



MODUŁ 5

CYBERBEZPIECZEŃSTWO I BEZPIECZNE KORZYSTANIE Z INTERNETU



erasmediah.eu



**Co-funded by
the European Union**



Lekcja 5.1

Wprowadzenie do podstaw cyberbezpieczeństwa



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

Lekcja 5.1

Wprowadzenie do podstaw cyberbezpieczeństwa

Cele:

- Rozwinięcie wiedzy na temat podstawowych koncepcji cyberbezpieczeństwa, w tym kluczowych pojęć, takich jak potencjalne zagrożenia, podatność i ryzyko.
- Identyfikowanie powszechnych zagrożeń internetowych, takich jak phishing, złośliwe oprogramowanie, ransomware, ataki socjotechniczne, oraz zrozumienie ich wpływu.
- Wspieranie aktywnej postawy do identyfikowania potencjalnych naruszeń cyberbezpieczeństwa i reagowania na nie.

Kluczowe przesłanie:

- Niezależnie od tego, czy jesteś osobą fizyczną, małą firmą, czy globalnym przedsiębiorstwem, zrozumienie podstawowych praktyk w zakresie cyberbezpieczeństwa jest niezbędne do ochrony twojego śladu cyfrowego.
- Wdrożenie prostych kroków zapobiegawczych może zaoszczędzić znaczną ilość czasu, pieniędzy i stresu w porównaniu z odzyskiwaniem danych po cyberataku.



RODZAJ LEKCJI:





Przegląd lekcji

W dzisiejszym cyfrowym świecie zrozumienie podstaw cyberbezpieczeństwa nie jest już opcjonalne - to konieczność. Ta lekcja wprowadza w podstawowe zasady cyberbezpieczeństwa, typowe zagrożenia i praktyczne sposoby na zwiększenie bezpieczeństwa online. Wspólnie zbadamy, jak chronić osobiste i zawodowe zasoby cyfrowe, wspierając kulturę cyberświadomości i odporności.

Warsztaty podzielone są na 4 etapy:

- 1: Wprowadzenie do podstaw cyberbezpieczeństwa (15 min)
- 2: Identyfikacja typowych zagrożeń cybernetycznych (10 min)
- 3: Strategie dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa (10 min)
- 4: Podsumowanie i wnioski (5 min)



Krok 1

Wprowadzenie do podstaw cyberbezpieczeństwa

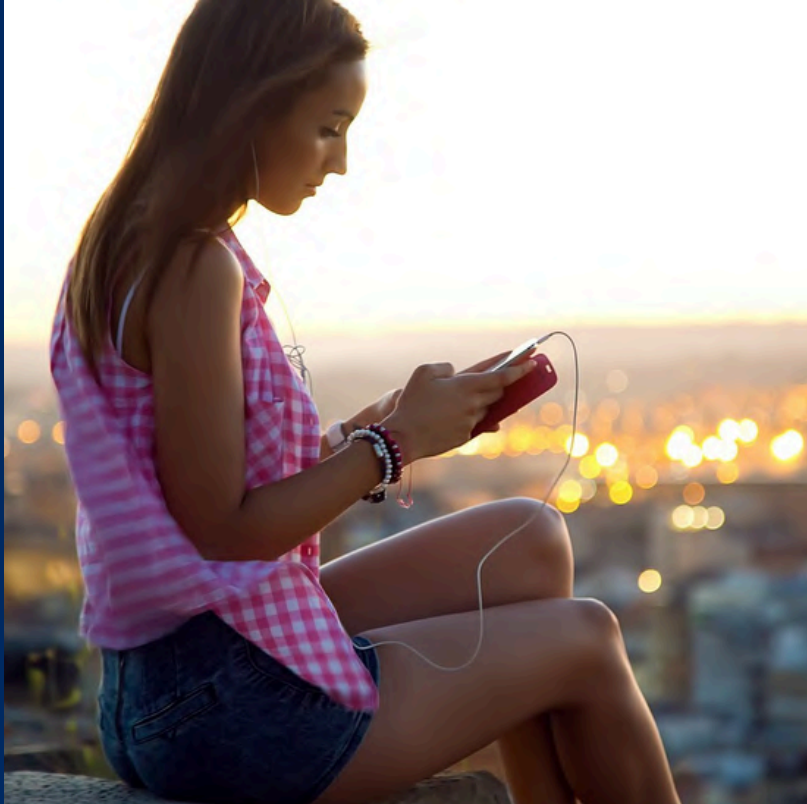
Zacznijmy od krótkiego filmu, który wprowadza pojęcie cyberbezpieczeństwa. W naszym codziennym życiu nieustannie korzystamy z narzędzi cyfrowych, ale jak często zastanawiamy się nad ich bezpieczeństwem? Cyberbezpieczeństwo jest niezbędne do zapewnienia bezpieczeństwa sobie i naszym danym osobowym w cyfrowym świecie. Dzisiaj zagłębimy się w podstawy cyberbezpieczeństwa i dowiemy się, dlaczego jest ono tak ważne.

Obejrzyjmy razem ten film:

<https://youtu.be/inWWhr5tnEA?si=Pxp1YyvjrFdLoo38>

Po obejrzeniu filmu, przejdźmy do dyskusji:

1. Co wyróżniało się dla ciebie w tym filmie na temat cyberbezpieczeństwa?
2. Dlaczego uważasz, że cyberbezpieczeństwo jest ważne w naszym codziennym życiu?



Krok 1

Wprowadzenie do podstaw cyberbezpieczeństwa

Cyberbezpieczeństwo to nie tylko ochrona systemów; to także zrozumienie naszych własnych zachowań online. Sposób, w jaki wchodzimy w interakcje z narzędziami cyfrowymi, może albo wzmocnić nasze bezpieczeństwo, albo uczynić nas podatnymi na zagrożenia.

Poświęćmy chwilę na refleksję nad swoim cyfrowym życiem.

Zapisz odpowiedzi na następujące pytania:

1. Jak często myślisz o bezpieczeństwie swoich działań online?
2. Czy możesz zidentyfikować jakiekolwiek nawyki, które mogą narazić twoje dane osobowe?

Przygotuj się na podzielenie się swoimi przemyśleniami!



Krok 2

Indentyfikacja typowych zagrożeń cybernetycznych

Przyjrzyjmy się bliżej rodzajom zagrożeń cybernetycznych, z którymi możemy się spotkać.

Internet to ogromna przestrzeń pełna możliwości, ale wiąże się również z ryzykiem. Zagrożenia cybernetyczne mogą być wymierzone w każdego i wszędzie, co sprawia, że zrozumienie ich natury i wpływu ma kluczowe znaczenie. Na tym etapie zbadamy różne rodzaje zagrożeń i ich wpływ na nas.

Przeczytaj artykuł: [IBM: Types of Cyber Threats](#)

Artykuł podkreśla:

- Różne rodzaje zagrożeń cybernetycznych, w tym phishing, ransomware i złośliwe oprogramowanie.
- Jak funkcjonują te zagrożenia i na kogo są skierowane.
- Przykłady szkód, jakie mogą wyrządzić.



Krok 2

Indentyfikacja typowych zagrożeń cybernetycznych

Po przeczytaniu artykułu zastanów się nad następującymi kwestiami:

1. Który rodzaj zagrożeń cybernetycznych był dla ciebie najbardziej niepokojący i dlaczego?
2. Czy ty lub ktoś, kogo znasz, doświadczył któregoś z tych zagrożeń?
3. Jak myślisz, w jaki sposób zrozumienie tych zagrożeń może pomóc w zapobieganiu im?

Następnie zapisz jeden prawdziwy przykład lub scenariusz (może być hipotetyczny), w którym występuje jedno z zagrożeń cybernetycznych wymienionych w artykule.

Przygotuj się do podzielenia się swoim przykładem i omówienia go z grupą!



Krok 3

Strategie dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa

Skupmy się teraz na ochronie w sieci.

Podczas gdy zagrożenia cybernetyczne stale ewoluują, istnieją proste i skuteczne kroki, które możemy podjąć, aby chronić nasze informacje i zachować bezpieczeństwo. Przyjmując najlepsze działania w zakresie cyberbezpieczeństwa, możemy zminimalizować ryzyko i zachować bezpieczeństwo w naszym cyfrowym życiu.

Cyberbezpieczeństwo nie wymaga zaawansowanych umiejętności technicznych - drobne, celowe działania mogą mieć duży wpływ na ochronę siebie i swoich danych.



Krok 3

Strategie dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa

Oto kilka kluczowych działań, które warto rozważyć:

- Twórz silne, unikalne hasła i regularnie je zmieniaj.
- Włącz uwierzytelnianie wieloskładnikowe w celu zwiększenia bezpieczeństwa.
- Zachowaj ostrożność w przypadku linków i załączników, zwłaszcza z nieznanych źródeł.
- Aktualizuj oprogramowanie i urządzenia, aby załatać luki w zabezpieczeniach.
- Korzystaj z bezpiecznych połączeń Wi-Fi, unikając w miarę możliwości sieci publicznych.

Aktywność: Lista najlepszych działań w zakresie cyberbezpieczeństwa

Krok 1: Oceń swoje obecne nawyki

- Zastanów się nad swoimi obecnymi zachowaniami i nawykami online. Czy istnieją obszary, w których możesz narażać się na ryzyko?

Przykład: „Używam tego samego hasła na wielu kontach.”

Krok 2: Stwórz plan

- Zapisz jeden możliwy do wykonania krok dla każdej kluczowej koncepcji wymienionej powyżej. Na przykład:

Silne hasła: „Zainstaluję menedżera haseł do generowania i przechowywania bezpiecznych haseł” itp.



Krok 3

Strategie dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa

Krok 3: Dyskusja grupowa

- Podziel się jednym z zaplanowanych działań z partnerem lub grupą.
- Omów, w jaki sposób te kroki mogą pomóc w poprawie bezpieczeństwa cyfrowego.
- Zaproponuj wskazówki lub sugestie dotyczące dodatkowych działań, które mogą podjąć inni.

Na sam koniec odpowiedz sobie w myślach na kluczowe pytanie:

Jaki jest jeden nawyk lub strategia, którą możesz zacząć stosować już dzisiaj, aby natychmiast poprawić swoje bezpieczeństwo online?

Krok 4

Podsumowanie i wnioski

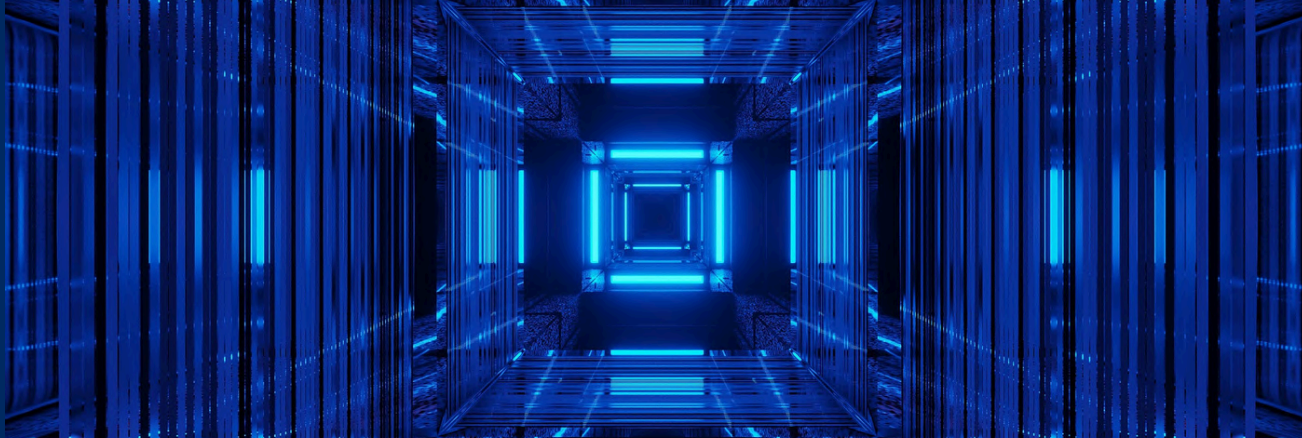
Podsumowując, poświęćmy chwilę na zastanowienie się nad wszystkim, co omówiliśmy w tej lekcji i jak możemy wykorzystać tę wiedzę w przyszłości.

Pomyśl o swoich nawykach online - czy są jakieś zmiany, do których czujesz się zmotywowany po dzisiejszej dyskusji? Jeśli tak, jaki krok podejmiesz w pierwszej kolejności, aby zwiększyć swoje cyberbezpieczeństwo?

Teraz zastanów się, jak możemy pomóc innym. Jaką prostą wskazówką lub nawykiem z tego warsztatu mógłbyś podzielić się z przyjacielem lub współpracownikiem, aby pomóc im zachować bezpieczeństwo w internecie?

Dziękujemy wszystkim za aktywny udział i wnikliwe wypowiedzi!





Podsumowanie kluczowych wniosków

- **Cyberbezpieczeństwo jest dla każdego. Zrozumienie zagrożeń i podjęcie najlepszych działań pomaga nam zachować bezpieczeństwo w sieci.**
- **Małe kroki robią dużą różnicę. Narzędzia takie jak menedżery haseł i regularne aktualizacje mogą znacznie zwiększyć bezpieczeństwo.**
- **Bądź na bieżąco. Zagrożenia cybernetyczne stale ewoluują, więc śledzenie najnowszych wskazówek i narzędzi jest niezbędne dla długoterminowego bezpieczeństwa.**
- **Podejmuj aktywne działania. Im bardziej zaangażujesz się w bezpieczne nawyki, tym bezpieczniejszy będziesz ty i osoby wokół ciebie.**



Instrukcje dla osób pracujących z młodzieżą, edukatorów i nauczycieli

Cel:

Ta lekcja ma na celu pomóc osobom pracującym z młodzieżą, edukatorom i nauczycielom wyposażyć młodych ludzi w niezbędną wiedzę na temat cyberbezpieczeństwa. Poprzez angażujące dyskusje, działania i refleksje uczestnicy zrozumieją powszechne zagrożenia cybernetyczne, poznają najlepsze działania na rzecz bezpieczeństwa w sieci i stworzą praktyczne plany ochrony w cyfrowym świecie.

Potrzebne materiały:

- Połączenie internetowe do materiałów wideo lub artykułów
- Projektor i ekran
- Głośniki
- Dostęp do zalecanych narzędzi cyberbezpieczeństwa
- Karteczki samoprzylepne lub markery do tablicy
- Długopisy lub ołówki
- Arkusze papieru





Krok 1: Wprowadzenie do podstaw cyberbezpieczeństwa (15 min)

1. Rozpocznij od zaangażowania uczestników za pomocą przykładu: „Pomyśl o ostatnim użyciu nowej aplikacji lub odwiedzeniu strony internetowej. Czy zastanawiałeś się nad tym, jak bezpieczne są twoje dane?”.
2. Podkreśl znaczenie cyberbezpieczeństwa: Wyjaśnij, że cyberbezpieczeństwo nie jest przeznaczone tylko dla specjalistów IT; to kluczowa umiejętność dla każdego w dzisiejszej erze cyfrowej. Podkreśl, w jaki sposób cyberbezpieczeństwo pomaga chronić informacje osobiste, zawodowe i organizacyjne.
3. Jasno określ cele sesji.
4. Zajęcie: Oglądanie filmu i dyskusja:
 - Odtwórz film: “What is Cybersecurity?” ([obejrzyj tutaj](#)).
 - Zadaj uczestnikom pytania przewodnie po obejrzeniu filmu.
5. Aktywność: Projekcja filmu i dyskusja:
 - „Co najbardziej zaskoczyło cię w kwestii cyberbezpieczeństwa?”
 - „Czy uważasz, że cyberbezpieczeństwo jest ważne dla każdego? Dlaczego lub dlaczego nie?”
 - „Jakie są zagrożenia wynikające z nieprzywiązywania wagi do bezpieczeństwa online?”





Krok 1: Wprowadzenie do podstaw cyberbezpieczeństwa (15 min)

6. Osobiste przemyślenia: Poproś uczestników, aby poświęcili kilka minut na zapisanie swoich przemyśleń:

- „Jak często zastanawiasz się nad bezpieczeństwem swoich działań online?”
- „Czy możesz zidentyfikować jeden lub dwa nawyki, które mogą narazić twoje dane osobowe na ryzyko?”
- „Jak myślisz, jakie zmiany mógłbyś wprowadzić, aby poprawić swoje bezpieczeństwo online?”

7. Zachęcaj do dzielenia się doświadczeniami w parach lub małych grupach:

- Opcja 1: Podziel się jednym nawykiem, który uważasz za ryzykowny i poproś grupę o radę, jak go poprawić.
- Opcja 2: Przedyskutuj, czy kiedykolwiek doświadczyłeś zagrożenia cybernetycznego lub słyszałeś o nim i jak sobie z nim poradzono.

8. Jeśli uczestnicy wolą nie dzielić się w grupach, pozwól im zapisać jedną zmianę, którą zamierzają wprowadzić i przesłać ją anonimowo moderatorowi do późniejszej dyskusji.





Krok 2: Identyfikacja typowych zagrożeń cybernetycznych (10 min)

1. Udostępnij artykuł [IBM: Types of Cyber Threats](#) lub wydrukowane podsumowanie jego kluczowych punktów.
2. Daj uczestnikom 5 minut na przeczytanie i zanotowanie zagrożeń, które uważają za najbardziej niepokojące, koncentrując się na ich działaniu i potencjalnym wpływie.
3. Dyskusja:
Prowadź rozmowę w grupie:
 - “Które zagrożenia cybernetyczne uważasz za najbardziej niepokojące i dlaczego?”
 - “Czy ty lub ktoś, kogo znasz, doświadczył któregoś z tych zagrożeń? Co się stało?”
4. W razie potrzeby dodaj spostrzeżenia:
Podaj statystyki lub przykłady, aby wzbogacić dyskusję, takie jak emaile phishingowe lub ataki ransomware.
5. Ćwiczenie ze scenariuszem:
Poproś uczestników o napisanie krótkiego przykładu, prawdziwego lub hipotetycznego, dotyczącego jednego zagrożenia cybernetycznego, np:
 - Phishing: „Fałszywy e-mail nakłonił kogoś do udostępnienia loginu do konta”.
 - Złośliwe oprogramowanie: „Kliknięcie podejrzanego linku spowodowało pobranie wirusa i zablokowanie plików”.
6. Podziel się scenariuszami w grupie i przeprowadź dyskusję na ten temat:
 - „Co poszło nie tak w tym scenariuszu?”
 - „Jak można było uniknąć tej sytuacji?”
 - „Jakie środki zapobiegawcze mogłyby pomóc?”
7. Opcjonalnie możesz dołączyć do dyskusji, podkreślając rzeczywiste strategie zapobiegawcze dla każdego rodzaju zagrożenia.





Krok 3: Strategie dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa (10 min)

1. Przegląd praktyk działań:

- Przedstawienie prostych, skutecznych strategii:
 - Używaj silnych, unikalnych haseł.
 - Włącz uwierzytelnianie wieloskładnikowe.
 - Unikaj podejrzanych linków i załączników.
 - Aktualizuj oprogramowanie i urządzenia.
 - Korzystaj z bezpiecznej sieci Wi-Fi lub VPN.
- Użyj prawdziwych przykładów lub krótkich prezentacji, aby pokazać efekt każdej strategii.

2. Jeśli to możliwe, zademonstruj lub wyjaśnij konfigurację jednego narzędzia (zawartego w sekcji „Narzędzia”), aby można było się z nim zapoznać.

3. Aktywność: lista cyberbezpieczeństwa:

- Rozdaj prosty szablon listy z podpunktami z wymienionymi strategiami.
- Poproś uczestników o napisanie jednego możliwego do wykonania kroku dla każdej z nich.
- Przykład: „Włączę uwierzytelnianie wieloskładnikowe w mojej skrzynce email”.
- Zachęć uczestników do skupienia się na prostych, natychmiastowych działaniach i w razie potrzeby wyjaśnij im poszczególne kroki.

4. Dyskusja grupowa:

- Uczestnicy dzielą się jednym krokiem, który planują podjąć.
- Zapewnij informacje zwrotne i zachęć do dyskusji na temat korzyści płynących z tych zmian.
- Zachęć uczestników do regularnego przeglądania listy w celu aktualizacji nawyków.





Krok 4 Podsumowanie i wnioski (5 min)

1. Wspieraj uczenie się oraz motywuj uczestników do stosowania tego czego się nauczyli.
2. Zapytaj uczestników:
 - „Jaki jest jeden z nawyków, który planujesz zmienić lub wprowadzić od dzisiaj?”
 - „Jak podzielisz się z innymi tym, czego się nauczyłeś?”
3. Dyskusja grupowa:
 - Poproś ochotników o podzielenie się swoimi refleksjami lub kluczowymi wnioskami.
4. Komunikat końcowy:
 - Przypomnij uczestnikom: „Cyberbezpieczeństwo to odpowiedzialność każdego z nas. Drobne, celowe kroki mogą mieć duże znaczenie dla zachowania bezpieczeństwa w internecie”.
 - Podziękuj wszystkim za aktywny udział i zachęć ich do natychmiastowego podjęcia działań.

Kluczowe wnioski:

Podkreśl uczestnikom, że cyberbezpieczeństwo to umiejętność, której potrzebuje każdy, niezależnie od posiadanej wiedzy technicznej. Wykorzystaj kluczowe punkty lekcji, aby podkreślić, w jaki sposób zrozumienie powszechnych zagrożeń i przyjęcie środków zapobiegawczych, takich jak używanie silnych haseł lub włączenie uwierzytelniania wieloskładnikowego, może znacznie zmniejszyć ryzyko w świecie online. Zachęć uczestników do aktywnego myślenia poprzez wyznaczenie prostych, osiągalnych celów w zakresie poprawy ich nawyków online. Podkreśl te wnioski poprzez dalsze dyskusje lub działania, które powracają do tych koncepcji, zapewniając, że uczestnicy pozostaną czujni i zmotywowani do utrzymywania silnych praktyk w zakresie cyberbezpieczeństwa.





Działania uzupełniające i zadanie domowe

Zachęć uczestników do przećwiczenia tego, czego się nauczyli, poprzez obserwację ich aktywności online w ciągu następnego tygodnia. Mogą oni zidentyfikować obszary, w których czują się najbardziej narażeni i każdego dnia wdrażać jedną nową strategię cyberbezpieczeństwa. Dodatkowo zasugeruj wypróbowanie narzędzi takich jak LastPass lub Bitdefender w domu i podzielenie się swoimi doświadczeniami z grupą podczas kolejnej sesji.

Wskazowki dla nauczycieli:

Wprowadź tematy związane z cyberbezpieczeństwem do codziennych rozmów lub lekcji, wykorzystując rzeczywiste przykłady, które odnoszą się do doświadczeń uczniów, takich jak bezpieczeństwo w mediach społecznościowych lub powszechne oszustwa. Korzystaj z interaktywnych metod, takich jak dyskusje grupowe lub scenariusze z odgrywaniem ról aby temat był angażujący i przydatny w praktyce. Regularnie sprawdzaj postępy i zapewniaj wsparcie, aby wzmocnić znaczenie budowania silnych nawyków w zakresie cyberbezpieczeństwa.





Narzędzia

LastPass



LastPass to zaawansowane narzędzie do zarządzania hasłami zaprojektowane w celu zwiększenia cyberbezpieczeństwa poprzez generowanie i bezpieczne przechowywanie silnych, unikalnych haseł dla wszystkich kont online. Eliminuje potrzebę zapamiętywania wielu złożonych haseł, przechowując je w zaszyfrowanym skarbcu cyfrowym, dostępnym tylko za pomocą hasła głównego.

www.lastpass.com

Bitdefender



Bitdefender to zaawansowane narzędzie cyberbezpieczeństwa, które oferuje kompleksową ochronę przed złośliwym oprogramowaniem, phishingiem, ransomware i innymi zagrożeniami internetowymi. Łączy w sobie solidne oprogramowanie antywirusowe z inteligentnymi środkami antyphishingowymi, aby zapewnić wielowarstwową ochronę do użytku osobistego i zawodowego.

www.bitdefender.com



Referencje

- Bitdefender. (n.d.). Pozyskano z <https://www.bitdefender.com>
- Cisco Networking Academy. (n.d.). Cybersecurity Essentials. Cisco Networking Academy: Learn Cybersecurity, Python & More. Pozyskano z <https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US>
- IBM. (2024, Marzec 25). Types of cyberthreats. Pozyskano z <https://www.ibm.com/think/topics/cyberthreats-types>
- Lakhwani, S. (2024, Czerwiec 19). Fundamentals of Cybersecurity [2024 Beginner's Guide]. upGrad KnowledgeHut Blog. Pozyskano z <https://www.knowledgehut.com/blog/security/cyber-security-fundamentals>
- LastPass. (n.d.). Pozyskano z <https://www.lastpass.com>
- Simplilearn. (2020, Czerwiec 10). What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn. [Film]. YouTube. <https://youtu.be/inWWhr5tnEA?si=3XP97c0H4JmHxWSo>





QUIZ

1. Jaki jest jeden z głównych celów cyberbezpieczeństwa?

- A. Zapewnienie, że nikt nie może mieć dostępu do internetu bez pozwolenia
- B. Umożliwienie firmom na monitorowanie aktywności użytkowników
- C. Ochrona cyfrowych zasobów poprzez zarządzanie ryzykiem i lukami w bezpieczeństwie
- D. Blokowanie wszystkich wiadomości email od nieznanych nadawców

2. Która z poniższych odpowiedzi jest przykładem uwierzytelniania wieloskładnikowego?

- A. Logowanie się poprzez udzielenie odpowiedzi na pytania bezpieczeństwa
- B. Używanie hasła email oraz zapasowego adresu email do odzyskania danych
- C. Połączenie hasła z tymczasowym kodem wysłanym na telefon
- D. Zapisywanie haseł w zaszyfrowanym pliku na komputerze.

3. Co wyróżnia phishing od innych zagrożeń internetowych?

- A. Polega na bezpośrednim włamywaniu się do systemów bez interakcji z użytkownikiem
- B. Wykorzystuje oszukiwanie aby nakłonić użytkowników do udostępnienia poufnych informacji.
- C. Rozprzestrzenia się za pośrednictwem fizycznych urządzeń, takich jak pendrive'y
- D. Działa wyłącznie poprzez instalowanie złośliwego oprogramowania na komputerze





QUIZ

4. W jaki sposób aktualizowanie oprogramowania zwiększa cyberbezpieczeństwo?
- A. Ulepsza design i użyteczność aplikacji
 - B. Zmniejsza szansę na błędy które utrudniają zadania
 - C. Zamyka luki w zabezpieczeniach które mogli by wykorzystać hakerzy
 - D. Zapewnia lepszą kompatybilność ze starszymi urządzeniami
5. Dlaczego używanie narzędzia do zarządzania hasłami jest korzystne?
- A. Zapewnia to, że hasła są zapisane na jednym dysku
 - B. Automatycznie wylogowuje użytkownika po pewnym czasie
 - C. Tworzy i bezpiecznie przechowuje złożone hasła do każdego konta
 - D. Powiadamia użytkownika, gdy ktoś ma dostęp do jego konta bez pozwolenia





Rozwiązania

Pytanie 1: C

Pytanie 2: A

Pytanie 3: B

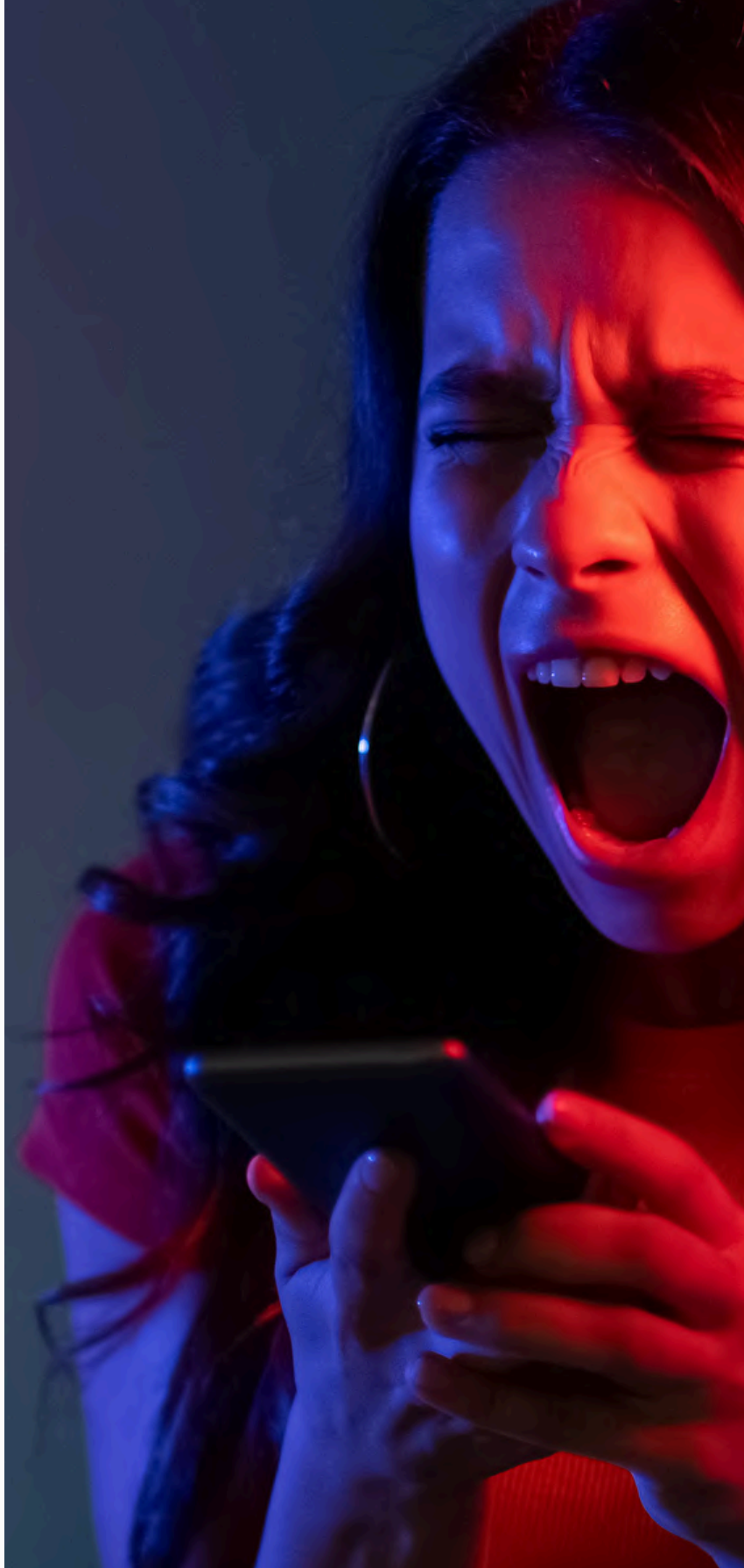
Pytanie 4: B

Pytanie 5: A





Centrum Wspierania
Edukacji
i Przedsiębiorczości



Co-funded by
the European Union

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak wyłącznie poglądami autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie ponoszą za nie odpowiedzialności.