MFO 2.0
Demokracja w erze cyfrowej

PODRĘCZNIK 03

Bezpieczeństwo w sieci

Praktyczny przewodnik ochrony cyfrowej tożsamości

Ten podręcznik zamienia wiedzę o cyberzagrożeniach w konkretne nawyki ochrony kont, danych i cyfrowej reputacji.

Dofinansowane przez Unię Europejską

SŁOWEM W TWARZ

Projekt w ramach Erasmus+ Młodzież - Działania partycypacyjne młodzieży (KA154-YOU)

Podręcznik 03

Bezpieczeństwo w sieci

Praktyczny przewodnik ochrony cyfrowej tożsamości

Ten podręcznik zamienia wiedzę o cyberzagrożeniach w konkretne nawyki ochrony kont, danych i cyfrowej reputacji.

Ta strona jest tekstowym odpowiednikiem okładki: zawiera najważniejsze informacje, które na pierwszej stronie są przedstawione graficznie.

Spis treści

Mapa podręcznika

Poniższa mapa pokazuje układ materiału: od krótkiego wejścia w temat, przez część główną, aż po ćwiczenia i plan działania.

Wskazówka: w wersji cyfrowej korzystaj także z panelu nawigacji po nagłówkach w edytorze tekstu.

Jak korzystać z tego podręcznika

Ten podręcznik zamienia wiedzę o cyberzagrożeniach w konkretne nawyki ochrony kont, danych i cyfrowej reputacji.

Proponowany rytm pracy

Najlepiej czytać ten materiał aktywnie: najpierw zrozum pojęcia, potem przećwicz narzędzie na przykładzie, a na końcu zaplanuj własne działanie.

- Czytaj z ołówkiem: podkreślaj decyzje, narzędzia i przykłady.
- Po każdej większej części zatrzymaj się przy pytaniu kontrolnym.
- Nie kończ na wiedzy: wykonaj kartę pracy i mini-projekt.

Cele uczenia się

- rozpoznawać phishing, spoofing i manipulację społeczną
- tworzyć bezpieczniejsze hasła i korzystać z menedżera haseł
- włączać uwierzytelnianie dwuskładnikowe
- sprawdzać prywatność kont i aplikacji
- reagować po kliknięciu podejrzanego linku lub utracie dostępu do konta

Słowniczek roboczy

Pojęcie	Jak rozumieć je w praktyce
Phishing	podszywanie się pod zaufaną osobę lub instytucję w celu wyłudzenia danych
Spoofing	fałszowanie numeru telefonu, nadawcy e-maila albo identyfikatora
2FA	drugi składnik logowania, który utrudnia przejęcie konta
Menedżer haseł	narzędzie do tworzenia i przechowywania silnych haseł
Ślad cyfrowy	informacje, które zostawiasz po sobie w sieci

Wstęp

Przeciętna osoba w wieku 15–25 lat posiada od dwudziestu do czterdziestu kont internetowych: media społecznościowe, poczta, bankowość, platformy streamingowe, gry, szkolne portale. Każde z tych kont to potencjalny punkt wejścia dla kogoś, kto chce ukraść twoje dane, pieniądze lub tożsamość.

Raport Warszawskiego Instytutu Bankowości z 2025 roku pokazuje paradoks: 88% Polaków wskazuje phishing jako największe cyberzagrożenie — ale tylko 29% dba o bezpieczeństwo w publicznym Wi-Fi. Wiemy, że problem istnieje, ale nie podejmujemy działań. Ten podręcznik zmienia to podejście: daje konkretne kroki, które możesz wykonać DZIŚ, żeby radykalnie poprawić swoje bezpieczeństwo cyfrowe.

1. Mapa zagrożeń — trzy główne schematy ataków

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „1. Mapa zagrożeń — trzy główne schematy ataków” zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.

- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Zanim nauczysz się obrony, musisz znać ataki. Trzy najczęstsze schematy, z którymi zetkniesz się jako młody użytkownik internetu:

Phishing to atak, w którym ktoś podszywa się pod zaufaną instytucję (bank, platforma streamingowa, urząd) i wysyła fałszywą wiadomość z linkiem, który prowadzi do strony wyłudzającej dane logowania, numer karty płatniczej lub inne poufne informacje. W 2025 roku policja w Rybniku ostrzegała mieszkańców przed masową kampanią phishingową „na Spotify" — fałszywe e-maile informujące o rzekomym anulowaniu subskrypcji, z linkiem do strony łudząco podobnej do prawdziwej. Według danych CERT Polska 98% zgłaszanych incydentów bezpieczeństwa to właśnie oszustwa tego typu.

Spoofing polega na podszywaniu się pod numer telefonu lub adres e-mail zaufanej instytucji. Dzwoni do ciebie „bank" — na wyświetlaczu widzisz prawdziwy numer infolinii — ale po drugiej stronie jest przestępca. Cel: wzbudzić zaufanie i wymusić działanie (np. podanie kodu BLIK, zainstalowanie aplikacji do „zdalnej weryfikacji"). Spoofing jest szczególnie skuteczny, bo ludzie ufają wyświetlanemu numerowi telefonu.

Social engineering (inżynieria społeczna) to manipulacja psychologiczna — ktoś zdobywa twoje zaufanie, a potem wykorzystuje je do wyłudzenia danych. Na Discordzie ktoś udaje administratora gry i prosi o dane logowania „w celu weryfikacji". Na Instagramie ktoś pisze „Twoje zdjęcie jest na tej stronie!" z linkiem do fałszywej witryny. Na Messengerze ktoś z przejętego konta znajomego prosi o kod BLIK. Wspólny mianownik: wykorzystanie relacji zaufania.

2. Anatomia ataku — jak wygląda phishing w praktyce

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „2. Anatomia ataku — jak wygląda phishing w praktyce" zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.
- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Phishing to nie prymitywna wiadomość pełna literówek (choć takie też istnieją). Nowoczesne ataki phishingowe są profesjonalne — używają prawdziwych logotypów, poprawnego języka i przekonującej grafiki. Oto cechy, po których je rozpoznasz:

Fałszywy adres nadawcy. To najczęstszy sygnał. Adres wygląda „prawie" jak prawdziwy — np. no-reply@spotlfy-support.com (literówka: „spotlfy" zamiast „spotify"), support@allegr0.pl (zero zamiast litery „o"), info@mbank-security.net (dodatkowa domena). Zawsze sprawdzaj PEŁNY adres nadawcy, nie tylko wyświetlaną nazwę.

Fałszywy link. Najedź myszką na link (NIE klikaj!) i sprawdź, dokąd prowadzi. Na telefonie: przytrzymaj link palcem, żeby zobaczyć pełny adres. Jeśli link prowadzi do domeny innej niż oficjalna strona firmy — nie klikaj.

Presja czasu. „Twoje konto zostanie zablokowane w 24 godziny!", „Ostatnia szansa na odbiór nagrody!", „Natychmiast potwierdź dane, inaczej stracimy twój dostęp". Presja czasu to celowa taktyka — ma cię zmusić do działania ZANIM pomyślisz.

Żądanie wrażliwych danych. Żaden bank, żadna platforma, żaden urząd NIE prosi o podanie pełnego hasła, kodu PIN, kodu BLIK czy numeru karty przez e-mail lub SMS. Nigdy. Jeśli ktoś tego żąda — to phishing.

Brak personalizacji. „Drogi Kliencie" zamiast twojego imienia. Legalne firmy, z którymi masz konto, zwracają się po imieniu, bo mają twoje dane. Ogólne zwroty to sygnał, że wiadomość wysłano masowo.

3. Hasła — fundament, który większość ignoruje

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „3. Hasła — fundament, który większość ignoruje" zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.
- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Hasła to pierwsza linia obrony — i jednocześnie najsłabsze ogniwo u większości użytkowników. Oto fakty:

Najpopularniejsze hasła w Polsce w 2025 roku to wciąż kombinacje typu „123456", „qwerty", „haslo", imiona dzieci i daty urodzin. Złamanie takiego hasła metodą brute force zajmuje dosłownie sekundy. Jednocześnie większość ludzi używa tego samego hasła (lub drobnych wariantów) na wielu kontach — co oznacza, że wyciek z jednego serwisu daje przestępcom dostęp do WSZYSTKICH twoich kont.

Menedżer haseł rozwiązuje oba problemy jednocześnie. Menedżer (np. Bitwarden — darmowy i open source) generuje losowe, silne hasła dla każdego konta i przechowuje je w zaszyfrowanym sejfie. Ty zapamiętujeszjedno hasło główne (master password) — reszta jest bezpiecznie przechowywana. Hasło główne powinno być długie (minimum 16 znaków) i unikalne — najlepiej zdanie, które łatwo zapamiętasz, ale trudno odgadnąć (np. „MojaKotkaJe3RybyNaSniadanie!").

Jak działa dobry menedżer haseł: generuje losowe hasła (np. „xK9$mP2vLq@7nR4w"), automatycznie wypełnia formularze logowania, synchronizuje się między urządzeniami, ostrzega o wyciekach i powtórzonych hasłach. Bitwarden jest open source — to znaczy, że każdy może sprawdzić jego kod źródłowy, co zwiększa zaufanie. Hasło główne nie jest przechowywane na serwerze — nawet twórcy Bitwarden nie mają do niego dostępu.

4. Weryfikacja dwuetapowa (2FA) — druga kłódka

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „4. Weryfikacja dwuetapowa (2FA) — druga kłódka" zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.
- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Nawet najsilniejsze hasło może wyciec. Wycieki danych zdarzają się regularnie — miliony kont z Facebooka, LinkedIn, Spotify wyciekają co roku. Dlatego samo hasło to za mało.

Weryfikacja dwuetapowa (2FA) dodaje drugi poziom zabezpieczenia: po wpisaniu hasła musisz potwierdzić tożsamość INNYM sposobem — kodem z aplikacji, SMS-em lub kluczem fizycznym. Nawet jeśli ktoś pozna twoje hasło, bez dostępu do twojego telefonu nie wejdzie na konto.

Rodzaje 2FA (od najsłabszego do najmocniejszego):

Kody SMS — najprostsze, ale najmniej bezpieczne (ataki SIM swap, przechwycenie SMS). Lepsze niż nic, ale nie idealne.

Aplikacja uwierzytelniająca (Google Authenticator, Authy, wbudowana w Bitwarden) — generuje kody co 30 sekund, działa offline, nie jest podatna na ataki SIM swap. To rekomendowane rozwiązanie dla większości ludzi.

Klucz fizyczny (YubiKey) — urządzenie USB, które fizycznie podłączasz do komputera lub telefonu. Najsilniejsze zabezpieczenie, ale wymaga zakupu sprzętu.

Gdzie włączyć 2FA w pierwszej kolejności: Gmail / Outlook (poczta to klucz do wszystkiego — kto ma dostęp do poczty, może resetować hasła na innych kontach), konto bankowe, Instagram, Discord, TikTok.

5. Wycieki danych — sprawdź, czy dotyczy ciebie

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „5. Wycieki danych — sprawdź, czy dotyczy ciebie" zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.
- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Strona **haveibeenpwned.com** (stworzona przez australijskiego specjalistę ds. bezpieczeństwa Troy'a Hunta) pozwala w kilka sekund sprawdzić, czy twój adres e-mail pojawił się w znanych wyciekach danych. Wpisujesz swój e-mail — strona pokazuje, w ilu wyciekach się znalazł i jakie dane mogły być ujawnione (hasła, numery telefonów, adresy).

Co zrobić, jeśli twój e-mail jest w wycieku: zmień hasło na serwisie, którego wyciek dotyczy (natychmiast), włącz 2FA na tym serwisie, jeśli używałeś tego samego hasła na innych kontach — zmień je WSZĘDZIE (i zainstaluj menedżer haseł, żeby to się nie powtórzyło).

6. Prywatność — kontrola nad tym, kto co o tobie wie

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „6. Prywatność — kontrola nad tym, kto co o tobie wie" zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.
- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Bezpieczeństwo i prywatność to dwie różne rzeczy. Bezpieczeństwo to ochrona przed atakami. Prywatność to kontrola nad tym, jakie informacje o tobie są dostępne — i dla kogo.

Ustawienia prywatności w mediach społecznościowych to potężne narzędzie, z którego większość ludzi nigdy nie korzysta. Każda platforma pozwala kontrolować: kto widzi twoje posty, kto może cię znaleźć, kto może pisać wiadomości, kto widzi twoją aktywność, czy twoje konto jest publiczne czy prywatne.

Instagram: Ustawienia → Prywatność → Konto prywatne (wyłącz publiczność), Aktywność na koncie, Wspomnij (kto może cię oznaczać), Ograniczone konta.

TikTok: Ustawienia i prywatność → Prywatność → Konto prywatne, Kto może komentować, Kto widzi polubione, Stitch/Duet (kto może używać twoich filmów).

Discord: Ustawienia → Prywatność i bezpieczeństwo → Wiadomości bezpośrednie (od kogo), Filtr treści, Kto może dodawać do znajomych.

Ślad cyfrowy to wszystko, co zostawiasz w internecie: posty, komentarze, zdjęcia, polubienia, lokalizacje, wyszukiwania. Ten ślad jest praktycznie trwały — nawet usunięte treści mogą być zarchiwizowane. Pracodawcy, uczelnie, a nawet potencjalni partnerzy coraz częściej sprawdzają ślad cyfrowy. Zanim opublikujesz cokolwiek, zadaj pytanie: „Czy za pięć lat będę zadowolony, że to wisi w internecie?".

7. Przemoc cyfrowa — to nie jest „problem internetowy"

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „7. Przemoc cyfrowa — to nie jest „problem internetowy"" zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.
- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Przemoc cyfrowa obejmuje: cyberstalking, hejt, groźby, szantaż, revenge porn (rozpowszechnianie intymnych zdjęć/filmów bez zgody), deepfake'owe materiały o charakterze seksualnym, doxing (upublicznianie prywatnych danych).

To są przestępstwa ścigane na podstawie polskiego prawa, w szczególności art. 190a KK (stalking), art. 191a KK (nagrywanie wizerunku osoby w stanie intymnym), art. 212 KK (zniesławienie), art. 216 KK (znieważenie).

Co robić, jeśli jesteś ofiarą:

- NIE kasuj dowodów — rób screenshoty (z widoczną datą, godziną, nazwą profilu sprawcy).
- Zablokuj sprawcę na platformie.
- Zgłoś na platformę (report).
- Zgłoś na policję lub prokuraturę — masz do tego prawo.
- Zgłoś na **Dyżurnet.pl** (NASK) — dedykowany serwis do zgłaszania nielegalnych treści w internecie.
- Zadzwoń na **Telefon Zaufania: 116 111** — bezpłatna, anonimowa pomoc.

Przypadek z 2024 roku, w którym zdjęcia nastolatek z Bydgoszczy posłużyły do tworzenia deepfake'ów, pokazuje, jak realne i poważne jest to zagrożenie. Technologia pozwala generować sfabrykowane materiały intymne na podstawie zwykłych zdjęć z Instagrama — kolejny powód, by kontrolować ustawienia prywatności i ograniczać publiczny dostęp do swoich zdjęć.

8. Dark patterns — jak platformy kradną twój czas

Cel tej części

Przeczytaj tę sekcję tak, aby na końcu umieć wyjaśnić, co temat „8. Dark patterns — jak platformy kradną twój czas” zmienia w twoim sposobie działania online lub w grupie.

- Zaznacz jedną definicję lub zasadę, którą warto zapamiętać.
- Dopisz własny przykład z życia szkoły, miasta albo internetu.
- Zapisz jedno pytanie, które warto zadać przed podjęciem działania.

Dark patterns to celowo zaprojektowane mechanizmy interfejsów, które manipulują twoim zachowaniem — sprawiają, że robisz rzeczy, których nie planowałeś: spędzasz więcej czasu, klikasz więcej, udostępniasz więcej danych.

Nieskończony scroll — brak „końca" strony sprawia, że ciągle scrollujesz, bo nie ma naturalnego punktu zatrzymania. TikTok, Instagram, Twitter — wszystkie to stosują.

Powiadomienia push — każde powiadomienie to mikroprzerwa, która wyrywa cię z tego, co robisz, i ciągnie z powrotem do aplikacji. Większość powiadomień nie jest pilna — ale twój mózg reaguje na nie jak na pilną wiadomość.

Social proof — „X osób to właśnie ogląda", „Twój znajomy polubił ten post" — fałszywa presja społeczna, która sugeruje, że musisz uczestniczyć.

Auto-play — filmy odtwarzają się automatycznie, żebyś nie musiał podejmować decyzji o oglądaniu. Brak decyzji = brak oporu = więcej czasu na platformie.

Obrona: wyłącz powiadomienia push ze WSZYSTKICH aplikacji oprócz komunikatora i kalendarza. Ustaw limity czasu w ustawieniach telefonu (Screen Time / Digital Wellbeing). Wyłącz auto-play w ustawieniach platform.

9. Publiczne Wi-Fi i bezpieczeństwo mobilne

Publiczne sieci Wi-Fi (kawiarnie, galerie, dworce) to potencjalne zagrożenie. W nieszyfrowanej sieci osoba w tej samej sieci może przechwytywać dane, które wysyłasz — hasła, wiadomości, dane kart płatniczych. Tylko 29% Polaków dba o bezpieczeństwo w publicznym Wi-Fi.

Zasady korzystania z publicznego Wi-Fi: nie loguj się do bankowości. Nie podawaj danych karty. Używaj VPN (Virtual Private Network), który szyfruje twoje połączenie. Jeśli nie masz VPN — korzystaj z danych mobilnych do wrażliwych operacji.

Bezpieczeństwo telefonu: włącz blokadę ekranu (PIN, wzór, biometria). Aktualizuj system operacyjny i aplikacje (aktualizacje często łatają luki bezpieczeństwa). Nie instaluj aplikacji spoza oficjalnych sklepów (Google Play, App Store). Sprawdzaj uprawnienia aplikacji — czy latarka naprawdę potrzebuje dostępu do kontaktów?

10. Emergency Kit — co robić, gdy padniesz ofiarą

Jeśli twoje konto zostało przejęte, dane wyciekły lub padłeś ofiarą oszustwa — oto procedura awaryjna:

Krok 1: Zmień hasło — natychmiast, na zaatakowanym koncie i na KAŻDYM koncie, gdzie używałeś tego samego hasła.

Krok 2: Włącz 2FA — na zaatakowanym koncie, jeśli jeszcze nie masz.

Krok 3: Sprawdź aktywne sesje — kto jest zalogowany na twoje konto? Gmail: myaccount.google.com → Bezpieczeństwo → Twoje urządzenia. Instagram: Ustawienia → Bezpieczeństwo → Aktywność logowania. Wyloguj wszystkie nieznane urządzenia.

Krok 4: Zgłoś — incydent.cert.pl (CERT Polska) dla incydentów cyberbezpieczeństwa. Policja lub prokuratura dla przestępstw. Bank — jeśli dotyczy danych finansowych (zablokuj kartę).

Krok 5: Monitoruj — sprawdź haveibeenpwned.com, obserwuj wyciągi bankowe, zwracaj uwagę na podejrzane wiadomości.

Przydatne zasoby

- **Bitwarden** (bitwarden.com) — darmowy menedżer haseł, open source
- **haveibeenpwned.com** — sprawdzanie wycieków danych
- **incydent.cert.pl** — zgłaszanie incydentów cyberbezpieczeństwa (CERT Polska)
- **Dyżurnet.pl** — zgłaszanie nielegalnych treści w internecie
- **Telefon Zaufania: 116 111** — pomoc dla dzieci i młodzieży
- **Google Authenticator / Authy** — aplikacje do 2FA
- **niebezpiecznik.pl** — polski portal o bezpieczeństwie cyfrowym

Opracowanie przygotowane w ramach projektu MFO 2.0 — warsztaty kompetencji cyfrowych i obywatelskich dla młodzieży subregionu rybnickiego.

Pytanie po lekturze części głównej

Wybierz jeden fragment, który można od razu zamienić w działanie. Co zrobisz inaczej po tej lekcji?

- Który element wiadomości najbardziej próbuje wymusić szybkie działanie?
- Jakie konto w twoim życiu ma największe konsekwencje po przejęciu?
- Co powinno się stać w pierwszych 15 minutach po podejrzeniu włamania?

Część ćwiczeniowa

Scenariusz pracy 90 minut

Czas	Etap	Co się dzieje
0-10 min	Start i diagnoza	Krótka rozmowa: co uczestnicy już wiedzą, czego się obawiają i gdzie spotykają temat w praktyce.
10-30 min	Pojęcia i przykłady	Praca z częścią główną podręcznika: definicje, pierwszy przykład, wspólne doprecyzowanie pojęć.
30-55 min	Analiza przypadku	Małe grupy wybierają przykład i sprawdzają go przez pytania z checklisty.
55-75 min	Projekt działania	Uczestnicy tworzą mini-rozwiązanie: komunikat, plan reakcji, kartę weryfikacji albo szkic kampanii.
75-90 min	Podsumowanie	Każda grupa pokazuje jeden wniosek, jedno ryzyko i jeden następny krok po zajęciach.

Ćwiczenie prowadzone

Wykonaj je indywidualnie albo w małej grupie. Celem nie jest perfekcyjna odpowiedź, tylko przejście przez cały proces myślenia.

- Wypisz pięć najważniejszych kont, z których korzystasz.
- Oceń dla każdego: hasło unikalne, 2FA, aktualny e-mail odzyskiwania.
- Wybierz jedno konto i popraw jego zabezpieczenia od razu.
- Przygotuj plan awaryjny: gdzie zgłosić problem i komu powiedzieć.
- Zapisz trzy sygnały, po których rozpoznasz phishing.

Projekt końcowy

Stwórz osobisty plan bezpieczeństwa cyfrowego: konta priorytetowe, hasła, 2FA, kopie zapasowe, reakcja po incydencie.

Rubryka oceny pracy

Kryterium	Do poprawy	Dobrze	Bardzo dobrze
Rozumienie pojęć	definicje są mylone lub używane przypadkowo	pojęcia są użyte poprawnie w większości przykładów	pojęcia są użyte precyzyjnie i pomagają wyjaśnić problem
Praca ze źródłami	brakuje źródeł albo są niejasne	źródła są wskazane i częściowo porównane	źródła są dobrane świadomie, porównane i ocenione
Zastosowanie w praktyce	wniosek jest ogólny i trudny do wykonania	wniosek wskazuje możliwe działanie	wniosek prowadzi do konkretnego, mierzalnego kroku
Współpraca i komunikacja	wypowiedź jest chaotyczna lub jednostronna	grupa przedstawia stanowisko i słucha pytań	grupa jasno pokazuje proces, decyzje i ograniczenia

Plan wdrożenia po zajęciach

Następne 7 dni

Podręcznik ma prowadzić do działania. Po zajęciach wybierzcie mały krok, który można wykonać bez dużego budżetu i bez czekania na idealne warunki.

- Dzień 1: wybierzcie jeden problem związany z tematem „Bezpieczeństwo w sieci".
- Dzień 2: zbierzcie jeden przykład, jedną daną i jedną opinię osoby zainteresowanej.
- Dzień 3: przygotujcie wersję roboczą rozwiązania lub komunikatu.
- Dzień 4-5: pokażcie wersję roboczą dwóm osobom i zbierzcie uwagi.
- Dzień 6-7: poprawcie materiał i zdecydujcie, gdzie zostanie wykorzystany.

Checklista przed oddaniem pracy

- nie klikaj linków z wiadomości, które wywołują presję lub strach
- używaj unikalnych haseł do najważniejszych kont
- włącz 2FA w poczcie, social mediach i bankowości
- regularnie sprawdzaj uprawnienia aplikacji
- zgłaszaj podejrzane wiadomości i ostrzegaj osoby narażone

Pytania do rozmowy

1. Który element wiadomości najbardziej próbuje wymusić szybkie działanie?
2. Jakie konto w twoim życiu ma największe konsekwencje po przejęciu?
3. Co powinno się stać w pierwszych 15 minutach po podejrzeniu włamania?

Miejsce na notatki

Zakończenie

Najważniejszym efektem pracy z podręcznikiem nie jest zapamiętanie wszystkich pojęć, lecz umiejętność użycia ich w realnej sytuacji: w rozmowie, w internecie, w klasie, w projekcie społecznym albo w działaniu lokalnym.

Wróć do checklisty po kilku dniach. Jeśli potrafisz wykonać większość punktów bez zaglądania do materiału, ten moduł spełnił swoje zadanie.