.
- **Podszywa się pod instytucję (np. ZUS, bank, policję)**.
- **Stara się wywołać presję** – np. mówi, że musisz natychmiast podjąć decyzję.

Jak reagować?

- **Nie podawaj żadnych danych przez telefon**.
- **Nie oddzwaniaj na podejrzane numery**.
- **Zweryfikuj informacje, dzwoniąc bezpośrednio do danej instytucji**.

3. Jak blokować podejrzane numery?

Blokowanie numerów na iPhone:

1. Otwórz aplikację **Telefon** lub **Wiadomości**.
2. Znajdź numer, kliknij **ikonę „i”** obok niego.
3. Wybierz **„Blokuj ten kontakt”**.

Blokowanie numerów na Androidzie:

1. Otwórz aplikację **Telefon** lub **Wiadomości**.
2. Przytrzymaj numer, który chcesz zablokować.
3. Wybierz **„Blokuj”** lub **„Zgłoś jako spam”**.

4. Jak unikać oszustw SMS i telefonicznych?

- **Nie klikaj w podejrzane linki**.
- **Nie odpowiadaj na nieznane wiadomości**.
- **Nie podawaj swoich danych w SMS-ach i rozmowach telefonicznych**.
- **Sprawdzaj informacje na oficjalnych stronach banków, operatorów i instytucji**.
- **Korzystaj z aplikacji blokujących spam** (np. Truecaller, Hiya).
- **Zapisz numer CERT Polska do zgłaszania oszustw** (799 448 084).

5. Jak zgłaszać oszustwa?

Jeśli otrzymałeś podejrzany SMS lub połączenie, zgłoś je do odpowiednich instytucji:

CERT Polska (rządowy zespół ds. cyberbezpieczeństwa)

📩 Wyślij podejrzanego SMS-a na numer: **799 448 084**
🌐 Zgłoś incydent na stronie: https://incydent.cert.pl/

UOKiK (Urząd Ochrony Konkurencji i Konsumentów)

🌐 Strona zgłoszeniowa: https://www.uokik.gov.pl/

Twój operator komórkowy

Większość operatorów umożliwia zgłaszanie podejrzanych numerów w aplikacjach mobilnych.

6. Jakie aplikacje mogą pomóc?

Możesz zainstalować aplikacje pomagające w identyfikacji i blokowaniu podejrzanych połączeń:

- **Truecaller** (Android, iOS) – identyfikuje i blokuje numery oszustów.
- **Hiya** (Android, iOS) – automatycznie filtruje spamowe połączenia.
- **CallBlocker** – blokowanie nieznanych numerów.

7. Co zrobić, jeśli padłeś ofiarą oszustwa?

Jeśli przez pomyłkę podałeś swoje dane:

1. **Zmień hasła do bankowości internetowej i innych ważnych kont**.
2. **Skontaktuj się ze swoim bankiem i sprawdź, czy nie doszło do nieautoryzowanych transakcji**.
3. **Zgłoś incydent do CERT Polska**.
4. **Poinformuj policję, jeśli oszustwo dotyczyło utraty pieniędzy**.
5. **Monitoruj swoje konto bankowe i raporty kredytowe**.

Oszustwa SMS-owe i telefoniczne to coraz większe zagrożenie. Jednak stosując odpowiednie środki ostrożności, można skutecznie się przed nimi chronić. Kluczowe zasady:

✅ **Nie klikaj w podejrzane linki**
✅ **Blokuj podejrzane numery**
✅ **Nie podawaj danych osobowych i finansowych przez telefon**
✅ **Używaj aplikacji antyspamowych**
✅ **Zgłaszaj oszustwa do CERT Polska**

Pamiętaj, że ostrożność i świadomość są najlepszą ochroną przed cyberprzestępcami!