



CYBERSEC
EDUCHECK

RAPORT

PODSUMOWANIE DZIAŁAŃ PROJEKTU CYBERSEC EDUCHECK

2024

Przygotowane przez:

Jadwiga Maj
Karolina Kornecka-Kupiec
Karolina Pokorska
Mateusz Pękala
Pavla Vybihalova
Weronika Kędzierska
Iwona Szczurek

PROJEKT NR 2023-2-PL01-KA210-VET-000176822



Dofinansowane przez
Unię Europejską

LIDER:

Research Institute
Europe



PARTNERZY:



RAPORT Z DZIAŁAŃ PROJEKTU CYBERSEC EDUCHECK

Data: 25 lipca 2024

Lider:

Coventry University Research Institute Europe

Partnerzy:

Stowarzyszenie Kreatywni dla Biznesu (eng. Creative for Business, KREA) – Poland
European Centre for Career Education (ECCEDU) – Czech Republic

I. Opis potrzeb

- Charakterystyka badanych i ich potrzeb.

II. Podsumowanie działań

- Proces rekrutacyjny (nazwy placówek edukacyjnych)
- Zaplanowane wydarzenia (webinary) – terminy, tematy, goście
- Wyniki badania dotyczące odpowiedzi otrzymanych.
- Wyzwania
- Sugestie

III. Rekomendacje dotyczące działania 2.

- Dyskusje na temat obecnych wyzwań i możliwości związanych z proponowanymi działaniami.
- Określenie kierunków działań i identyfikacja obszarów priorytetowych.
- Przygotowanie listy tematów do dalszej pracy i ustalenie harmonogramu działań.
- Zawartość podręcznika/skryptu
- Profile użytkowników

IV. Wnioski i postęp

- Początkowe wnioski z analizy, które umożliwiają planowanie działań na przyszłość.

.....
Podpis lidera

OPIS POTRZEB



Charakterystyka uczestników badania i ich potrzeby różnią się znacząco między uczniami szkół średnich a nauczycielami szkół średnich w obszarze edukacji dotyczącej cyberbezpieczeństwa. Uczniowie szkół średnich zazwyczaj posiadają podstawową świadomość zagrożeń cyberbezpieczeństwa, takich jak cyberprzemoc, kwestie prywatności, phishing i kradzież tożsamości. Znają pojęcia takie jak prywatność w Internecie i ryzyko związane z udostępnianiem danych osobowych, lecz często brakuje im głębszego zrozumienia i praktycznego zastosowania. Chociaż rozumieją znaczenie silnych haseł i bezpiecznego przeglądania, często nie stosują tych praktyk konsekwentnie w swoich działaniach online.

Wiedza wśród studentów jest zauważalna, zwłaszcza w praktycznych aspektach cyberbezpieczeństwa. Wielu studentów boryka się z tworzeniem silnych, unikalnych haseł, rozumieniem znaczenia uwierzytelniania dwuskładnikowego oraz weryfikacją wiarygodności źródeł informacji online. Brak umiejętności krytycznej oceny sprawia, że są podatni na dezinformację i ataki phishingowe. Dodatkowo uczniowie często niedoceniają długoterminowych konsekwencji swoich działań online, takich jak kradzież danych i nieautoryzowane udostępnianie danych osobowych.

Przekonania i obawy uczniów szkół średnich związane z korzystaniem z technologii i cyberbezpieczeństwa są zróżnicowane. Pomimo wyrażanych obaw o kradzież tożsamości, naruszenia prywatności i cyberprzemoc, wielu uczniów uważa, że potrafią samodzielnie radzić sobie z tymi zagrożeniami, co prowadzi do niespójnego stosowania praktyk cyberbezpieczeństwa. To przekonanie czasami wzmacnia fałszywe poczucie bezpieczeństwa, dopóki nie doświadczą bezpośredniego incydentu cybernetycznego. Obawy związane z naruszeniem prywatności oraz narażeniem na szkodliwe treści online kształtują ostrożne zachowania w ich interakcjach online.

Natomiast nauczyciele szkół średnich napotykają wyzwania w efektywnym przekazywaniu wiedzy z obszaru cyberbezpieczeństwa z uwagi na różnorodne czynniki. Obejmują one ograniczony czas poświęcony nauczaniu o cyberbezpieczeństwie, przestarzałe materiały dydaktyczne oraz brak pewności co do własnej wiedzy w tym obszarze. Wielu nauczycieli wyraża silną potrzebę dodatkowych szkoleń i zasobów w celu podniesienia jakości nauczania i dostosowania się do zmieniających się zagrożeń cybernetycznych. Dodatkowe informacje można znaleźć w części II.

Podsumowanie działań

01. Planowanie badań nad edukacją z zakresu cyberbezpieczeństwa w szkołach średnich



Celem tego etapu było przeprowadzenie kompleksowych badań User Experience (UX) w celu zrozumienia potrzeb i wyzwań nauczycieli w zakresie skutecznych narzędzi edukacyjnych i szkoleń z zakresu cyberbezpieczeństwa w szkołach średnich w Polsce i Czechach. Badania te ułatwiły utworzenie szczegółowych profili Persona w celu dostosowania wyników projektu do konkretnych wymagań użytkowników końcowych.

Badanie celowości

Celem badania było ocenienie skuteczności obecnych metod edukacyjnych oraz rola kadry szkół średnich w rozwijaniu kompetencji uczniów w bezpiecznym korzystaniu z technologii. Badanie to dostarcza wniosków mających na celu poprawę inicjatyw edukacyjnych z zakresu cyberbezpieczeństwa w szkołach średnich w Polsce i Republice Czeskiej.

Problematyka badawcza



1.

Aktualna świadomość: Jakie jest zrozumienie zagrożeń cyberbezpieczeństwa przez uczniów szkół średnich?

To pytanie ma na celu ocenę poziomu wiedzy studentów na temat potencjalnych zagrożeń cyberbezpieczeństwa, z którymi mogą się spotkać podczas codziennego korzystania z technologii.

2.

Luki w wiedzy: Czego uczniowie szkół średnich nie wiedzą o cyberbezpieczeństwie? W pytaniu analizowane są konkretne braki w zrozumieniu przez uczniów zasad cyberbezpieczeństwa oraz identyfikowane są obszary, w których potrzebne są dodatkowe działania edukacyjne i uświadamiające w celu podniesienia ich kompetencji w dziedzinie bezpiecznych praktyk technologicznych.

3.

Przekonania i obawy uczniów: Jakie zagrożenia, obawy i przekonania mają uczniowie, które mogą wpływać na ich postawy i zachowania dotyczące bezpiecznych praktyk technologicznych?

Celem badania jest zbadanie percepcji i postaw studentów wobec zagrożeń cyberbezpieczeństwa. Poprzez identyfikację obaw i przekonań można skorygować błędne wyobrażenia i dostosować strategie edukacyjne, które będą rezonować z ich perspektywami.

4.

Efektywność metod nauczania: Jak bardzo obecne metody nauczania przyczyniają się do praktycznego zrozumienia i stosowania przez uczniów zasad cyberbezpieczeństwa?

To pytanie analizuje wpływ obecnych podejść edukacyjnych na zdolność studentów do zrozumienia i zastosowania koncepcji cyberbezpieczeństwa w praktyce, sprawdzając, czy metody te skutecznie integrują wiedzę teoretyczną z umiejętnościami praktycznymi.

5.

Rola personelu szkolnego: Jak personel szkół średnich, w tym nauczyciele i dyrektorzy, postrzegają swoją obecną rolę, stojące przed nimi wyzwania i potencjalne obszary udoskonalień w edukacji na temat cyberbezpieczeństwa w kontekście kształtowania kompetencji uczniów w zakresie bezpiecznego korzystania z technologii?

To badanie analizuje perspektywy personelu szkolnego dotyczące ich obowiązków i wyzwań związanych z dostarczaniem edukacji w obszarze cyberbezpieczeństwa. Zrozumienie ich stanowiska pomaga zidentyfikować potrzeby wsparcia oraz obszary, w których rozwój zawodowy lub dostosowanie programu nauczania mogą przynieść korzyści.

Badania nad doświadczeniem użytkownika:

01

Zrozumienie potrzeb użytkowników:

Poprzez przeprowadzone wywiady, ankiety i obserwacje nasze badania UX dostarczyły wartościowych spostrzeżeń na temat konkretnych wymagań nauczycieli zaangażowanych w edukację w obszarze cyberbezpieczeństwa. To zrozumienie skierowało projektowanie narzędzi, które efektywnie zaspokajają ich potrzeby edukacyjne.

02

Profile odbiorców

Na bazie danych empirycznych opracowaliśmy szczegółowe profile Personas, które precyzyjnie odzwierciedlają zróżnicowane potrzeby i preferencje nauczycieli. Personas te pełnią rolę archetypów, naprowadzając proces projektowania i rozwoju w stronę rozwiązań, które spotykają się z aprobatą użytkowników końcowych.

03

Dostosowywanie rozwiązań:

Nasze badania UX pozwalają na dostosowanie narzędzi edukacyjnych z zakresu cyberbezpieczeństwa do unikalnych kontekstów edukacyjnych w Polsce i Czechach. Dzięki nim narzędzia stają się nie tylko funkcjonalne, ale także przyjazne dla użytkowników i istotne dla lokalnego krajobrazu edukacyjnego.

04

Poprawione zaangażowanie użytkownika:

Poprzez zajmowanie się zidentyfikowanymi punktami zapalnymi i dopasowywanie rozwiązań do potrzeb person, przewidujemy zwiększone zaangażowanie użytkowników i wskaźniki adopcji. Nauczyciele chętniej przyjmują i skuteczniej wykorzystują narzędzia, które są zaprojektowane z myślą o ich konkretnych wyzwaniach.

05

Optymalizacja wyniki projektu:

Integracja spostrzeżeń z badań UX i rozwoju osoby zoptymalizowała skuteczność i sukces inicjatywy edukacyjnej w zakresie cyberbezpieczeństwa w szkołach średnich. To dopasowanie zapewnia, że wyniki projektu spełniają praktyczne potrzeby nauczycieli i przyczyniają się pozytywnie do wyników edukacyjnych.

Podsumowując, zakończenie badań UX i opracowanie osoby odegrały kluczową rolę w kształtowaniu projektu oraz wdrożeniu skutecznych narzędzi edukacyjnych z zakresu cyberbezpieczeństwa dla szkół średnich w Polsce i Czechach. Koncentrując się na potrzebach i preferencjach użytkowników, opracowaliśmy rozwiązania, które nie tylko są technologicznie solidne, lecz także intuicyjne i zorientowane na użytkownika, maksymalizując w ten sposób ich wpływ na wyniki edukacyjne.

Podsumowanie działań

02. Rekrutacja do szkoły

Rekrutacja szkół do projektu została przeprowadzona wspólnie przez Coventry University i partnera w Czechach. Obejmowało to bezpośredni kontakt ze szkołami, które już były zaangażowane w inicjatywy cyberbezpieczeństwa lub wykazały zainteresowanie poprawą edukacji w zakresie cyberbezpieczeństwa. W Polsce znaczną liczbę zrekrutowanych szkół stanowiły instytucje prywatne, które wykazały większą chęć uczestnictwa w dodatkowych działaniach i programach pilotażowych. Proces rekrutacji rozpoczął się w marcu i zakończył pod koniec kwietnia. Po pomyślnej rekrutacji w kwietniu zorganizowano wydarzenie wprowadzające, aby zapoznać uczestniczące szkoły z celami projektu, metodologiami i oczekiwanymi wynikami oraz zaoferować dodatkową wiedzę. Wydarzenie to stanowiło platformę wymiany pomysłów między edukatorami i przygotowało grunt pod produktywną współpracę przez cały okres trwania projektu.



Spis szkół i uczestników badania:

W badaniu w Polsce uczestniczyło 17 nauczycieli i 443 uczniów, podczas gdy w Czechach było to 5 nauczycieli i 198 uczniów.

POLSKA:

Nauczyciele:

Autorskie Liceum Navigo Wrocław: 5 osób
Niepubliczna Szkoła Podstawowa Montessori we Wrocławiu: 7 osób
Liceum Ogólnokształcące nr X we Wrocławiu: 1 osoba
British International School we Wrocławiu: 2 osoby
IPS International School of Wrocław: 2 osoby

Uczniowie:

Autorskie Liceum Navigo Wrocław: 26 uczniów
Niepubliczna Szkoła Podstawowa Montessori we Wrocławiu: 28 uczniów
Liceum Ogólnokształcące nr X we Wrocławiu: 385 uczniów
British International School we Wrocławiu: 2 uczniów
IPS International School of Wrocław: 2 uczniów



CZECHY:

Nauczyciele:

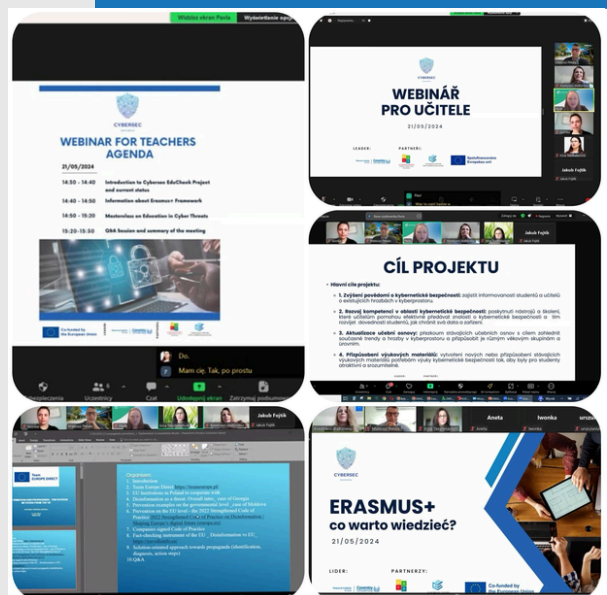
Střední škola technická a ekonomická: 1 osoba
Duhovka, gymnázium: 1 osoba
Gymnázium, Praha 6, Arabská 14: 1 osoba
Gymnázium Karla Sladkovského: 1 osoba
Hotelová škola: 1 osoba

Uczniowie:

Střední škola technická a ekonomická: 64 uczniów
Duhovka, gymnázium: 35 uczniów
Gymnázium, Praha 6, Arabská 14: 53 uczniów
Gymnázium Karla Sladkovského: 24 uczniów
Hotelová škola: 22 uczniów

Podsumowanie działań

Webinar dla nauczycieli uczestniczących w badaniach



21 maja 2024 r. odbyło się webinarium dotyczące zagrożeń cybernetycznych dla nauczycieli z Polski i Czech, którzy brali udział w projekcie. Moderatorami byli eksperci: Mateusz Pekala i Pavla Vybihalova, którzy zaprezentowali cele, zalety projektu oraz program Erasmus+ uczestnikom.

SEMINARIUM ONLINE DLA PEDAGOGÓW

Nauczyciele mieli okazję uczestniczyć w warsztacie prowadzonym przez Irinę Tkeshelashvili, członkinię Team Europe Direct Poland, która jest ekspertem Komisji Europejskiej ds. polityki i stosunków międzynarodowych. Przedstawiła ona interesujące przemówienie na temat znaczenia cyberświadości w kontekście edukacyjnym, opierając się na swoich doświadczeniach na arenach międzynarodowych, takich jak Gruzja.



CYBERSEC
EDUCHECK

SEMINARIUM ONLINE DLA PEDAGOGÓW PORZĄDEK OBRAD

21.05.2024

- | | |
|---------------|---|
| 14:30 - 14:40 | Inicjacja projektu Cybersec EduCheck bieżąca sytuacja |
| 14:40 - 14:50 | Informacje dotyczące programu Erasmus+ |
| 14:50 - 15:20 | Kurs mistrzowski dotyczący edukacji na temat zagrożeń cybernetycznych. |
| 15:20-15:30 | Spotkanie z sesją pytań i odpowiedzi oraz podsumowaniem. |



Co-funded by
the European Union

LIDER:

Research Institute Europe

Coventry University

WZMACNIA

CZ:

STOWARZYSZENIE
KREATYWNÓW DLA
BUDUCI

EUROPEAN CENTRE
FOR CAREER EDUCATION

Podsumowanie działań

Badania naukowe



Ankiety

Uczniowie szkół średnich: Ankiety zostały wysłane do 443 uczniów w Polsce i 198 uczniów w Czechach. Ankiety skupiały się na ocenie świadomości uczniów dotyczącej zagrożeń cyberbezpieczeństwa, identyfikacji braków w wiedzy oraz ocenie skuteczności obecnych metod edukacyjnych.

Nauczyciele: 17 nauczycieli w Polsce i 5 nauczycieli w Czechach wypełniło ankiety. Celem ankiet było ocenienie perspektyw nauczycieli dotyczących ich roli w edukacji z zakresu cyberbezpieczeństwa, wyzwań, z którymi się zmagają, oraz sugestii dotyczących ulepszeń.

Studenci polscy

443

Ankiety zostały wypełnione przez 443 uczniów w Polsce.

Studenci z Czech.

198

Ankiety zostały wypełnione przez 198 uczniów w Czechach.

Nauczyciele

22

Ankiety wypełniło 17 nauczycieli w Polsce i 5 nauczycieli w Czechach.

Podsumowanie działań

Wywiady pogłębione



Wywiady:

Nauczyciele: Przeprowadzono wywiady z ośmioma nauczycielami (trzema z Polski i pięcioma z Czech), aby poznać ich poglądy na potrzeby uczniów w obszarze cyberbezpieczeństwa, efektywność obecnych metod nauczania oraz sugestie dotyczące doskonalenia edukacji w dziedzinie cyberbezpieczeństwa.

8

Nauczyciele

Przeprowadzono wywiady z **8 nauczycielami** (trzema z Polski i pięcioma z Czech).

Ta sekcja podsumowuje kluczowe wnioski z analizy praktyk edukacyjnych dotyczących cyberbezpieczeństwa w szkołach średnich, opartych na odpowiedziach zebranych od nauczycieli. Wyniki podkreślają różnorodne metody, wyzwania oraz skuteczne strategie obserwowane w procesie nauczania cyberbezpieczeństwa uczniów.

Ocena świadomości cyberbezpieczeństwa uczniów szkół średnich ujawnia znaczące rozbieżności między samooceną a oceną zewnętrzną. Podczas gdy uczniowie oceniają siebie wysoko, na poziomie 3,89 na 5, w zakresie świadomości cyberbezpieczeństwa, nauczyciele oceniają ich niżej, na poziomie 2,86. Wskazuje to na lukę w postrzeganiu, która sugeruje potrzebę bardziej wszechstronnej edukacji na temat praktyk cyberbezpieczeństwa, zwłaszcza zaawansowanych środków, takich jak uwierzytelnianie wieloskładnikowe (MFA), z którymi połowa uczniów nie jest zaznajomiona.

Badanie podkreśla niepokojące trendy w korzystaniu z Internetu i nawykach studentów. Większość, 61%, spędza 4 godziny lub więcej online dziennie, często sprawdzając urządzenia przed snem, co potencjalnie wpływa na jakość snu i ogólne samopoczucie.

W kontekście bezpieczeństwa online, 25% respondentów zgłosiło doświadczenie cyberprzemocy lub nienawiści online, podczas gdy 60% nie miało takich doświadczeń, a pozostali nie udzielili odpowiedzi, co podkreśla delikatność problemu. Odpowiedzi różniły się pod względem sposobów radzenia sobie z incydentami, gdzie znaczna liczba osób postanowiła zignorować incydent lub nie podjąć żadnych działań (72), podczas gdy inni zareagowali negatywnie (24) lub próbowali pomóc lub zgłosić problem (13).

Studenci zaproponowali różne pomysły na zwiększenie świadomości cyberbezpieczeństwa, wskazując konkretne tematy, które powinny być poruszone podczas zajęć z tego obszaru. Propozycje obejmują kwestie cyberprzemocy, konkretnych zagrożeń, ogólnej edukacji cyberbezpieczeństwa oraz tematów mieszanych.

Odpowiedzi otwarte również wykazały różnorodność opinii. Wiele z nich było nieistotnych lub negatywnych, podczas gdy inne zawierały konstruktywne opinie na tematy takie jak bezpieczeństwo przeglądarki. Niektórzy respondenci podzielili się osobistymi doświadczeniami z cyberprzemocą i podkreślili potrzebę lepszych środków ochronnych oraz surowszych przepisów online dla młodych użytkowników.

W ogólności, chociaż uczniowie wykazują przyzwoity poziom samoświadomości w zakresie cyberbezpieczeństwa, istnieje wyraźna możliwość poszerzenia edukacji na temat zaawansowanych środków bezpieczeństwa i skuteczniejszego rozwiązywania powszechnych problemów, takich jak cyberprzemoc.



INTERNET

61% respondentów spędza codziennie 4 godziny lub dłużej w sieci.



BEZPIECZEŃSTWO W SIECI

25% respondentów potwierdziło, że doświadczyło cyberprzemocy i hejtu online.



CYBERBEZPIECZEŃSTWO

Studenci wysoko oceniają swoją świadomość z zakresu cyberbezpieczeństwa, uzyskując ocenę 3,89 na 5.



CYBERBEZPIECZEŃSTWO PRAKTYKI

Ujawnia brak w postrzeganiu, co wskazuje na konieczność bardziej wszechstronnej edukacji na temat cyberbezpieczeństwa.



Skuteczna edukacja z zakresu cyberbezpieczeństwa

Skuteczna edukacja w dziedzinie cyberbezpieczeństwa w szkołach średnich wymaga zrównoważonego podejścia, które łączy tradycyjne metody nauczania z interaktywnymi i praktycznymi doświadczeniami edukacyjnymi.

Bieżąca świadomość i braki wiedzy:

Uczniowie szkół średnich wykazują ogólną świadomość zagrożeń związanych z cyberbezpieczeństwem, takich jak cyberprzemoc, kwestie prywatności, phishing i kradzież tożsamości. Znają podstawowe koncepcje, takie jak prywatność online i ryzyko związane z ujawnianiem danych osobowych. Niemniej jednak ich zrozumienie często pozostaje powierzchowne, co skutkuje niedocenianiem złożoności i powszechności tych zagrożeń. Przykładowo, są świadomi niebezpieczeństw związanych ze słabymi hasłami i potrzebą bezpiecznego przeglądania, ale nie zawsze konsekwentnie stosują tę wiedzę w swoim zachowaniu online.

Studenci wykazują znaczne braki w swojej wiedzy na temat cyberbezpieczeństwa, zwłaszcza jeśli chodzi o środki praktyczne. Wielu nie ma pojęcia, jak tworzyć silne, unikalne hasła ani jak istotne jest dwuskładnikowe uwierzytelnianie. Napotykają trudności z weryfikacją wiarygodności stron internetowych i rozróżnianiem źródeł informacji od fałszywych. Brak umiejętności w dokonywaniu krytycznej oceny sprawia, że są podatni na dezinformację i ataki phishingowe. Ponadto uczniowie często nie do końca rozumieją potencjalne długoterminowe konsekwencje swoich działań online, takie jak kradzież danych i nieautoryzowane udostępnianie informacji.

Przekonania, obawy i efektywność edukacyjna:

Uczniowie szkół średnich mają różne obawy i przekonania, które wpływają na ich postawy i zachowania wobec korzystania z technologii. Obawiają się kradzieży tożsamości, naruszeń prywatności oraz wpływu cyberprzemocy na ich życie społeczne. Mimo tych obaw wielu uczniów uważa, że potrafią samodzielnie radzić sobie z tymi zagrożeniami, co prowadzi do niekonsekwentnego stosowania praktyk bezpieczeństwa. To przekonanie czasami prowadzi do fałszywego poczucia bezpieczeństwa, które sprawia, że czują się odporni na cyberzagrożenia, dopóki nie staną się ofiarami incydentu osobiście. Strach przed naruszeniem prywatności i ekspozycją na szkodliwe treści kształtuje również ich ostrożne podejście do interakcji online.



Skuteczna edukacja w dziedzinie cyberbezpieczeństwa w szkołach średnich wymaga zrównoważonego podejścia, które łączy tradycyjne metody nauczania z interaktywnymi i praktycznymi doświadczeniami edukacyjnymi. Tradycyjne metody dydaktyczne, takie jak wykłady, są powszechnie stosowane do przekazywania teoretycznej wiedzy na temat cyberbezpieczeństwa. Jednak preferowane są metody interaktywne, takie jak dyskusje grupowe, studia przypadków i symulacje, ze względu na ich zdolność do zaangażowania uczniów i zastosowania koncepcji cyberbezpieczeństwa w realnych sytuacjach. Ćwiczenia praktyczne i symulacje są szczególnie cenione za dostarczanie praktycznego doświadczenia i demonstrację konsekwencji cyberzagrożeń. Osobiste anegdoty i przykłady z życia mają silny wpływ na uczniów, sprawiając, że abstrakcyjne koncepcje stają się bardziej zrozumiałe i mają większe znaczenie. Wykorzystanie narzędzi online, takich jak „haveibeenpwned”, do sprawdzania potencjalnych naruszeń danych, znacząco zwiększyło świadomość uczniów na temat podatności ich danych osobowych. Projekty grupowe i wspólne inicjatywy edukacyjne, takie jak kampanie „Stop Cyberbullying” i zadania grupowe, sprzyjają pracy zespołowej i pozwalają uczniom dogłębnie zgłębiać kwestie cyberbezpieczeństwa. Te metody nie tylko angażują uczniów, ale także zwiększają ich praktyczne umiejętności i wiedzę.

Personel szkolny:

Pracownicy szkół średnich, w tym nauczyciele i dyrektorzy, rozumieją swoją istotną rolę w rozwijaniu kompetencji uczniów w obszarze cyberbezpieczeństwa, ale napotykają na istotne wyzwania. Problemy te obejmują niedobór aktualnych materiałów dydaktycznych, ograniczony czas na dedykowaną edukację z zakresu cyberbezpieczeństwa oraz brak pewności co do własnej wiedzy na temat tego zagadnienia. Wielu nauczycieli wyraża potrzebę większej liczby szkoleń i zasobów, aby skutecznie nauczać cyberbezpieczeństwa. Dostrzegają oni również potencjał poprawy poprzez lepszą integrację tematyki cyberbezpieczeństwa w całym programie nauczania oraz zwiększone zaangażowanie zewnętrznych ekspertów. Promowanie kultury świadomości cyberbezpieczeństwa w całej placówce edukacyjnej i propagowanie dobrych praktyk są postrzegane jako kluczowe kroki w kierunku zwiększenia bezpiecznego korzystania z technologii przez uczniów.

Podsumowanie działań

Możliwości nauczania

Nauczyciele zauważyli różne zachowania i zagrożenia cybernetyczne, z którymi borykają się uczniowie, co pozwoliło im lepiej zrozumieć naturę tych zagrożeń oraz metody, jakimi uczniowie starają się im przeciwdziałać. Jednym z częstych problemów jest cyberprzemoc, gdzie uczniowie doświadczają upokorzenia, wykluczenia, krytyki oraz manipulacji za pomocą obrazów lub filmów. Mimo że zwykle zgłaszają takie incydenty nauczycielom lub rodzicom, zwłaszcza gdy zaangażowani są inni uczniowie, wielu z nich początkowo próbuje samodzielnie poradzić sobie z takimi sytuacjami, stosując różne strategie.

Kwestie prywatności stanowią istotny problem, gdyż uczniowie często ujawniają osobiste i poufne informacje online, w tym poprzez publiczne konta w mediach społecznościowych, takich jak Instagram. Mimo świadomości, że internet nie gwarantuje anonimowości, uczniowie borykają się z trudnościami w zabezpieczeniu swojej prywatności, co niesie ze sobą ryzyka, takie jak kradzież danych, nieuprawnione udostępnianie informacji oraz ekspozycję na treści szkodliwe.



Phishing oraz kradzież danych stanowią powszechne zagrożenia, których często stają się ofiarami uczniowie z powodu braku wystarczającej wiedzy na temat cyberbezpieczeństwa. Do typowych środków zapobiegawczych zalicza się uwierzytelnianie dwuskładnikowe, weryfikację wiarygodności witryny oraz unikanie nieznanych linków. Dodatkowo uczniowie przejawiają nieodpowiednie praktyki cyberbezpieczeństwa, stosując słabe i powtarzające się hasła, udostępniając hasła innym osobom oraz nie wylogowując się z prywatnych kont, co sprawia, że stają się podatni na nieautoryzowany dostęp do konta oraz kradzież tożsamości.

Kolejnym wyzwaniem jest identyfikacja legalnych źródeł informacji oraz rozróżnienie treści faktycznych od fałszywych. Studenci często uznają informacje z mediów społecznościowych za wiarygodne i mają trudności z dokonywaniem krytycznej oceny treści online, co sprzyja rozprzestrzenianiu się dezinformacji i manipulacji.

Podsumowanie działań

Możliwości nauczania

Nadmierne korzystanie z Internetu i ekspozycja na szkodliwe treści, takie jak przemoc i pornografia, również są zauważane. Studenci spędzają zbyt wiele czasu online, często mając dostęp do nieodpowiednich treści i nie potrafiąc się samoregulować. To nadmierne korzystanie jest powiązane z dążeniem do nierealistycznych standardów wyglądu i zachowania.



Wśród studentów powszechnie brakuje odpowiedniej świadomości na temat cyberbezpieczeństwa. Mają oni ograniczoną wiedzę o dostępnych środkach ochrony oraz potencjalnych konsekwencjach swoich działań online. Czyni ich to podatnymi na manipulację i naruszenia prywatności.



Nauczyciele napotykają wiele wyzwań związanych z efektywnym nauczaniem cyberbezpieczeństwa. Często mają trudności z zainteresowaniem uczniów oraz uświadamianiem im istoty cyberbezpieczeństwa, gdyż uczniowie mogą bagatelizować problemy lub nie przekładać wiedzy teoretycznej na praktykę. Brak odpowiednich materiałów dydaktycznych, ograniczenia czasowe, niepewność co do własnej wiedzy oraz niewystarczający dostęp do sprzętu stanowią przeszkody w skutecznym nauczaniu. Dodatkowo niektóre szkoły borykają się z kompleksową integracją cyberbezpieczeństwa z programem nauczania oraz podnoszeniem świadomości na temat jego znaczenia.

Aby sprostać wyzwaniom, zidentyfikowano skuteczne strategie i narzędzia. Zaproszenie ekspertów ds. cyberbezpieczeństwa do dyskusji na temat bieżących problemów i scenariuszy z życia wzmacnia naukę i znaczenie. Wykorzystanie interaktywnych metod, takich jak ankiety, dyskusje i sesje burzy mózgów, sprzyja zaangażowaniu uczniów i głębszemu zrozumieniu. Praktyczne zastosowania, w tym zajęcia praktyczne, projekty i symulacje, skutecznie łączą wiedzę teoretyczną z zastosowaniem w świecie rzeczywistym. Dostęp do kompleksowych zasobów edukacyjnych, w tym podręczników, dedykowanych sesji szkoleniowych i narzędzi online, wspiera skuteczną edukację w zakresie cyberbezpieczeństwa. Promowanie dobrych praktyk, takich jak dzielenie się wiedzą w społeczności szkolnej i angażowanie rodziców, może zwiększyć ogólną skuteczność edukacji w zakresie cyberbezpieczeństwa. Zapewnianie jasnych protokołów reagowania na incydenty i wspieranie współpracy interdyscyplinarnej również przyczynia się do bardziej spójnego i skutecznego doświadczenia edukacyjnego.

Skuteczna edukacja w dziedzinie cyberbezpieczeństwa w szkołach średnich wymaga zrównoważonego podejścia, które łączy tradycyjne metody nauczania z interaktywnymi i praktycznymi doświadczeniami edukacyjnymi. Nauczyciele odgrywają kluczową rolę w przezwyciężaniu wyzwań poprzez wykorzystanie innowacyjnych strategii nauczania, zaangażowanie ekspertów i zapewnienie uczniom szerokich możliwości praktycznego wykorzystania zdobytej wiedzy. Konieczne jest zwrócenie uwagi na ograniczenia zasobów oraz zwiększenie integracji we wszystkich obszarach programu nauczania, aby wychować pokolenie świadomych cyberbezpieczeństwa, posiadających umiejętności bezpiecznego poruszania się w środowiskach cyfrowych.

Dalsze informacje na temat projektu



-  <https://www.coventry.ac.uk/wroclaw/>
-  <https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/>
-  <https://eccedu.net/>

Finansowane przez Unię Europejską. Wyrażone poglądy i opinie są jednak poglądami i opiniami wyłącznie autora(-ów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Ani Unia Europejska, ani EACEA nie mogą być za nie pociągnięte do odpowiedzialności.

Wszystkie rezultaty opracowane w ramach niniejszego projektu są dostępne na podstawie otwartych licencji (CC BY-NC 4.0). Mogą być wykorzystywane bezpłatnie i bez ograniczeń. Kopiowanie lub przetwarzanie tych materiałów w całości lub w części bez zgody autora jest zabronione. W przypadku wykorzystania rezultatów konieczne jest podanie źródła finansowania i ich autorów.

PROJEKT NR 2023-2-PL01-KA210-VET-000176822



**Dofinansowane przez
Unię Europejską**

LIDER:

Research Institute
Europe



PARTNERZY:

