cybergia.pl

Inżynieria społeczna – socjotechniki

NAUKA DLA SPOŁECZEŃSTWA

Ministerstwo Nauki i Szkolnictwa Wyższego

cybergia.pl

Projekt dofinansowany ze środków budżetu państwa, przyznanych
przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II”

SOCJOTECHNIKA

Socjotechnika to sposób manipulowania ludźmi tak, aby zrobili coś, czego normalnie by nie zrobili, np. kliknęli w link, podali swoje dane, otworzyli podejrzany plik. Cyberprzestępcy stosują ją, by ominąć zabezpieczenia komputerów i zdobyć dostęp do kont, pieniędzy czy prywatnych informacji. Często podszywają się pod zaufane osoby czy instytucje.

Ponad 600 tys. przypadków phishingu zgłoszonych w Polsce w 2024 r. (wzrost o 62%).

Zablokowano 1,5 mln złośliwych SMS-ów.

Tylko co piąta osoba zgłasza podejrzane wiadomości.

NAUKA DLA SPOŁECZEŃSTWA
Ministerstwo Nauki i Szkolnictwa Wyższego
cybergia.pl
Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

PHISHING

Phishing to oszustwo polegające na wysyłaniu fałszywych wiadomości udających oficjalne komunikaty. Ich celem jest nakłonienie odbiorcy do kliknięcia w złośliwy link lub pobrania pliku, a następnie do podania poufnych danych, takich jak loginy, hasła czy informacje finansowe, które trafiają w ręce przestępców.

Przykłady wiadomości phishingowych:

Mail z banku o blokadzie konta – link prowadzi do fałszywej strony.

Wiadomość o niedostarczonej paczce z prośbą o dopłatę.

Najczęściej podrabiane serwisy:

Allegro

Facebook

OLX

NAUKA DLA SPOŁECZEŃSTWA

Ministerstwo Nauki i Szkolnictwa Wyższego

cybergia.pl

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

SMISHING

Smishing, czyli oszustwa przez SMS.

Dlaczego SMS-y są tak skuteczne?

98% SMS-ów jest otwieranych (dla porównania: e-maile – tylko 20%).

60% osób czyta SMS-a w kilka minut od otrzymania.

80% korzysta z kuponów i zniżek przez telefon.

Na SMS-a odpowiadamy 4 razy częściej niż na e-mail.

NAUKA DLA SPOŁECZEŃSTWA

Ministerstwo Nauki i Szkolnictwa Wyższego

cybergia.pl

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

VISHING

Vishing to oszustwo, w którym przestępcy dzwonią do Ciebie, udając pracownika banku, urzędu albo kogoś z rodziny, żeby wyłudzić dane lub pieniądze. Coraz częściej używają do tego automatycznych infolinii lub sztucznej inteligencji, która potrafi naśladować czyjś głos.

Złodzieje wykorzystują np. nagranie głosu z TikToka i dzwonią z numeru, który wygląda jak numer bliskiej osoby (tzw. spoofing). Starsza osoba odbiera telefon i słyszy „wnuczka", który mówi, że miał wypadek i potrącił kobietę w ciąży. Prosi, żeby rozmawiać z jego „adwokatem".
Chwilę później dzwoni oszust-prawnik, mówi szybko, oficjalnie i twierdzi, że można uniknąć aresztu, jeśli natychmiast zostanie wpłacona „kaucja" – np. 30 tysięcy złotych. Podaje dane do przelewu albo wysyła kuriera po gotówkę.
Dlaczego to działa? Bo ofiara jest w szoku, działa pod wpływem emocji i chce pomóc. Oszuści specjalnie wywołują presję i nie dają czasu na myślenie. Dzięki AI potrafią reagować na to, co mówisz, więc trudno zorientować się, że to oszustwo.

NAUKA DLA SPOŁECZEŃSTWA
Ministerstwo Nauki i Szkolnictwa Wyższego
cybergia.pl
Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

NAJCZĘSTSZE TECHNIKI SOCJOTECHNICZNE

w 2024 roku w Polsce

Oszustwo na dziecko przez WhatsApp:
Oszust udaje dziecko, które rzekomo dzwoni z telefonu kolegi lub koleżanki i prosi rodziców lub dziadków o pilny przelew pieniędzy, np. na „nowy telefon".

Fałszywy policjant:
Przestępca podaje się za funkcjonariusza i straszy zarzutami karnymi. Oferuje „załatwienie sprawy" bez sądu – oczywiście za opłatą.

Podszycie się pod kancelarię prawną:
Mail informuje o rzekomym naruszeniu praw autorskich i zawiera „dokumenty", które w rzeczywistości są zainfekowanymi plikami.

Fałszywe mandaty za wycieraczką:
Na samochodach pojawiają się kartki przypominające wezwania do zapłaty. Po zeskanowaniu kodu QR ofiara trafia na fałszywą stronę płatności. Kody QR są wykorzystywane, ponieważ pozwalają ominąć filtry antyphishingowe.

Jak się chronić?

Nie skanuj kodów QR z nieznanych źródeł

Używaj aplikacji do skanowania, które pokazują link przed otwarciem

Nie loguj się ani nie podawaj danych na stronach otwieranych przez QR, jeśli nie masz 100% pewności

Zwracaj uwagę na domeny po zeskanowaniu kodu – fałszywe linki często mają drobne literówki lub dziwne końcówki.

NAUKA DLA SPOŁECZEŃSTWA
Ministerstwo Nauki i Szkolnictwa Wyższego
cybergia.pl
Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

SPEAR PHISHING

gdy oszust celuje dokładnie w Ciebie

Spear phishing to bardzo dobrze przygotowany atak, który jest skierowany do konkretnej osoby lub organizacji. Oszuści wykorzystują dane z internetu, np. Twoje posty, zdjęcia, zainteresowania, żeby stworzyć wiadomość, która wygląda wiarygodnie. Często podszywają się pod nauczyciela, znajomego albo instytucję, z którą masz kontakt.

Sztuczna inteligencja pomaga im dobrać styl pisania, moment wysyłki (np. poniedziałek rano) i treść, która wywoła emocje: strach, presję czasu albo współczucie. Przykład? „Twoje konto zostanie zablokowane" albo „Znajomy potrzebuje pilnej pomocy".

Takie wiadomości są coraz trudniejsze do rozpoznania, bo każda jest inna i dopasowana do konkretnej osoby. Jeśli odpowiesz lub klikniesz w link, możesz stracić dane, pieniądze albo dać dostęp do swojego konta. Dlatego ważne jest, żeby czytać wiadomości uważnie i nie działać pod presją.

NAUKA DLA SPOŁECZEŃSTWA
Ministerstwo Nauki i Szkolnictwa Wyższego
cybergia.pl
Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

PO CZYM POZNAĆ ATAK SOCJOTECHNICZNY?

Zwróć uwagę na te sygnały:

1. **PRESJA CZASU** – Ktoś chce, żebyś natychmiast coś zrobił? Straszy konsekwencjami lub kusi „super okazją”? To trik, żebyś działał bez zastanowienia.
2. **PODSZYWANIE SIĘ POD WAŻNE OSOBY** – Oszust może udawać nauczyciela, szefa, pracownika banku albo działu IT, żebyś mu zaufał i zrobił, o co prosi.
3. **ZBYT PIĘKNE, BY BYŁO PRAWDZIWE** – Obietnice wygranych, prezentów, rabatów czy łatwej kasy? Najpewniej ktoś próbuje Cię oszukać.
4. **SILNE EMOCJE** – Smutne historie, groźby albo prośby o pomoc mają sprawić, że przestaniesz myśleć logicznie i zrobisz to, czego chce oszust.
5. **DZIWNA FORMA WIADOMOŚCI** – E-mail z nietypowego adresu, błędy językowe, dziwne załączniki albo prośby przez Messenger?
6. **BŁĘDY JĘZYKOWE** – Gdy wiadomość wygląda, jakby pisał ją automat albo ktoś, kto słabo zna język – prawdopodobnie coś jest nie tak.
7. **PROŚBA O DANE** – Pamiętaj: bank, urząd ani szkoła nie proszą o hasła, kody czy PESEL przez SMS czy e-mail.

NAUKA DLA SPOŁECZEŃSTWA
Ministerstwo Nauki i Szkolnictwa Wyższego
cybergia.pl
Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II”

JAK DZIAŁA SOCJOTECHNIKA?

Oszust nie łamie hasła, ale sprawia, że sam je podasz.

Socjotechnika to nie atak na komputer, tylko na człowieka. Oszust wykorzystuje emocje i przyzwyczajenia, żebyś sam zrobił to, czego on chce: kliknął, odpisał, podał dane.

NA CO LICZY PRZESTĘPCA?

STRACH I POŚPIECH

„Twoje konto zostanie zablokowane!" brzmi groźnie? Właśnie o to chodzi. Masz się przestraszyć i działać bez zastanowienia.

ZAUFANIE

Wiadomość wygląda, jakby była od banku, policji albo znajomego. Oszust chce, żebyś nawet nie sprawdził, czy to prawda.

EMPATIA

Wiadomość wygląda, jakby była od banku, policji albo znajomego. Oszust chce, żebyś nawet nie sprawdził, czy to prawda.

AUTORYTET I PRESJA

„Twoje konto zostanie zablokowane!" brzmi groźnie? Właśnie o to chodzi. Masz się przestraszyć i działać bez zastanowienia.

PRZYZWYCZAJENIE

Wiadomość wygląda, jakby była od banku, policji albo znajomego. Oszust chce, żebyś nawet nie sprawdził, czy to prawda.

ROZPROSZENIE

Wiadomość wygląda, jakby była od banku, policji albo znajomego. Oszust chce, żebyś nawet nie sprawdził, czy to prawda.

NAUKA DLA SPOŁECZEŃSTWA

Ministerstwo Nauki i Szkolnictwa Wyższego

cybergia.pl

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

JAK DZIAŁAJĄ NOWOCZESNE TECHNIKI MANIPULACJI Z UŻYCIEM AI

Nowe technologie, takie jak sztuczna inteligencja (AI), sprawiają, że oszuści działają szybciej, sprytniej i trudniej ich wykryć:

1. **DEEPFAKE I SZTUCZNY GŁOS** – Dzięki AI można podrobić głos lub twarz konkretnej osoby, np. wnuczka, szefa czy nauczyciela. Oszust może zadzwonić lub nagrać filmik, który wygląda bardzo wiarygodnie.

2. **INTELIGENTNE ROZMOWY** – Zamiast sztywnych wiadomości, oszuści używają chatbotów, które prowadzą naturalną rozmowę przez maila, czat czy telefon. Trudno się zorientować, że są fałszywe.

3. **CELOWANY PHISHING** – AI potrafi zebrać dane z internetu (np. z mediów społecznościowych) i stworzyć bardzo osobistą wiadomość, dopasowaną do Twoich zainteresowań, pracy czy znajomych.

4. **ATAKI Z RÓŻNYCH STRON** – Wiadomość na Facebooku, potem mail, SMS i telefon – wszystko wygląda spójnie. To tzw. atak wielokanałowy. AI pomaga to zaplanować i przeprowadzić.

5. **PROFIL PSYCHOLOGICZNY** – AI analizuje Twój sposób pisania, godziny aktywności czy znajomych, żeby wybrać najlepszy moment i styl ataku, np. poniedziałek rano, kiedy jesteś najbardziej zajęty.

6. **AUTOMATYZACJA NA DUŻĄ SKALĘ** – Dawniej przestępcy musieli wszystko robić ręcznie. Teraz AI robi to za nich – szybko, masowo i skutecznie.

7. **OMIJANIE ZABEZPIECZEŃ** – AI tworzy wiadomości, które wyglądają jak normalne i nie są blokowane przez filtry antyspamowe. Tworzy też fałszywe kody QR i strony, które omijają ochronę.

NAUKA DLA SPOŁECZEŃSTWA
Ministerstwo Nauki i Szkolnictwa Wyższego
cybergia.pl
Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II”

JAK SIĘ CHRONIĆ PRZED ATAKAMI SOCJOTECHNICZNYMI?

UWAŻNIE SPRAWDZAJ ADRESY E-MAIL I STRONY INTERNETOWE

Zwróć uwagę na literówki i nietypowe domeny. Wiadomość może wyglądać, jakby pochodziła z banku lub znajomej osoby (np. imię i nazwisko współpracownika), ale być wysłana z podobnego adresu, ale z błędną końcówką.

NIE UFAJ AUTOMATYCZNIE NUMEROM TELEFONU

Nawet jeśli wygląda znajomo, może być sfałszowany. Cyberprzestępcy potrafią tak przekierować połączenie, że na ekranie wyświetla się numer bliskiej osoby.

NIE KLIKAJ W LINKI Z NIEZNANYCH ŹRÓDEŁ

Jeśli wiadomość wydaje się podejrzana, lepiej ją zignorować niż ryzykować. W razie wątpliwości skontaktuj się bezpośrednio z nadawcą i zapytaj, czy faktycznie wysłał tę wiadomość i czy sprawa jest rzeczywiście pilna.

WŁĄCZ UWIERZYTELNIANIE WIELOSKŁADNIKOWE

Najlepiej, jeśli kod potwierdzający przychodzi na inne urządzenie (np. telefon).

KORZYSTAJ Z AKTUALNEGO OPROGRAMOWANIA ANTYWIRUSOWEGO I ZAPORY SIECIOWEJ (FIREWALLA)

Regularne aktualizacje pomagają chronić system przed nowymi zagrożeniami.

NAUKA DLA SPOŁECZEŃSTWA

Ministerstwo Nauki i Szkolnictwa Wyższego

cybergia.pl

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

ZGŁASZAJ PODEJRZANE WIADOMOŚCI I ATAKI

Jeśli nie zgłaszamy ataków, nie dajemy systemom bezpieczeństwa szansy na naukę i ochronę innych. W przypadku phishingu e-mailowego kliknij „Zgłoś jako phishing" lub „Zgłoś jako spam" w skrzynce pocztowej.

Niestety, **tylko 1 na 20 starszych osób** zgłasza ataki często z powodu wstydu lub pogarszającej się pamięci. Dlatego tak ważna jest edukacja i wsparcie bliskich.

Jak zgłosić incydent cyberbezpieczeństwa?

Jeżeli otrzymałeś podejrzaną wiadomość smsem, przekaż ją lub udostępnij na numer 8080. Ważne jest aby przekazać całą wiadomość w oryginalnej formie.
Nie wycinaj odnośnika ani treści. Z jednego numeru możesz zgłosić maksymalnie 3 wiadomości w ciągu 4 godzin.
Oprócz policji można skontaktować się z CERT Polska poprzez https://incydent.cert.pl/ lub w aplikacji mObywatel – usługa Bezpiecznie w sieci.

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"

CO ROBIĆ JEŚLI...

W przypadku podejrzenia, że padło się ofiarą **PHISHINGU** (uruchomiło się podejrzany załącznik lub odwiedziło fałszywą stronę), należy natychmiast **zmienić hasła** do swoich kont. W sytuacji podania danych finansowych należy **skontaktować się ze swoim bankiem.**
Konieczne jest również **zgłoszenie incydentu** – w Polsce istnieje kilka instytucji zajmujących się oszustwami internetowymi. Oprócz policji można skontaktować się z CERT Polska (poprzez https://incydent.cert.pl/ lub w aplikacji mObywatel – usługa Bezpiecznie w sieci – podejrzane wiadomości SMS z linkami można zgłosić na nr 8080).
Należy również **przeskanować urządzenia programem antywirusowym,** ponieważ kliknięcie podejrzanego linka mogło spowodować pobranie złośliwego oprogramowania.

Zadbaj o prywatność w **mediach społecznościowych.** AI bardzo łatwo przeszukuje publiczne profile, pobierając z nich dane (np. miejsce zamieszkania, imiona członków rodziny, wydarzenia, lokalizacje). Te informacje są potem wykorzystywane do personalizacji ataków. Ustaw swoje profile jako prywatne, ogranicz dostęp do informacji osobistych i unikaj publikowania w czasie rzeczywistym, np. informacji o wyjazdach.

W przypadku **podejrzanego telefonu** – rozłącz się i oddzwoń.

Używaj osobnych adresów e-mail do różnych celów - Załóż oddzielne konto e-mail do spraw finansowych (bankowość, inwestycje). Jeśli otrzymasz wiadomość z „ofertą z banku" na ogólny adres (np. do zakupów), od razu będziesz wiedzieć, że to oszustwo.

PLUS ADDRESSING
– prosty sposób na ochronę e-maila

Dodając „+" i dowolne słowo do swojego adresu e-mail (np. jan.kowalski+netflix@gmail.com), możesz:

- Rozpoznać źródło wiadomości – wiesz, która usługa ujawniła Twój adres.
- Zarządzać pocztą – ustawisz filtry, np. +bank → folder „Finanse".
- Chronić się przed phishingiem – jeśli e-mail ma inne „+" niż podane przy rejestracji, coś jest nie tak.
- Używać jednego konta do wielu usług, zachowując porządek.

Działa m.in. w Gmailu i Outlook.com. Niektóre strony nie akceptują znaku „+", ale coraz więcej to umożliwia.

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II"