Konspekt zajęć: Inżynieria społeczna i socjotechniki - strategie rozpoznawania zagrożeń i metody ochrony	
Grupa docelowa	uczniowie szkół ponadpodstawowych (klasy 1-4)
Cel główny	uczeń zna i rozumie techniki socjotechniczne stosowane przez cyberprzestępców i potrafi reagować na próby wyłudzania danych w środowisku cyfrowym
Cele szczegółowe	– uczeń potrafi rozpoznać techniki socjotechniczne stosowane przez cyberprzestępców; – uczeń potrafi wyjaśnić, jakie mechanizmy psychologiczne są wykorzystywane przez oszustów; – uczeń potrafi bronić się przed próbami wyłudzania danych.
Metody i formy pracy	– metoda problemowa (analiza przypadków, praca w grupach); – dyskusja moderowana; – burza mózgów; – scenki sytuacyjne.
Czas trwania zajęć	– 90 minut
Materiały, pomoce dydaktyczne	– projektor i komputer do prezentacji materiałów multimedialnych; – karty pracy dla ucznia
Przebieg zajęć	1. Wprowadzenie 2. Omówienie pojęcia socjotechniki i inżynierii społecznej. 3. Przegląd typów ataków 4. Analiza przypadków – praca w grupach. 5. Zasady ochrony przed atakiem – quiz oraz dyskusja moderowana.

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

Karta Pracy

Inżynieria społeczna i socjotechniki –

strategie rozpoznawania zagrożeń i metody ochrony

Socjotechnika to manipulacja psychologiczna, która skłania ofiarę do podjęcia konkretnych działań, często sprzecznych z jej interesem, np. kliknięcia w link, podania danych czy otwarcia pliku. Cyberprzestępcy wykorzystują ją, by ominąć zabezpieczenia techniczne i zdobyć dostęp do systemów lub poufnych informacji. Podszywają się pod zaufane osoby czy instytucje.

Ataki phishingowe to najczęstsza forma oszustwa w sieci, w której przestępcy podszywają się pod zaufane instytucje w celu wyłudzenia poufnych danych, takich jak loginy, hasła oraz dane finansowe, nakłonienia ofiary do kliknięcia w złośliwy link lub pobrania niebezpiecznego pliku. Oszustwa przez SMS-y to smishing.
Mechanizm działania
Otrzymujesz fałszywy e-mail lub SMS z linkiem do podrobionej strony logowania. Oszuści zachęcają Cię do kliknięcia i wpisania swoich danych, które trafiają w ich ręce.

Ćwiczenie 1: Przeczytaj uważnie poniższe przykłady wiadomości. Odpowiedz na trzy pytania:

a) Co w tej wiadomości ma skłonić Cię do kliknięcia?

b) Dlaczego to może być oszustwo?

c) Jak najlepiej zareagować?

1. SMS: „Twoje konto zostanie zablokowane, jeśli natychmiast nie uzupełnisz danych karty kredytowej. Kliknij tutaj: www.serwis-konto-24.info”
2. Mail:

   Szanowny Użytkowniku,
   W związku z podejrzaną aktywnością na Twoim koncie bankowym, dostęp został tymczasowo ograniczony.
   Aby przywrócić pełny dostęp, prosimy o pilne potwierdzenie danych:
   Kliknij tutaj, aby się zalogować i potwierdzić dane: www.link.co.biz
   Jeśli nie potwierdzisz danych w ciągu 24 godzin, konto zostanie ZABLOKOWANE.
   Dziękujemy za zaufanie,
   Zespół Bezpieczeństwa Banku
3. Powiadomienie: „Hej! Odblokuj specjalne funkcje aplikacji! Kliknij link i wpisz swój login – działa tylko przez 10 minut!”
4. Powiadomienie: „Zostałeś oznaczony na zdjęciu! Kliknij, by zobaczyć: www.dostawa.dzisiaj.pl”
5. SMS: „Twoja przesyłka nie mogła zostać doręczona. Kliknij, by opłacić 2,99 zł i ustawić nowy termin dostawy: www.link.net”

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

Ćwiczenie 2: Przeczytaj poniższe opisy sytuacji. Następnie dopasuj do każdego z nich odpowiednią nazwę rodzaju oszustwa z listy.

Wybierz spośród:

- spear phishing
- smishing
- quishing
- vishing
- pretexting
- baiting
- caller ID spoofing
- tailgating

1. Otrzymujesz SMS z informacją o niedostarczonej przesyłce i linkiem do uiszczenia drobnej opłaty.
   Typ oszustwa: ……..
2. Dzwoni ktoś, kto brzmi jak Twój wnuczek i błaga o pomoc, mówiąc, że miał wypadek. Potem kontaktuje się „prawnik" z prośbą o natychmiastowy przelew.
   Typ oszustwa: ……..
3. Dzwoni do Ciebie ktoś z numeru wyglądającego jak telefon Twojego wnuczka, kolegi lub banku.
   Typ oszustwa: ……..
4. Znajdujesz pendrive na uczelni. Wkładasz go do komputera, a on uruchamia złośliwe oprogramowanie.
   Typ oszustwa: ……..
5. Przypadkowa osoba wchodzi z Tobą do budynku firmy, prosząc o przytrzymanie drzwi.
   Typ oszustwa: ……..
6. Ktoś pisze do Ciebie, podając się za rekrutera z firmy, w której chcesz pracować. Pyta o szczegóły Twojej tożsamości – datę urodzenia, nazwisko panieńskie matki.
   Typ oszustwa: ……..
7. Otrzymujesz wiadomość na Messengerze od znajomego, który prosi Cię o podanie kodu BLIK – twierdzi, że jest w sklepie i zapomniał portfela. Jego profil wygląda autentycznie.
   Typ oszustwa: ……..
8. Znajdujesz za wycieraczką samochodu kartkę wyglądającą jak mandat lub wezwanie do zapłaty. Zawiera kod QR prowadzący do strony płatności.
   Typ oszustwa: ……..

Ćwiczenie 3: Uzupełnij brakujące dane liczbowe w poniższych zdaniach na podstawie faktów o zagrożeniach online:

. com	.net	Allegro	Facebook	OLX
1	5	10%	20%	30
60%	62%	80%	98%	600 000
seniorzy		zakupów		kontaktów
1,5 miliona		100 milionów		połowę

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

1. W 2024 roku phishing stanowił ponad ___ wszystkich incydentów obsłużonych przez CERT Polska – zgłoszono _____ przypadków, o ___% więcej niż rok wcześniej.
2. Zablokowano prawie _____ złośliwych SMS-ów (wzrost o ___%).
3. Nadal tylko ___ na ___ incydentów jest zgłaszanych.
4. Google codziennie blokuje około _____ wiadomości phishingowych.
5. Ponad połowa z nich pochodzi z domen _____ oraz _____
6. Najczęściej podrabiane marki w Polsce to: _____, _____ oraz _____.
7. Prawie ___% osób kliknęło w phishingowy link.
8. Najczęściej atakowani są użytkownicy poniżej ___ roku życia – spędzają więcej czasu online.
9. Najwięcej pieniędzy tracą _____ – są mniej odporni na manipulacje.
10. W czasie pandemii wzrosła liczba ataków, ponieważ seniorzy zaczęli korzystać z internetu do _____ i _____.

Smishing – oszustwa przez SMS:

11. ___% SMS-ów jest otwieranych (dla porównania: e-maile – tylko ___%).
12. ___% osób czyta SMS-a w ciągu kilku minut od otrzymania.
13. ___% użytkowników korzysta ze zniżek i kuponów na telefonach.
14. Na SMS-a odpowiadamy ponad ___ razy częściej niż na e-maila.

Główne cechy ataków socjotechnicznych
1. Atakujący wywołuje poczucie pilności, by skłonić ofiarę do działania bez zastanowienia. Typowe sygnały to: żądania natychmiastowej reakcji, groźby konsekwencji (np. zablokowania konta) lub obietnice wyjątkowych korzyści. 2. Przestępcy często udają przełożonych, pracowników działu IT lub inne zaufane osoby, by zwiększyć szansę na posłuszeństwo i wykonanie polecenia. 3. Obietnice wysokiej wygranej, szybkiego zarobku czy ekskluzywnych okazji mogą być próbą wyłudzenia danych lub pieniędzy. 4. Historie wywołujące silne emocje, takie jak litość, współczucie czy strach, służą do osłabienia czujności i skłonienia do pochopnych decyzji. 5. Nietypowe adresy e-mail, błędy językowe, niecodzienne dokumenty czy prośby przesyłane przez prywatne kanały (np. komunikatory lub social media) powinny wzbudzić podejrzenia. 6. Błędy językowe, niepoprawna gramatyka i składnia mogą świadczyć o tym, że wiadomość pochodzi z zagranicy lub została wygenerowana automatycznie. 7. Nietypowe prośby o dane. Instytucje nie proszą o poufne dane (np. numery kont, hasła, PESEL) przez e-mail, SMS czy media społecznościowe.

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

Ćwiczenie 4: Na podstawie opisanych powyżej cech ataku socjotechnicznego zaplanuj realistyczny scenariusz ataku. Wybierz jedną z przykładowych postaci poniżej. Stwórz treść fałszywej wiadomości (e-mail, SMS, wiadomość głosowa lub media społecznościowe). Wskaż, które techniki socjotechniczne zostały użyte. Napisz, co powinno wzbudzić podejrzenia ofiary. Podaj właściwą reakcję.

1. Marek, 17 lat – uczeń technikum informatycznego, aktywny gracz online, często korzysta z Discorda i TikToka.
2. Pani Teresa, 68 lat – emerytka, która zaczęła korzystać z internetu w pandemii, kupuje online i używa WhatsAppa do kontaktu z rodziną.
3. Kasia, 22 lata – studentka, szuka pracy, aktywna na Instagramie i portalach z ogłoszeniami.
4. Pan Andrzej, 45 lat – kierownik w firmie logistycznej, często podróżuje służbowo, korzysta ze służbowego maila i telefonu.
5. Natalia, 35 lat – samotna mama, często szuka promocji w internecie, korzysta z OLX i Allegro.
6. Adam, 60 lat – właściciel małej firmy, nie zna się na technologii, współpracuje z wieloma kontrahentami.
7. Ania, 13 lat – uczennica, używa Messengera, ogląda YouTube Shorts, marzy o nowym smartfonie.

Ćwiczenie 5: W jaki sposób sztuczna inteligencja, np. ChatGPT, narzędzia do zmiany głosu lub projektowania obrazów, może być używana przez cyberprzestępców do oszukiwania ludzi? Podajcie konkretne przykłady i wyjaśnijcie, dlaczego takie ataki są trudne do rozpoznania.

Ćwiczenie 6: Jak się chronić przed atakami socjotechnicznymi? Przeczytaj zdania i uzupełnij brakujące słowa. Wybierz spośród podanych opcji.

1. Zawsze dokładnie sprawdzaj adresy _____ i strony internetowe.

A. kontaktowe
C. IP
B. e-mail
D. prywatne

2. Regularne _____ oprogramowania pomagają chronić system przed nowymi zagrożeniami.

A. usuwanie
C. instalacje gier
B. aktualizacje
D. restarty

3. Cyberprzestępcy mogą fałszować numer telefonu, dlatego nie ufaj numerom wyświetlanym na ekranie – to tzw. _____.

A. firewall
C. caller ID spoofing
B. spoofing e-mail
D. phishing głosowy

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

4. _____ to sposób logowania, w którym oprócz hasła potrzebny jest dodatkowy kod np. SMS.

A. Firewall
C. Biometria
B. Uwierzytelnianie dwuskładnikowe
D. Antyspam

5. Kiedy otrzymałeś e-mail, który podejrzewasz, że stanowi próbę wyłudzenia twoich danych, kliknij „_____”.

A. Zgłoś jako phishing
C. Przenieś do folderu „Rodzina”
B. Odpowiedz
D. Potwierdź dane

6. Jeśli otrzymasz podejrzanego SMS-a, prześlij go na numer _____.

A. 112
C. 997
B. 8080
D. 2024

7. Jeżeli klikniesz podejrzany link, natychmiast zmień _____.

A. adres e-mail
C. przeglądarkę
B. hasła
D. komputer

8. Jeśli masz podejrzenia, że rozmawiasz z oszustem przez telefon, powinieneś się _____.

A. rozłączyć
C. kliknąć w link
B. zgodzić na rozmowę
D. poprosić o kontakt mailowy

9. AI może wykorzystywać dane z twoich profili w mediach społecznościowych, dlatego ustaw je jako _____.

A. prywatne
C. reklamowe
B. służbowe
D. firmowe

10. W przypadku vishingu należy ustalić w rodzinie specjalne _____, które pomoże potwierdzić tożsamość rozmówcy.

A. zdjęcie
C. numer konta
B. słowo-klucz
D. aplikację

11. Oprócz policji, incydent można zgłosić do _____ lub przez aplikację mObywatel.

A. banku
C. urzędu gminy
B. CERT Polska
D. Ministerstwa Zdrowia

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

12. AI może przeszukiwać twoje publiczne profile i wykorzystać dane do _____ ataków.

A. blokowania
C. personalizacji
B. testowania
D. reklamowania

13. Konto e-mail do spraw finansowych warto trzymać _____ od konta do zakupów.

A. osobno
C. w chmurze
B. razem
D. anonimowo

14. Aby lepiej zarządzać wiadomościami, możesz korzystać z funkcji _____ addressingu, np. jan.kowalski+olx@gmail.com.

A. plus
C. spam
B. safe
D. proxy

Ciekawostka:

Plus addressing to sposób, by lepiej chronić swój adres e-mail i łatwiej zarządzać pocztą. Wystarczy dodać znak „+" i słowo po swoim adresie (np. jan.kowalski+olx@gmail.com). Wiadomość i tak trafi na twoją skrzynkę, ale:

- Wiesz, kto przekazał twój adres – np. jeśli potem dostajesz spam na „+olx", wiesz, która firma mogła ujawnić adres.
- Łatwiej sortujesz pocztę – możesz ustawić, że maile z „+olx" trafiają do folderu „Zakupy".
- Możesz wykryć oszustwo – jeśli ktoś używa innego „+", niż podałeś przy rejestracji, wiadomość jest podejrzana.

Działa to np. w Gmailu i Outlooku, ale jeszcze nie każda strona jeszcze to akceptuje.

Pytania do dalszej dyskusji:

1. Dlaczego mimo ostrzeżeń i edukacji tak wiele osób nadal klika w podejrzane linki?
2. Kto twoim zdaniem powinien być odpowiedzialny za ochronę przed cyberoszustwami: użytkownik, państwo czy firmy technologiczne?
3. Czy sztuczna inteligencja powinna być wykorzystywana także przez instytucje państwowe do wykrywania oszustw? Jakie mogą być tego plusy i minusy?
4. Czy można zbudować kampanię społeczną, która naprawdę zmieniłaby zachowania ludzi w internecie? Jak powinna wyglądać, by dotarła np. do seniorów?
5. Jakich danych nigdy nie powinno się udostępniać online, nawet jeśli wiadomość wydaje się pochodzić od znajomego lub instytucji?
6. Czy twoim zdaniem powinno się karać osoby, które nieświadomie przekazały dane przestępcom, ale spowodowały przez to szkody (np. w firmie)?

Dodatkowe zasoby edukacyjne:

Quiz online: https://phishingquiz.withgoogle.com/

(w języku angielskim): https://app.socialmediatestdrive.org/intro/phishing

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