CYBER BEZPIECZNI

PFR Fundacja

RAPORT 2023

Centralny Dom Technologii

NIEBEZPIECZNIK.PL

Fundacja Cyber

SPIS TREŚCI

O RAPORCIE

Niniejszy raport jest podsumowaniem projektu Cyberbezpieczni oraz próbą odpowiedzi na pytania związane z największymi wyzwaniami w obszarze cyberbezpieczeństwa dla dzieci i młodzieży. Na kolejnych stronach raportu opisywane są dotychczasowe działania w ramach programu oraz ich cele edukacyjne, a także analizowane są wyniki procesów ewaluacyjnych i wyników oraz ankiet zebranych w ramach organizacji Testu Wiedzy. Choć te ostatnie nie mają charakteru badań reprezentatywnych, ich analiza może stanowić cenne narzędzie ewaluacji działań edukacyjnych w projekcie oraz wskazywać na największe wyzwania w obszarze cyberbezpieczeństwa, z którymi stykali się uczestnicy i uczestniczki projektu.

O PROJEKCIE „CYBERBEZPIECZNI”

„Cyberbezpieczni” to ogólnopolski program edukacyjny realizowany przez Fundację Polskiego Funduszu Rozwoju, promujący wiedzę i bezpieczne zachowania w Internecie. Jest on skierowany do uczniów i nauczycieli szkół podstawowych i ponadpodstawowych. W projekcie wzięło udział ponad 7000 uczniów i ponad 100 nauczycieli. W edycji 2023 roku oprócz warsztatów (4000 uczestników) i kursów dla nauczycieli (ponad 100 uczestników) zaplanowaliśmy także ogólnopolski test wiedzy na temat bezpieczeństwa w sieci (ponad 3000 uczestników).

PROJEKT SKŁADA SIĘ Z PIĘCIU KOMPONENTÓW EDUKACYJNYCH:

- Szkolenia dla nauczycieli
- Warsztaty dla uczniów
- Praktyczny przewodnik po cyberbezpieczeństwie dla rodziców
- Publikacja ze scenariuszami
- Ogólnopolski Konkurs i Test wiedzy

Wyniki działań edukacyjnych

Struktura projektu Cyberbezpieczni zaprojektowana została jako edukacyjna ścieżka pozwalająca na możliwie jak najbardziej kompleksowe działania edukacyjne docierające do kilku grup docelowych: **uczniów, nauczycieli i rodziców**. Przez cały czas trwania projektu realizowane były bezpłatne warsztaty dla szkół w całej Polsce. Warsztaty realizowane były zarówno w formule stacjonarnej (w Centralnym Domu Technologii) jak i online, co umożliwiało wzięcie udziału w projekcie uczestnikom z całej Polski. Zrealizowano łącznie **460 warsztatów** dla **4000 uczestników i uczestniczek.**

460 warsztatów dla 4000 uczestników i uczestniczek.

Bezpłatne warsztaty dla uczniów uzupełnione zostały o **szkolenia dla nauczycieli.** Szkolenia prowadzone w Krakowie, Wrocławiu, Białymstoku oraz online, dotarły do ponad setki nauczycieli i nauczycielek. Działania dla uczniów i nauczycieli wspierane były następnie przez kampanie edukacyjne przeznaczone dla rodziców. Specjalna broszura dla opiekunów, rozesłana do szkół biorących udział w projekcie oraz webinar dla rodziców na temat bezpieczeństwa dzieci w sieci, przygotowane zostały we współpracy z redakcją niebezpiecznik.pl.

Wszystkie te działania nakierowane były na zapewnienie kompleksowego wsparcia grupom stanowiącym podstawę systemu edukacji w Polsce, czyli triadzie **uczeń-rodzic-nauczyciel**. Uczniowie i uczennice, nauczyciele i nauczycielki oraz rodzice mieli możliwość wspólnego zadbania o bezpieczeństwo w sieci dzieci i młodzieży.

Zwieńczeniem projektu był Konkurs i Ogólnopolski **Test Wiedzy „Cyberbezpieczni”**, w którym dzieci i młodzież mogły sprawdzić swoją wiedzę na temat bezpieczeństwa w Internecie. Do konkursu mogli przystąpić uczestniczki i uczestnicy zajęć w ramach projektu, a także wszyscy chętni. Każdy uczestnik konkursu odpowiedział w Teście Wiedzy na **27 pytań** o trzech poziomach trudności i w trzech tematach: „Cyberbezpieczeństwo”, „Fake newsy i manipulacje medialne” oraz „Oszustwa internetowe”. W teście wzięło ponad 3,5 tysiąca osób. W teście dla szkół podstawowych było to dokładnie **698 uczniów i uczennic.** Liczba uczestników i uczestniczek ze szkół ponadpodstawowych wynosiła natomiast **2891**.

Zebrane wyniki testu, a także wyniki ewaluacji warsztatów dla dzieci i młodzieży, zostały następnie przeanalizowane w celu wyłonienia największych wyzwań związanych z edukacją o cyberbezpieczeństwie. To właśnie tym wyzwaniom, tematom i zagadnieniom, a także odpowiedziom na nie ze strony ekspertów, poświęcone są dalsze strony niniejszego raportu.

Warsztaty

W ramach projektu Cyberbezpieczni przeprowadzono warsztaty z zakresu cyberbezpieczeństwa, prywatności w mediach społecznościowych oraz manipulacji medialnych. Warsztaty, które odbywały się w dwóch 90-minutowych blokach, poprzedzone były pretestem i zakończone posttestem z tymi samymi pytaniami.

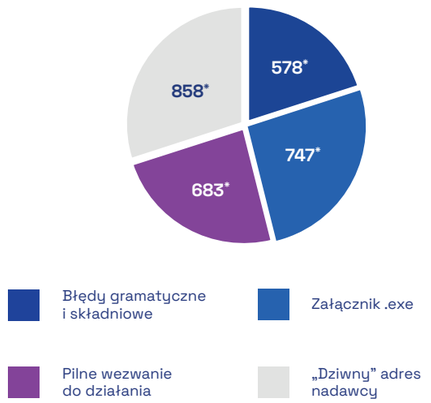
Cyberbezpieczeństwo

Średnia punktacja pretestu z zakresu cyberbezpieczeństwa wyniosła 3,8/9 punktów, zaś średnia punktacja posttetsu wyniosła 5,2/9 punktów, co stanowi progres i świadczy o wysokiej efektywności prowadzonych warsztatów.

Poniżej zaprezentowane zostały wybrane pytania oraz wyniki pretestów i posttestów zajęć o cyberbezpieczeństwie. Wybrane zostały trzy pytania sprawiające największe trudności oraz trzy pytania, w których stwierdzono największy przyrost wiedzy. Uczniowie największe problemy mieli z zadaniem dotyczącym ataku IDN homograph oraz sposobami ochrony przed keyloggerem i phishingiem. Udział uczniów w warsztatach zwiększył poziom ich wiedzy o kilkanaście punktów procentowych.

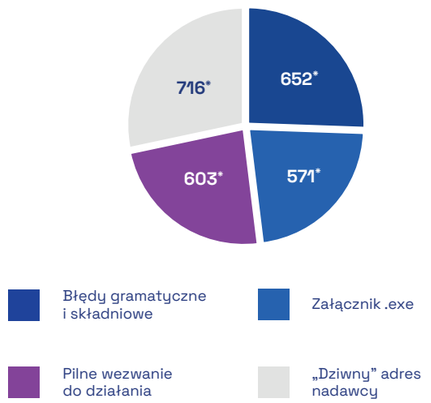
Pytania o najniższym wyniku w preteście:

1. Co może wskazywać na wiadomość phishingową?
15% uczestników (245 z 1586) odpowiedziało poprawnie na to pytanie



Rysunek 1. Co może wskazywać na wiadomość phishingową - **Pretest**.

2. Co może wskazywać na wiadomość phishingową?
41% uczestnikó (411 z 1003) odpowiedziało poprawnie na to pytanie

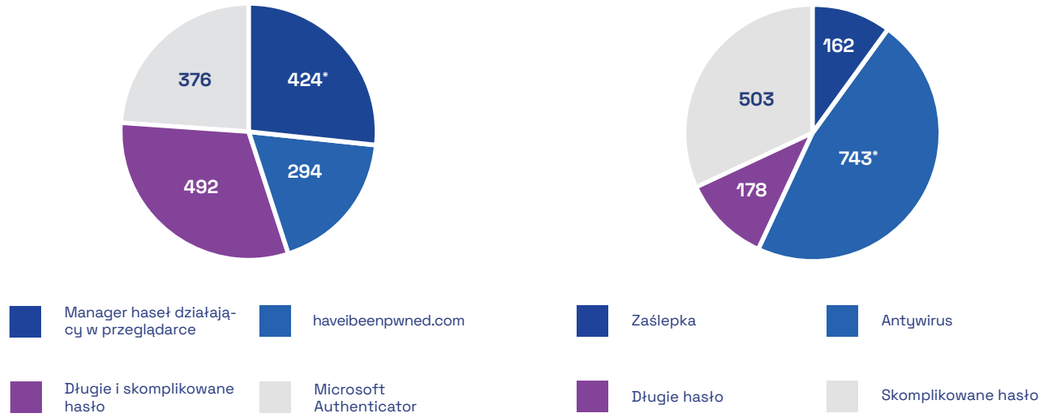


Rysunek 2. Co może wskazywać na wiadomość phishingową - **Posttest**.

*odpowiedź prawidłowa

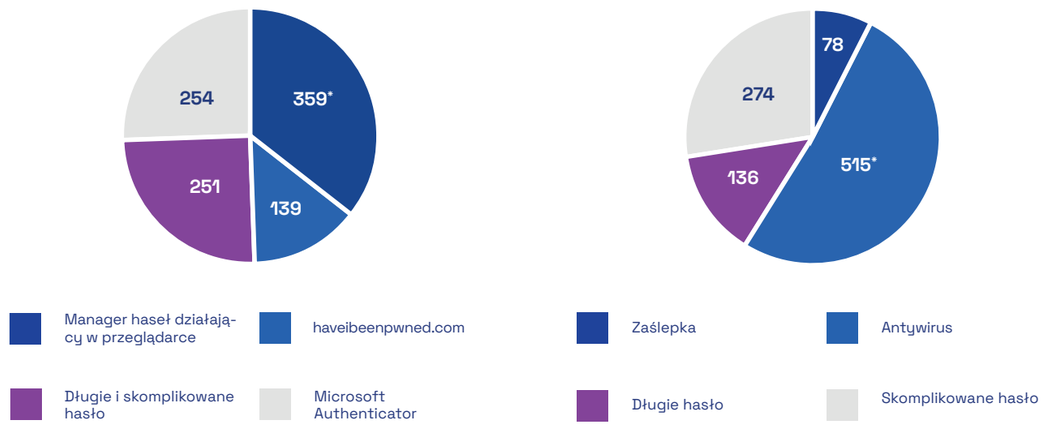
Pytania o najniższym wyniku w preteście:

3. Co obroni mnie przed atakiem IDN homograph?
27% uczestników (424 z 1586) odpowiedziało poprawnie na to pytanie.



3. Co obroni mnie przed atakiem IDN homograph? - **Pretest.**

4. Co obroni mnie przed atakiem IDN homograph?
36% uczestników (359 z 1003) odpowiedziało poprawnie na to pytanie.



Rysunek 4. Co obroni mnie przed atakiem IDN homograph? - **Posttest**.

5. Co obroni mnie przed Keyloggerem?
47% uczestników (743 z 1586) odpowiedziało poprawnie na to pytanie.

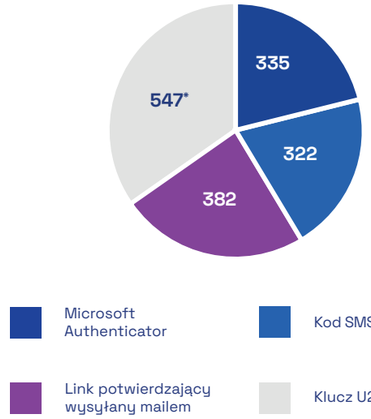
Rysunek 5. Co obroni mnie przed Keyloggerem - **Pretest.**

6. Co obroni mnie przed Keyloggerem?
51% uczestników (515 z 1003) odpowiedziało poprawnie na to pytanie.

Rysunek 6. Co obroni mnie przed Keyloggerem - **Posttest**.

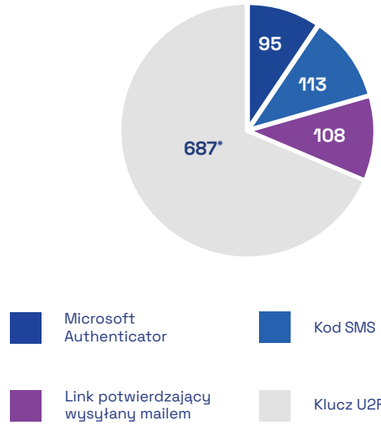
Pytania o największym przyroście wiedzy:

Rysunek 7. Który z poniższych narzędzi obroni mnie najlepiej przed Spear phishingiem?
34% uczestników (547 z 1586) odpowiedziało poprawnie na to pytanie.



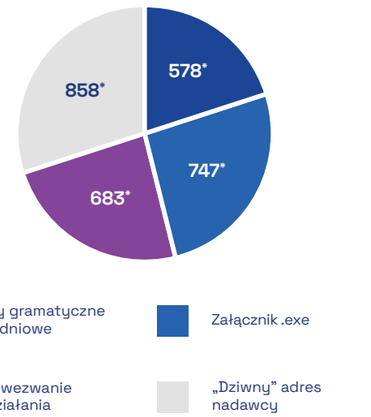
Rysunek 7. Które z poniższych narzędzi obroni mnie najlepiej przed Spear phishingiem? - **Pretest.**

Rysunek 8. Który z poniższych narzędzi obroni mnie najlepiej przed Spear phishingiem?
68% uczestników (687 z 1003) odpowiedziało poprawnie na to pytanie.



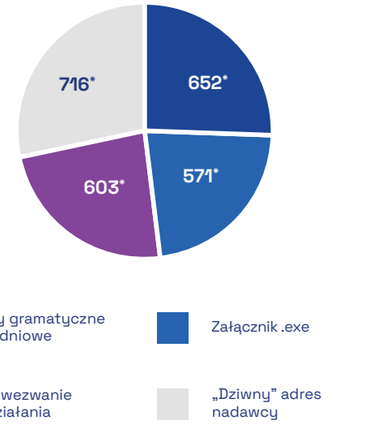
Rysunek 8. Które z poniższych narzędzi obroni mnie,najlepiej przed Spear phishingiem? - **Posttest**.

Rysunek 9. Co może wskazywać na wiadomość phishingową?
15% uczestników (245 z 1586) odpowiedziało poprawnie na to pytanie.



Rysunek 9. Co może wskazywać na wiadomość phishingową? - **Pretest**.

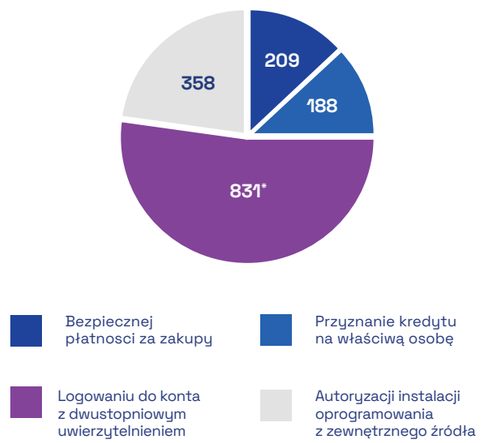
Rysunek 10. Co może wskazywać na wiadomość phishingową?
41% uczestników (411 z 1003) odpowiedziało poprawnie na to pytanie.



Rysunek 10. Co może wskazywać na wiadomość,phishingową? - **Pretest**.

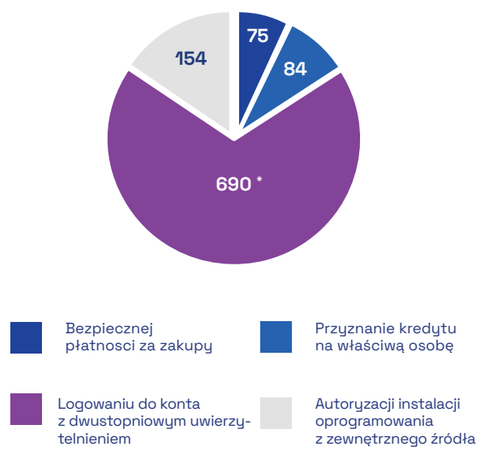
Pytania o najniższym wyniku w preteście:

11. Czemu służy Microsoft Authenticator?
52% uczestników (831 z 1586) odpowiedziało poprawnie na to pytanie.



Rysunek 11. Czemu służy Microsoft Authenticator? - **Pretest.**

12. Czemu służy Microsoft Authenticator?
69% uczestników (690 z 1003) odpowiedziało poprawnie na to pytanie.



Rysunek 14. Czemu służy Microsoft Authenticator? - **Posttestt.**

Pozytywnym wynikiem całego procesu edukacyjnego były odpowiedzi, w których zdiagnozowano największy przyrost wiedzy: Pytania o narzędzia obrony przed Spear phishingiem, rozpoznawanie cech charakterystycznych phishingu oraz działanie programów do dwustopniowej weryfikacji użytkownika. Wskazują one na tendencję do zapamiętywania przez uczestników kluczowych narzędzi w obszarze ochrony swoich danych w sieci, takich jak narzędzia dwustopniowej weryfikacji.

Prywatność w sieci i manipulacje medialne

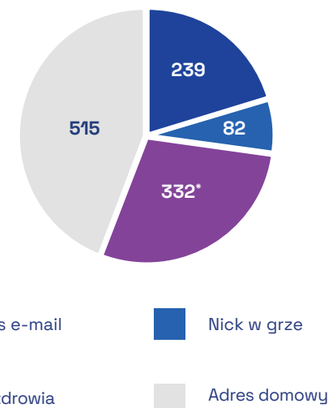
Średnia punktacja pretestu z zakresu prywatności danych i manipulacji wyniosła 2/5 punktów, zaś średnia punktacja posttetsu wyniosła 3,7/5 punktów, co stanowi progres i świadczy o wysokiej efektywności prowadzo nych warsztatów.

Uczniowie największe problemy mieli z określeniem danych wrażliwych/danych osobowych szczególnej kategorii, podaniem nazwy popularnego testy oceny wiarygodności źródeł informacji (Test CRAAP) oraz wymieniem wszystkich zalet posiadania dodatkowego, zanonimizowanego adresu e-mail (szczegółowe dane dostępne są w tabelach na końcu rozdziału).

Poniżej zaprezentowane zostały wybrane pytania oraz wyniki pretestów i posttestów zajęć o prywatności w sieci i manipulacjach medialnych. Wybrane zostały trzy pytania sprawiające największe trudności oraz trzy pytania, w których stwierdzono największy przyrost wiedzy:

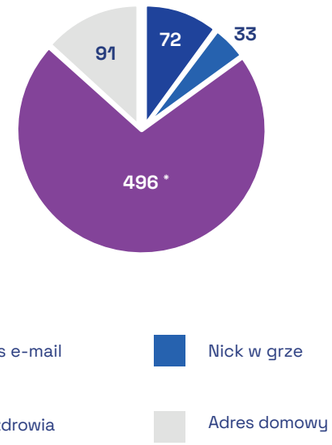
Pytania o najniższym wyniku w preteście:

13. Daną wrażliwą będzie:
28% uczestników (332 z 1168) odpowiedziało poprawnie na to pytanie.



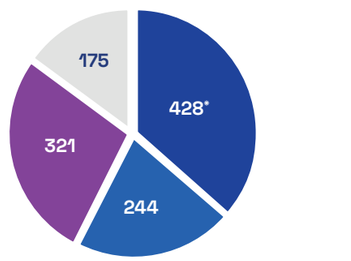
Rysunek 13. Daną wrażliwą będzie: - **Pretest.**

14. Daną wrażliwą będzie:
72% uczestników (496 z 692) odpowiedziało poprawnie na to pytanie.



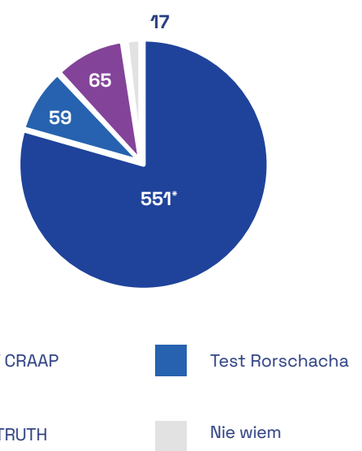
Rysunek 14. Daną wrażliwą będzie: - **Posttestt.**

15. Nazwa (akronim) popularnego testu oceny wiarygodności źródeł informacji to:
37% uczestników (428 z 1168) odpowiedziało poprawnie na to pytanie.



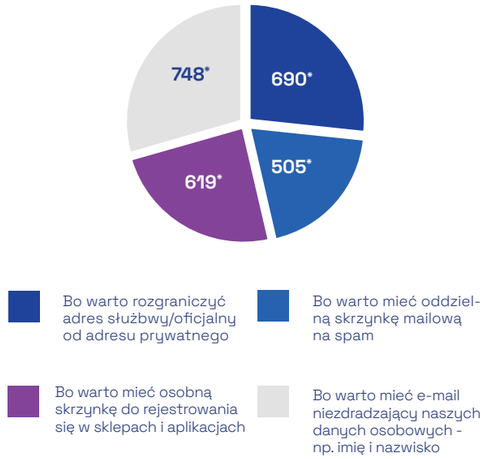
Rysunek 15. Nazwa(akronim) popularnego testu oceny wiarygodności źródeł informacji to: - **Pretest.**

16. Nazwa (akronim)popularnego testu oceny wiarygodności źródeł informacji to:
80% uczestników (551 z 692) odpowiedziało poprawnie na to pytanie.



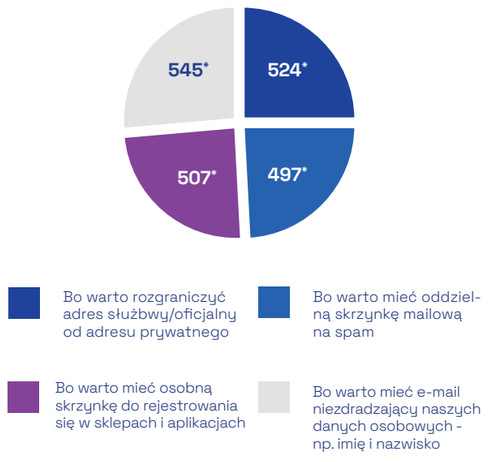
Rysunek 16. Nazwa(akronim) popularnego testu oceny wiarygodności źródeł informacji to: - **Posttestt**

17. Dlaczego warto posiadać dodatkowy, zanonimizowany adres e-mail (wielokrotny wybór)?
29% uczestników (342 z 1168) odpowiedziało poprawnie na to pytanie.



Rysunek 17. Dlaczego warto posiadać dodatkowy, zanonimizowany adres e-mail - **Pretest**.

18. Dlaczego warto posiadać dodatkowy, zanonimizowany adres e-mail (wielokrotny wybór)?
62% uczestników (430 z 692) odpowiedziało poprawnie na to pytanie.



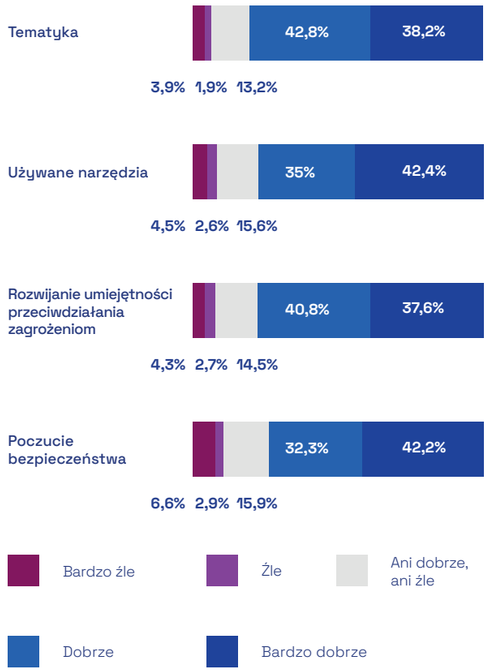
Rysunek 18. Dlaczego warto posiadać dodatkowy, zanonimizowany adres e-mail (wielokrotny wybór)? - Posttest.e-mail (wielokrotny wybór)? - **Pretest.**

Pytania o największym przyroście wiedzy:

Warte zauważenia wydaje się, że w tym temacie, pytania najtrudniejsze tożsame są z pytaniami o największym wskaźniku wzrostu wiedzy. W opinii autorów poniższego raportu, może to wskazywać na dużą wartość edukacyjną zajęć prowadzonych w tym konkretnym temacie.

Po zakończeniu warsztatów z zakresu cyberbezpieczeństwa i prywatności danych i manipulacji, uczniowie wypełniali ankietę ewaluacyjną. Uczniowie bardzo wysoko ocenili jakość zajęć (4,16/5) oraz osoby prowadzące (4,51/5). W ramach ankiety ewaluacyjnej zadano kilka pytań. Pytania wraz z wynikami przedstawiają się następująco:

Jak oceniasz przebieg warsztatów?



Działania warsztatowe wydawały się zatem być dobrze oceniane przez ich uczestników i uczestniczki.

Charakterystyka Testu i Badania

Zwieńczeniem projektu był Ogólnopolski Konkurs i Test Wiedzy „Cyberbezpieczni". Test składał się 27 pytań jednokrotnego wyboru wylosowanych z bazy ok. 200 pytań, obejmujących trzy obszary tematyczne (Bezpieczeństwo Danych, Fake Newsy, Oszustwa Internetowe), o trzech poziomach trudności (łatwy, średni i trudny). Każdy uczestnik otrzymał trzy losowe pytania z każdego z poziomów trudności i z każdego z tematów. Każdy uczestnik odpowiadał zatem na trzy pytania łatwe, trzy pytania średnie i trzy pytania trudne, w każdym z trzech tematów. Razem 27 pytań. Mechanizm ten pozwolił na zachowania losowości pytań przy jednoczesnym równym poziomie dla każdego uczestnika. Za każdą poprawną odpowiedź otrzymywało się 1 punkt. Odpowiedzi nieprawidłowe nie były punktowane.

Cel Testu

Celem testu była ocena poziomu wiedzy uczestników całego projektu Cyberbezpieczni w trzech kluczowych obszarach tematycznych: **Bezpieczeństwo Danych, Fake Newsy oraz Oszustwa Internetowe**. Chcieliśmy zrozumieć, jak dobrze znane są osobom młodym zagadnienia związane z cyberbezpieczeństwem, w tym ochroną danych osobowych, rozpoznawaniem fałszywych informacji oraz zabezpieczeniem przed oszustwami online. Główne pytanie badawcze stanowiło zagadnienie: Które pytania okażą się najtrudniejsze, czyli jakie tematy i zagadnienia okażą się szczególnie kłopotliwe dla uczestników testu oraz z czym mogą wiązać się ewentualne problemy i wyzwania edukacyjne. Z tego powodu Test wiedzy otwarty został dla szeroko rozumianej młodzieży – uczniów szkół podstawowych od 13 roku życia oraz uczniów szkół ponadpodstawowych. Test dostępny był też dla uczestników i uczestniczek warsztatów, jak i młodych odbiorów innych działań projektowych, czyli wszystkich chętnych i zainteresowanych, którzy poprzez działania marketingowe lub kampanie informacyjne dowiedzieli się o projekcie. Test uzupełniony został również o krótką, dobrowolną ankietę pytającą uczestników o podstawowe dane demograficzne, subiektywne poczucie bezpieczeństwa onlinе czy też doświadczenia z różnymi formami cyberprzestępczości. Dodatkowym elementem konkursu, były nagrody rzeczowe, którymi zostali nagrodzeni uczestnicy z najwyższymi wynikami.

Charakterystyka badanej grupy

Ankieta obejmowała uczestników projektu Cyberbezpieczni, będących uczniami i uczennicami szkół podstawowych (od 13 roku życia) i ponadpodstawowych. Choć liczba osób biorących udział w teście przekroczyła trzy tysiące osób, stanowiąc tym samym relatywnie dużą próbę, to niniejszego badania i płynących z niego wniosków nie można traktować jako reprezentatywnego i reprezentatywnych dla całości populacji uczniów w Polsce.

Ze względu na metodę zbierania danych i sposób przeprowadzenia ankiety (pozyskiwanie wiedzy przy okazji testu), próba nie jest losowa. Dobór próby jest przypadkowy – w projekcie wzięły bowiem udział osoby chętne, co już na wstępie zdecydowało o nielosowym doborze grupy. Szczegółowe informacje o uczestnikach badania przedstawione są w podrozdziale „Kim byli uczestnicy testu?". Niniejsze dane i wnioski mogą być jednak wartościowe jako rozbudowana diagnoza największych wyzwań i najtrudniejszych problemów w obszarze cyberbezpieczeństwa, z którymi stykają się (lub nie) młodzi ludzie. Jako takie, badanie to i płynące z niego wnioski powinny być wartościowe dla wszystkich organizacji zajmujących się edukacją w zakresie cyberbezpieczeństwa.

Instrumenty Badawcze

Test jednokrotnego wyboru z 27 pytaniami, losowanymi z trzech obszarów tematycznych i trzech poziomów trudności. Ankieta dotycząca doświadczeń z cyberprzestępczością, postaw wobec bezpieczeństwa oraz oceny programu Cyberbezpieczni.

Przebieg Badania

1. Zgłoszenie do Konkursu i Testu oraz wypełnienie ankiety: Uczestnicy, zgłaszając się do udziału w Ogólnopolskim Konkursie i Teście wiedzy, uzupełnili dobrowolną ankietę, dostarczając informacji dotyczących doświadczeń z cyberprzestępczością, postaw wobec bezpieczeństwa, a także oceny programu Cyberbezpieczni.

2. Przeprowadzenie Testu: Uczestnicy zostali poddani testowi składającemu się z 27 pytań z trzech obszarów tematycznych na trzech poziomach trudności. Każde pytanie miało na celu ocenę konkretnej wiedzy związanej z bezpieczeństwem online, fake newsami lub oszustwami internetowymi.

3. Analiza Wyników: Zebrane dane zostały poddane analizie statystycznej w celu zidentyfikowania największych wyzwań i problemów oraz oceny poziomu wiedzy i doświadczeń uczestników.

4. Raportowanie wyników: Na podstawie analizy danych, przygotowany został raport zawierający istotne statystyki, wnioski oraz rekomendacje dotyczące dalszych działań edukacyjnych.

Badanie ma na celu dostarczenie wglądu w skuteczność projektu Cyberbezpieczni oraz poziom wiedzy i doświadczeń uczestników w obszarze cyberbezpieczeństwa

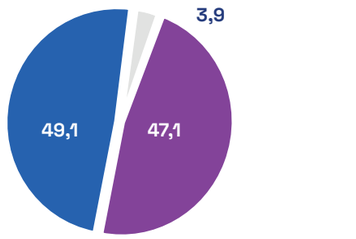
Test wiedzy Cyberbezpieczni wraz z pytaniami ankietowymi

Kim byli uczestnicy testu?

- **Płeć**

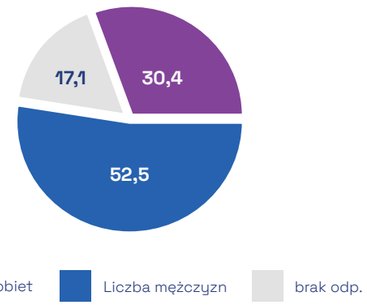
W szkołach podstawowych udział w teście wiedzy mogli wziąć uczniowie powyżej trzynastego roku życia. Według deklaracji uczestników, **328 osób** stanowiły kobiety, a **342 osoby** stanowili mężczyźni. **27 osób** nie udzieliło odpowiedzi na to pytanie.

Procentowy udział płci w badaniu dla szkół podstawowych:



W szkołach ponadpodstawowych widoczne są większe różnice. Według deklaracji uczestników, **880 osób** stanowiły kobiety, a **1517 osób** stanowili mężczyźni. **493 osoby** nie udzieliły odpowiedzi na to pytanie.

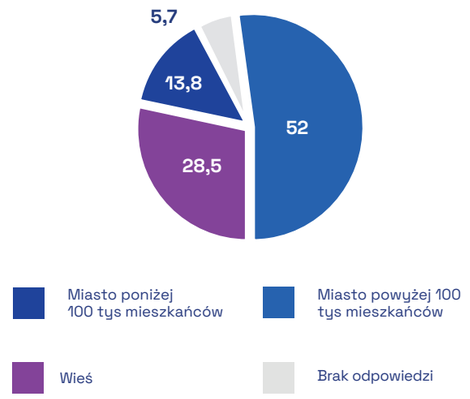
Procentowy udział płci w badaniu dla szkół ponadpodstawowych:



- **Miejsce zamieszkania**

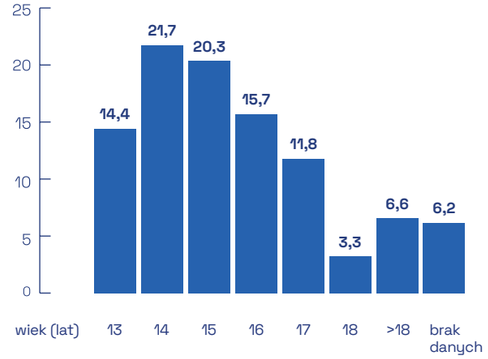
Procentowy podział ze względu na miejsce zamieszkania wskazywał, że uczestnikami testu i konkursu byli przede wszystkim mieszkańcy miast poniżej 100 tys. mieszkańców.

Procentowy udział Procentowy podział ze względu na miejsce zamieszkania:



- **Wiek uczestników**

Procentowy rozkład wieku uczestników



Kim byli uczestnicy testu - podsumowanie

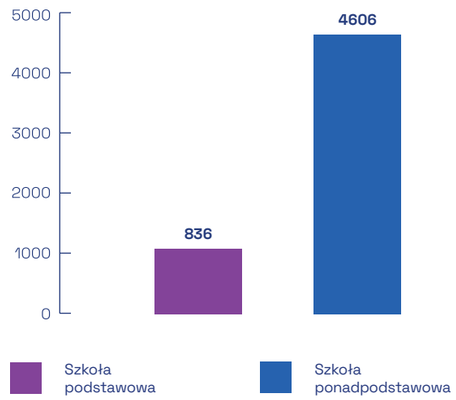
Warto zwrócić uwagę, że uczestnikami testu byli przede wszystkim uczniowie szkół ponadpodstawowych, a także na problem potencjalnej nadreprezentacji mężczyzn wśród uczestników projektu. Mała liczba uczniów szkół podstawowych może być tłumaczona tym, że zarówno konkurs jak i test wiedzy dostępne były dla uczestników od 13 roku życia, czyli dla uczniów kończących ten etap edukacji. Z tego też powodu, w dalszych wykresach nie wprowadzaliśmy rozróżnienia na szkoły podstawowe i ponadpodstawowe oraz posługujemy się zbiorczym określeniem „Uczestnicy testu" lub „młodzież biorąca udział w projekcie". Potencjalny problem nadreprezentacji mężczyzn wymaga dalszych badań. Może on bowiem wynikać z braku innych opcji odpowiedzi w kwestionariuszu lub chęci zanonimizowania tej danej (aż 17,1% uczestników w grupie szkół ponadpodstawowych nie zaznaczyła żadnej odpowiedzi w kwestionariuszu). Może być to jednak bardziej znaczącym problemem sygnalizującym potrzebę dalszego zbadania i konkretnych działań (więcej o tym, w rekomendacjach).

Wyniki testu wiedzy

Liczba podejść do testu

Każdy uczestnik mógł podejść do testu wiedzy trzykrotnie. W szkołach podstawowych, przy 697 uczestnikach, **wpłynęło 836 wyników,** dając średnią 1,2 podejścia na uczestnika. W szkołach ponadpodstawowych, na **2890 uczestników**, zarejestrowano **4606 wyników** testu, co daje średnią 1,6 podejścia na uczestnika.

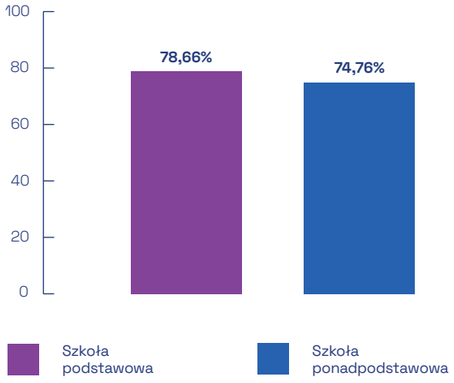
Liczba podejść do testu



Średnie procentowe wyniki testu:

Szkoła podstawowa **78,68%**

Szkoła ponadpodstawowa - **74,76%**



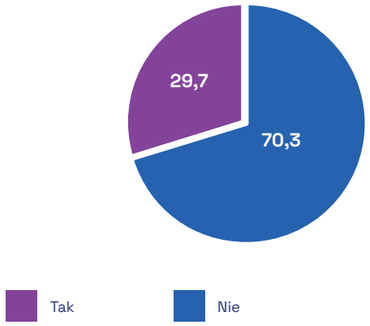
Wyniki testu wiedzy – podsumowanie

Średnie procentowe wyniki testu wskazują na wyższy wynik po stronie szkół podstawowych. Trzeba przy tym jednak pamiętać, że porównywanie obu wyników nie jest miarodajne ze względu na dwie różne bazy pytań. Baza pytań dla szkół ponadpodstawowych zawierała często pytania trudniejsze i bardziej zaawansowane.

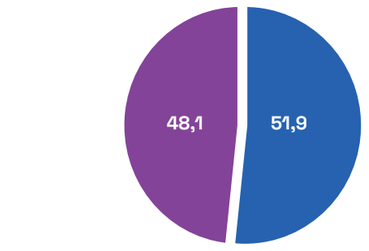
Doświadczenie z cyberprzestępczością

W ankiecie, zapytaliśmy również uczestników testu o dotychczasowe doświadczenia z cyberprzestępczością. Wyniki prezentują odsetek odpowiedzi na poszczególne pytania.

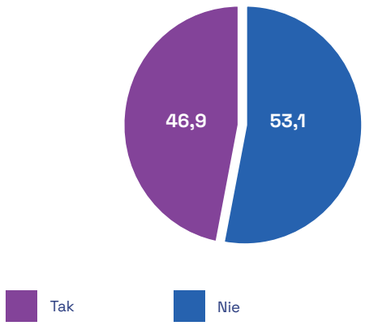
Czy doświwiadczyłeś/łaś kiedyś phishingu?



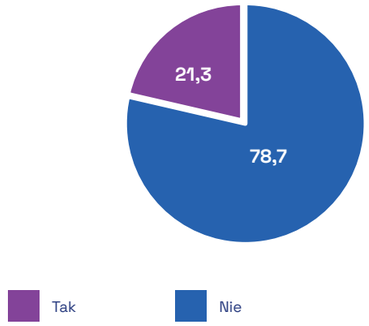
Czy doświwiadczyłeś/łaś kiedyś złośliwego oprogramowania?



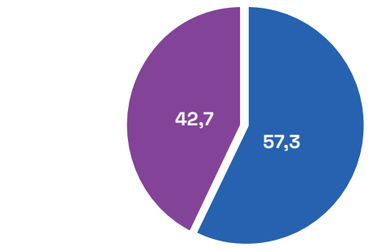
Czy doświwiadczyłeś/łaś kiedyś włamania na konto?



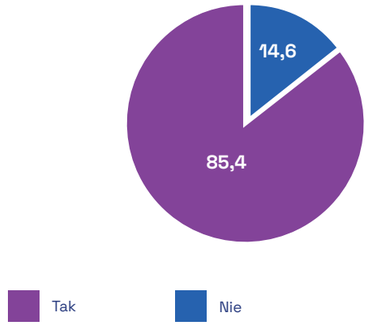
Czy doświwiadczyłeś/łaś kiedyś wycieku danych?



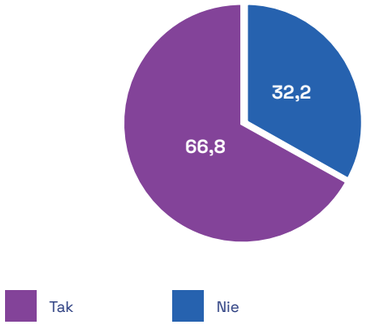
Czy doświwiadczyłeś/łaś kiedyś manipulacji medialnych?



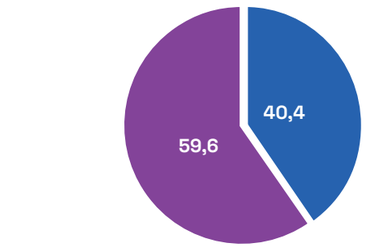
Czy doświwiadczyłeś/łaś kiedyś fake newsów?



Czy doświwiadczyłeś/łaś kiedyś mowy nienawiści?



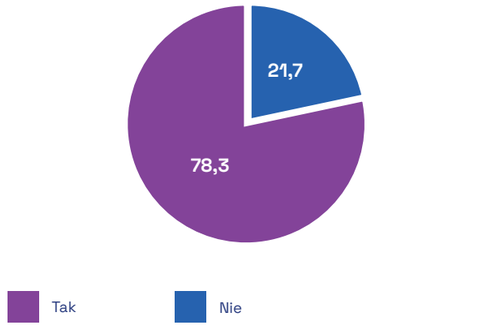
Czy doświwiadczyłeś/łaś kiedyś hejtu w sieci?



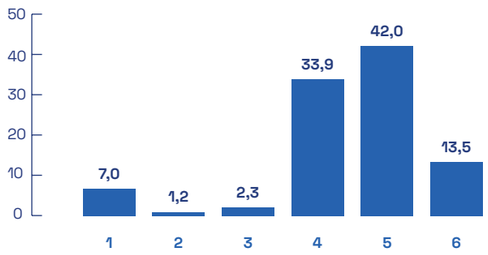
Znaczącą obserwacją może być wskazanie, że większość ankietowanych uczestników projektu deklarowała, że nie doświadczyła sytuacji naruszeń cyberbezpieczeństwa takich jak włamanie na konto, wyciek danych, złośliwe oprogramowanie czy phishing. Ponad połowa uczestników projektu deklarowała natomiast doświadczenie hejtu w sieci **(59,6%)**, mowy nienawiści **(66,8%)** oraz fake newsów **(85,4%)**. Ponownie, może to wskazywać na potrzebę dalszych badań i procesów diagnostycznych, nakierowanych w szczególności na doświadczenia różnych form cybeprzemocy, jak i na potrzebę uzupełnienia programów edukacyjnych o powyższe obszary tematyczne.

Poczucie bezpieczeństwa

Czy miałeś/łaś już zajęcia o cyberbezpieczeństwie w szkole?



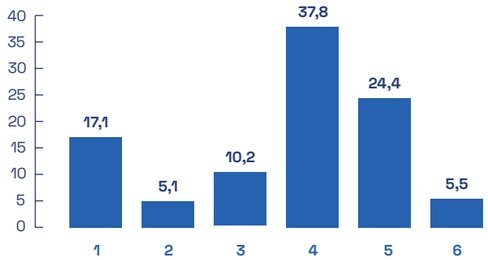
Czy jesteś poinformowany o cyberzagrożeniach?



1. nie mam zdania **2.** nie zgadzam się **3.** raczej się nie zgadzam

4. raczej się zgadzam **5** zgadzam się **6.** brak odpowiedzi

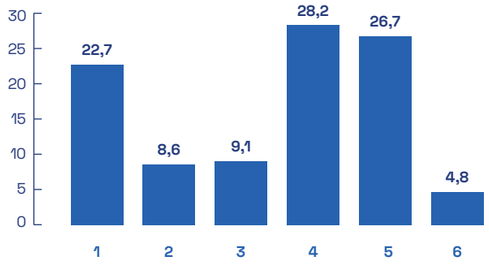
Czy uważasz, że Twoje dane są odpowiednio chronione przez usługi online, których używasz?



1. nie mam zdania **2.** nie zgadzam się **3.** raczej się nie zgadzam

4. raczej się zgadzam **5** zgadzam się **6.** brak odpowiedzi

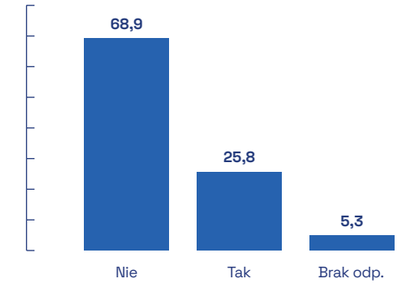
Czy uważasz, że szkoła odpowiednio przygotowała Cię do dbania o swoje bezpieczeństwo w sieci?



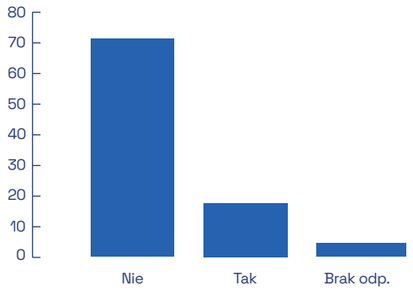
1. nie mam zdania **2.** nie zgadzam się **3.** raczej się nie zgadzam

4. raczej się zgadzam **5** zgadzam się **6.** brak odpowiedzi

Czy pytasz rodziców lub opiekunów prawnych o porady dotyczące bezpiecznego korzystania z Internetu?



Czy pytasz nauczycieli o porady dotyczące bezpiecznego korzystania z Internetu?



Doświadczenie z cyberprzestępczością i poczucie bezpieczeństwa – podsumowanie

Zebrane odpowiedzi uczestników projektu wskazują, że stosunkowo dobrze oceniają oni swoją wiedzę oraz to, w jaki sposób szkoła przygotowała ich do dbania o swoje cyberbezpieczeństwo.

Pewnym wyzwaniem wymagającym dalszego zbadania może być kwestia tego, do kogo uczestnicy projektu zwracają się o porady dotyczące bezpiecznego korzystania z Internetu. W ankiecie zapytaliśmy uczestników o zwracanie się po porady dotyczące bezpiecznego korzystania z Internetu do nauczycieli lub rodziców (nawiązując do triady uczeń-rodzic-nauczyciel, stanowiącej podstawowych odbiorców dotychczasowych działań projektowych).

Naszym celem było zweryfikowanie, która część triady ma w tym temacie największy autorytet wśród uczniów. W zadeklarowanych przez uczestników odpowiedziach nie są to jednak ani rodzice (prawie **70%** uczestników nie pyta ich o porady) ani nauczyciele(ponad **70%** uczestników nie pyta ich o porady). Jednocześnie, większość uczestników pozytywnie ocenia działania szkoły w obszarze edukacji o cyberbezpieczeństwie (**28,2%** uczestników „raczej zgadza się", a **26,7%** „zgadza się" z tezą, że szkoła odpowiednio przygotowała ich do dbania o swoje bezpieczeństwo w sieci).

Pytanie o inne autorytety w obszarze cyberbezpieczeństwa jest zatem zagadnieniem wymagającym dalszych badań, jak również ważnym pytaniem, które powinny zadać sobie organizacje zajmujące się edukacją w tym zakresie.

Największe wyzwania w obszarze Cyberbezpieczeństwa

Jednym z głównych celów Ogólnopolskiego Testu Wiedzy było znalezienie najtrudniejszych pytań i największych problemów (z perspektywy uczestników projektu) związanych z cyberbezpieczeństwem. Po przeanalizowaniu bazy ok. **200 pytań**, zidentyfikowano pytania, które sprawiły uczestnikom testu największe trudności. Lista tych pytań wskazuje to na to, że młodzi uczestnicy projektu wykazują się dość rozległą wiedzą z zakresu Cyberbezpieczeństwa, Mediów społecznościowych i Fake Newsów. Uczestnicy testu dobrze radzili sobie z pytaniami dotyczącymi częstych zagrożeń oraz pytaniami dotyczącymi właściwych sposobów postępowania w danej sytuacji (stanowiącej

naruszenie cyberbezpieczeństwa). Najtrudniejszymi pytaniami okazały się natomiast te, zawierające specjalistyczne słownictwo i terminologię:

- **Co to jest enkrypcja?**
- **Co to jest Keylogger?**
- **Co to jest Jailbreak (w odniesieniu do urządzeń Apple)?**
- **Co to jest koperta SSL?**
- **Jakie korzyści płyną z korzystania z programów typu Sandbox?**
- **Co oznacza „feeds reboot”?**
- **Co to jest factcheckingowe narzędzie „CRAAP”?**
- **Czym jest rozejście się informacji (echo chamber)?**
- **Co to jest botnet?**
- **Co oznacza wyrażenie „zero-day exploit”**
- **Czym jest atak typu „spoofing”**
- **Co to jest „clickjacking”**

Wiele z tych terminów stanowi albo istotne zagrożenia albo skuteczne sposoby i narzędzi do zwiększenia swojego cyberbezpieczeństwa w sieci. W dalszej części raportu, poprosiliśmy zatem o ich omówienie ekspertów merytorycznych zaangażowanych w projekt.

Wyjaśnienia ekspertów:

Enkrypcja

Enkrypcja to proces przekształcania czytelnych danych (tekstu, plików, informacji) w sposób, który utrudnia lub uniemożliwia nieupoważnionym osobom dostęp do ich treści. Jest to technika stosowana w celu ochrony poufności danych i zabezpieczenia przed nieautoryzowanym dostępem.

W procesie enkrypcji dane oryginalne, nazywane tekstem jawnym, są przekształcane za pomocą algorytmu matematycznego i klucza szyfrującego w dane zaszyfrowane, zwane tekstem szyfrogramu. Proces odwrotny, nazywany deszyfrowaniem, polega na przywróceniu oryginalnych danych z tekstu zaszyfrowanego i wymaga posiadania odpowiedniego klucza deszyfrującego.

Enkrypcja jest szeroko stosowana w dziedzinie bezpieczeństwa informatycznego, zwłaszcza w transmisji danych przez Internet, przechowywaniu poufnych informacji, takich jak dane użytkowników, oraz w ochronie komunikacji między różnymi systemami. Istnieje wiele różnych algorytmów i metod enkrypcji, a bezpieczeństwo systemów zależy często od stosowania odpowiednich protokołów i kluczy szyfrowania.

Marek Grzywna

Koperta SSL

Termin „koperta SSL” odnosi się do **procesu szyfrowania danych** przesyłanych między użytkownikiem a serwerem internetowym za pomocą protokołu SSL/TLS. SSL (Secure Sockets Layer) i jego następca, TLS (Transport Layer Security), to protokoły kryptograficzne używane do zabezpieczania komunikacji internetowej. Koperta SSL (ang. SSL envelope) to metafora, która opisuje, jak te protokoły zapewniają bezpieczne środowisko dla przesyłanych danych.

W skrócie, proces ten działa następująco:
Handshake SSL/TLS: Kiedy użytkownik łączy się z serwerem, zachodzi tzw. **„handshake”** SSL/TLS. W tym procesie następuje wymiana kluczy kryptograficznych między użytkownikiem a serwerem. Klucze te są używane do zabezpieczenia dalszej komunikacji.

Szyfrowanie danych: Po ustanowieniu bezpiecznego połączenia, dane przesyłane między użytkownikiem a serwerem są szyfrowane. Oznacza to, że nawet jeśli ktoś przechwyciłby te dane, nie byłby w stanie ich zrozumieć bez klucza deszyfrującego.

Integralność danych: Protokoły SSL/TLS zapewniają również integralność danych, co oznacza, że nie można ich modyfikować podczas transmisji. Jeśli dane zostałyby zmienione lub sfałszowane, to zostanie to zauważone.

W ten sposób koperta SSL tworzy bezpieczne środowisko dla przesyłania danych przez Internet, chroniąc je przed nieautoryzowanym dostępem i przechwytywaniem. Współcześnie, zwłaszcza po kilku aktualizacjach, zaleca się korzystanie z TLS, który jest bardziej bezpieczną wersją protokołu, niż SSL. Termin „koperta SSL” jest więc często używany ogólnie, nawet jeśli protokół TLS jest właściwy.

Marek Grzywna

Rozejście się informacji (echo chamber)

Pojęcie echo chamber w kontekście społecznym lub medialnym, wskazuje na sytuację, w której ludzie koncentrują się na informacjach, które potwierdzają ich własne przekonania, jednocześnie odrzucając lub ignorując różne perspektywy. W takim przypadku, „rozejście się informacji” związane jest z tym, jak grupa ludzi wchodzi w środowisko myślowe, gdzie dominują pewne przekonania lub ideologie, a różnorodność poglądów jest minimalizowana. To zjawisko może występować zarówno w tradycyjnych mediach, jak i w mediach społecznościowych, gdzie algorytmy dostosowują prezentowane treści do wcześniejszych preferencji użytkowników.

Termin ten można interpretować jako opis zjawiska, w którym ludzie skupiają się na informacjach zbieżnych z ich własnymi przekonaniami, co prowadzi do pewnej izolacji od różnorodności poglądów.

Marek Grzywna

Jailbreak

W odniesieniu do systemu iOS, jest to proces usuwania ograniczeń systemu na danym urządzeniu, w celu nadania użytkownikowi urządzenia większych uprawnień. W praktyce jest to proces pozwalający użytkownikowi danego urządzenia np. na instalację aplikacji spoza App Store czy też dowolne dostosowanie interfejsu urządzenia do własnych potrzeb. Jest to jednak proces „otwierający” system na potencjalne ataki. Instalowana przez nas aplikacja z innego źródła może bowiem zawierać np. malware. Choć jailbreak może być dosyć prostym i popularnym zabiegiem, trzeba być świadomym związanych z nim zagrożeń.

Zbigniew Bujak

Feeds Reboot

Feeds Reboot to termin wymyślony przez Davida Pierce’a, w artykule **Your internet life needs a Feeds Reboot — here’s how to do it.** Oznacza on “restartowanie” naszych algorytmów w mediach społecznościowych by chronić się przed nadmiernym/błędnym profilowaniem oraz zjawiskiem „bańki informacyjnej”. David Pierce proponuje kilka działań składających się na Feeds Reboot, takich jak: przegląd obserwowanych stron i profili, porządki w treściach do przeczytania/na później oraz resetowanie i modyfikowanie ustawień algorytmów w konkretnych mediach społecznościowych (modyfikacje opcji „zainteresowań” lub wyświetlanych reklam). Okazjonalny Feeds Reboot pomaga budować świadomość na temat zjawiska coraz dalej idącego profilowania naszych zachowań w mediach społecznościowych, a także pozwala nam na poznanie i modyfikację informacji, które zebrały o nas algorytmy.

Zbigniew Bujak

CRAAP

Test CRAAP to narzędzie weryfikacji i oceny prawdziwości informacji znajdowanych w sieci. Składa się on z listy pytań pozwalających ocenić aktualność (Currency), istotność (Relevance), źródło (Authority), poprawność (Accuracy) oraz cel (Purpose) danej informacji. Jest to narzędzie wykorzystywane na gruncie akademickim (do oceny wiarygodności źródeł), ale może być z sukcesem wykorzystywane w analizowaniu i wykrywaniu fake newsów i dezinformacji w sieci.

Zbigniew Bujak

Zero-day exploit

To pojęcie składa się z dwóch części - „zero day” oraz „exploit”. Termin „zero day” oznacza istnienie takiej wady oprogramowania, która albo nie jest jeszcze znana, albo nie została jeszcze naprawiona. Innymi słowy jest to „dziura” w oprogramowaniu, która może być użyta do ataków i niestety nie mamy na to obrony w danym momencie (poprawka dopiero jest w drodze).

„Zero day" bierze się stąd, że producenci lub użytkownicy mają dosłownie zero dni na zareagowanie na zagrożenie. Słowo „Exploit" pochodzi od ang. „exploit" – wykorzystać.

Jest to program albo kod, który wykorzystuje jakiś błąd w oprogramowaniu aby narobić szkód. Ten program może być wprowadzony do kodu przez przestępcę, może być podesłany użytkownikowi w wiadomości e-mail, może być skryptem działającym na stronie internetowej itd.

Podsumowując – **„zero-day exploit"** oznacza taki program lub kod, na którego w danym momencie nie ma poprawki.
Przed exploitami zero day właściwie nie ma 100% ochrony, ale można znacznie zmniejszyć zagrożenie stosując się do następujących porad:

- **Aktualizuj swoje oprogramowanie tak szybko i często jak to możliwe (chodzi o to, by jak najszybciej wprowadzić poprawki i zmniejszyć czas wystawienia naszego komputera na exploity)**
- **Unikaj zachowań ryzykownych (np. instalowania na komputerze programów niewiadomego pochodzenia).**

Niebezpiecznik.pl

Spoofing

Słowo „spoofing" (od angielskiego „spoof" – bujda, szachrajstwo) często jest używane jako określenie ataku. Tak naprawdę oznacza ono coś innego – zmienianie informacji o nadawcy danego komunikatu.

Spoofigniem możemy zatem nazwać:
- **Fałszowanie informacji o nadawcy komunikatu w wiadomościach e-mail.**
- **Wyświetlanie użytkownikowi telefonu fałszywej informacji o numerze osoby dzwoniącej.**
- **Wyświetlanie użytkownikowi telefonu fałszywej informacji o nadawcy SMS-a.**
- **Wszelkie inne sytuacje, w których dochodzi do podmianki prawdziwej informacji o nadawcy jakiejś informacji lub komunikatu.**

Jeśli słowa «spoofing» używamy na określenie ataku to mamy na myśli wszelkie rodzaje działań, w których ktoś podszywa się pod inną osobę lub organizację, aby wyłudzić dane, pieniądze lub zrobić coś szkodliwego.
Niektóre rodzaje spoofingu mogą być wykrywalne (np. Spoofing mailowy), ale wymaga to złożonych czynności. Dlatego najlepiej jest przyjąć jedną, prostą zasadę bezpieczeństwa. Jeśli dostajesz jakąś wiadomość mailem, telefonicznie lub przez SMS i nadawca tej wiadomości chce abyś coś zrobił, musisz potwierdzić tożsamość nadawcy kontaktując się z nim osobiście. Możesz przykładowo zadzwonić do danej osoby (firmy, urzędu) i spytać, czy faktycznie ta osoba nadała daną wiadomość. Ważne jest to, abyś to TY wykonał połączenie do danej osoby. Najpewniejszym sposobem jest potwierdzenie telefoniczne.

Niebezpiecznik.pl

Clickjacking

Clickjacking to rodzaj oszustwa, który polega na ukrywaniu złośliwego linku pod atrakcyjnym przyciskiem lub grafiką na stronie internetowej. Co jednak ważne, przy typowym clickjackingu ofiara sądzi, że przegląda znaną i zaufaną stronę internetową. Bardzo często odbywa się to w taki sposób, że na stronę legalną (np. Na facebooka) nałożona jest niewidoczna «nakładka» (iframe), a użytkownik tego nie wie (zob. https://niebezpiecznik.pl/symantec/clickjacking-na-facebooku/). Czasami clickjacking nie wyrządza wielkich szkód, a służy np. Pozyskaniu tzw. Like'ów dla stron wykorzystywanych przez oszustów. Może być jednak użyty w celu przekierowania użytkownika na bardziej szkodliwe treści. Aby się przed clickjackingiem chronić, należy być nieufnym wobec nieznanych lub podejrzanych stron internetowych. Nie powinniśmy «klikać» w treści, jeśli nie jesteśmy pewni kto je dostarcza i co się za nimi kryje. Dodatkowym zabezpieczeniem (potrzebnym również z innych powodów) będzie posiadanie oprogramowania antywirusowego oraz jak najczęstsze i najszybsze aktualizowanie oprogramowania.

Niebezpiecznik.pl

Sandbox

Słowo Sandbox (ang. piaskownica) oznacza stworzenie w programie bezpiecznego, oddzielnego środowiska, w którym można uruchamiać nieznane lub podejrzane pliki i programy nie ryzykując uszkodzenia systemu. Programy lub pliki działające w „piaskownicy" nie mają wszystkich uprawnień, nie mają pełnego dostępu do zadań systemu, pełnego dostępu do sieci albo urządzeń peryferyjnych podłączonych do komputera. Istnieją zarówno „piaskownice" w postaci programów na komputery (np. Sandboxie) jak i działające w chmurze. W pewnym sensie z dobrodziejstw piaskownicy korzystamy również wtedy, gdy przeglądamy zasoby dysków sieciowych (możemy np. zapoznać się z treścią dokumentu w przeglądarce, bez pobierania go na komputer).

Niebezpiecznik.pl

Keylogger

Keylogger to po prostu **program, który zapisuje znaki wprowadzane z klawiatury**. Bardzo często keyloggery są programami złośliwymi instalują się bez wiedzy użytkownika, „nasłuchują" znaki z klawiatury i przesyłają informację na ich temat do swojego twórcy. W ten sposób może dochodzić do wykradania danych poufnych, w tym haseł. Keyloggerom należy przede wszystkim zapobiegać, a zatem należy mieć oprogramowanie antywirusowe i aktualny system.

Dodatkowym zabezpieczeniem przed keyloggerem może być użycie tzw. klawiatur ekranowych, czyli wprowadzania hasła myszą na wirtualnej klawiaturze wyświetlonej na ekranie (niektóre banki oferują taką możliwość). Pamiętajmy jednak, że jest jeszcze jeden i to lepszy sposób, by haseł nie wpisywać. Menedżery haseł nie tylko pamiętają nasze hasła i ułatwiają zarządzanie nimi, ale zwalniają nas z konieczności wpisywania ich z klawiatury. Dlatego właśnie menedżery haseł chronią również przed tym zagrożeniem.

Niebezpiecznik.pl

Botnet

Botnet to sieć komputerów zainfekowanych złośliwym oprogramowaniem. Sieć ta znajduje się pod kontrolą przestępców i może być wykorzystywana do różnych celów, takich jak wysyłanie spamu, kradzież danych, kopanie kryptowalut czy przeprowadzanie ataków DDoS. Jeśli Twój komputer zostanie zainfekowany i stanie się częścią botnetu to – niestety – nie będzie on pracował już tylko dla Ciebie. Część jego mocy zostanie przeznaczona na rzecz botnetu, a Ty będziesz miał powolny, kiepsko działający sprzęt, który w dodatku będzie używany do szkodzenia innym.

Aby temu zapobiec:

- **miej aktualne oprogramowanie antywirusowe**
- **nie otwieraj załączników i wiadomości od byle kogo,**
- **nie instaluj oprogramowania nieznanego pochodzenia,**
- **zadbaj o firewall,**
- **monitoruj wydajność komputera, jego zużycie zasobów i aktywność sieciową.**

Niebezpiecznik.pl

Atak IDN homograph

Atak IDN homograph polega na tym, że użytkownikowi wyświetlany jest fałszywy adres strony, który wygląda jak prawdziwy, ale zawiera znaki z innego alfabetu. Atak ten jest możliwy, ponieważ istnieją sposoby na tworzenie adresów internetowych zawierających znaki greckie, rosyjskie, hebrajskie czy armeńskie. Niektóre z tych znaków są bardzo do siebie podobne np. Litera «o» w cyrylicy wygląda identycznie jak litera «o» w alfabecie łacińskim, ale technicznie rzecz biorąc są to inne znaki. W cyrylicy litera «r» wygląda podobnie do naszego «p», a litera «u» przypomina łacińskie «y».

- Aby zobaczyć jak to działa, możesz zrobić proste doświadczenie. Wpisz do paska adresu w przeglądarce adres xn—niebezpiecznikwka-tyb.pl . Zobaczysz, że w pasku pojawi się

słowo «niebezpiecznikówka». Aby osiągnąć ten efekt użyliśmy tzw. Punycode, czyli sposobu kodowania znaków Unicode za pomocą dodatkowych liter, cyfr i myślników.

Przestępcy mogą Ci podrzucać adresy, które po załadowaniu do przeglądarki wyglądają bardzo wiarygodnie, a jednak składają się z innych liter niż sądzisz. Najlepiej chronić się przed tym atakiem poprzez sprawdzanie adresów stron, które odwiedzacie. Nie sprawdzaj ich jednak po załadowaniu się strony, ale jeszcze zanim klikniesz adres. Najedź na link, w który chcesz kliknąć i rzuć okiem na lewy dolny róg przeglądarki. Wyświetli się tam adres, który masz odwiedzić (w razie użycia punycode, będziesz widział myślniki i dodatkowe znaki).

Dodatkowo jednak pamiętaj, aby nigdy, przenigdy, nie logować się na stronach, na które ktoś skierował Cię przez link lub przycisk. Na strony logowania najlepiej jest wchodzić przez zakładkę we własnej przeglądarce.

Niebezpiecznik.pl

Wnioski i rekomendacje

Wnioski

Analiza procentowego udziału płci w badaniu wykazuje, że liczba mężczyzn (52,5%) przewyższa liczbę kobiet (30,4%), co może być wynikiem brakiem innych opcji w kwestionariuszu lub chęcią anonimizacji tej konkretnej danej przez uczestników/uczestniczki. Może to jednak również wskazywać na istotne zróżnicowanie między płciami w kontekście zainteresowania tematyką cyberbezpieczeństwa. Zagadnienie to wymaga zatem dalszych badań i dalszej weryfikacji, a na gruncie działań edukacyjnych większej uwagi ze strony różnych organizacji. Warto przyjrzeć się metodom warsztatowym oraz metodom promocji działań edukacyjnych pod kątem nieumyślnego utrwalania stereotypów lub podziałów płciowych. W przypadku potwierdzenia tych wyników w kolejnych badaniach, działaniach edukacyjnych, warto rozważyć przyjęcie strategii skierowanych do zwiększenia zainteresowania dziewcząt tą dziedziną, przy użyciu dedykowanych warsztatów oraz kampanii informacyjnych.

- Większość respondentów pochodzi z miast poniżej 100 tys. mieszkańców (52%), co może wynikać z lepszego dostępu do zasobów edukacyjnych. Najrzadszą grupą są natomiast mieszkańcy wsi (13,8%). W celu skutecznego dostarczania edukacji z zakresu cyberbezpieczeństwa, konieczne jest rozszerzenie programów edukacyjnych na obszary wiejskie oraz mniejsze miejscowości lub mocniejszy akcent kładziony na promocję programu poza dużymi ośrodkami miejskimi.

- Analiza doświadczeń uczestników z cyberzagrożeniami ukazuje zróżnicowanie w ich doświadczeniach. Istnieje potrzeba dostosowania programów edukacyjnych w celu uwzględnienia indywidualnych doświadczeń uczestników, co wpłynie na ich poziom świadomości w zakresie cyberbezpieczeństwa, fake newsów i mediów społecznościowych.

- Chociaż większość uczniów uważa, że szkoła skutecznie ich przygotowała do dbania o bezpieczeństwo w sieci, istnieją uczestnicy (nieco ponad 15%), którzy mają wątpliwości lub nie wyrazili jednoznacznej opinii na ten temat. Konieczne jest dostosowanie programu do różnych poziomów doświadczenia uczniów.

- Badanie ukazuje, że zdecydowana większość uczniów nie konsultuje się z rodzicami i nauczycielami w kwestiach bezpiecznego korzystania z Internetu. Programy edukacyjne powinny uwzględniać inne formy autorytetów dla młodych w tej dziedzinie.

Rekomendacje

- Ekspansja programów edukacyjnych na obszary wiejskie, mająca na celu zagwarantowanie równego dostępu do wiedzy o cyberbezpieczeństwie dla uczniów z różnych środowisk.

- Równoległe rozwijanie programów edukacyjnych dotyczących ochrony danych osobowych, mowy nienawiści i hejtu aby zwiększyć świadomość uczestników na temat ryzyka związanego z przetwarzaniem ich informacji online oraz formami cyberprzemocy.

- Dostosowanie programów edukacyjnych do indywidualnych potrzeb uczniów, biorąc pod uwagę różnice w doświadczeniach z cyberprzestępczością i poziomie wiedzy na temat bezpieczeństwa online.

- Prowadzenie spotkań z rodzicami i nauczycielami w celu informowania ich o treściach programów edukacyjnych oraz zachęcanie do aktywnego udziału w procesie edukacji.

- Systematyczne przeprowadzanie ewaluacji programów edukacyjnych w celu monitorowania ich skuteczności i dostosowania do zmieniających się potrzeb uczniów.

- Prowadzenie kampanii promocyjnych obejmujących plakaty, ulotki, prezentacje i media społecznościowe w celu zwiększenia świadomości programów edukacyjnych wśród

Co dalej?

Efekty programu Cyberbezpieczni to nie tylko zakończone warsztaty i szkolenia dla nauczycieli, ale również gotowe do wykorzystania materiały edukacyjne dla nauczycieli i rodziców. Zachęcamy do zapoznania się ze scenariuszami zajęć dostępnych na licencji Creative Commons oraz z ulotką dla rodziców, dostępną na stronie projektu: https://fundacjapfr.pl/cyberbezpieczni.html

Mamy nadzieję, że przygotowane przez nas działania, materiały, a także wnioski i rekomendację okażą się pomocne dla wszystkich nauczycieli, rodziców i organizacji zajmujących się edukacją w zakresie bezpieczeństwa dzieci i młodzieży w sieci.

Fundacja Polskiego Funduszu Rozwoju

Fundacja Polskiego Funduszu Rozwoju to organizacja non-profit utworzona w 2018 roku przez Polski Fundusz Rozwoju. Fundacja realizuje swoje zadania statutowe poprzez działania i projekty z zakresu edukacji poprzez własne projekty, wspieranie inicjatyw społecznych (granty i darowizny) i wolontariat pracowniczy. Główny cel tych projektów to przeciwdziałanie wykluczeniu cyfrowemu, wyrównywanie szans edukacyjnych, wyrównywanie szans na rynku pracy różnych grup społecznych – w tym dzieci zamieszkujących tereny Polski wschodniej, dzieci-wychowanków ośrodków wychowawczych i pieczy zastępczej oraz seniorów – poprzez programy edukacyjne bazujące na nowych technologiach.

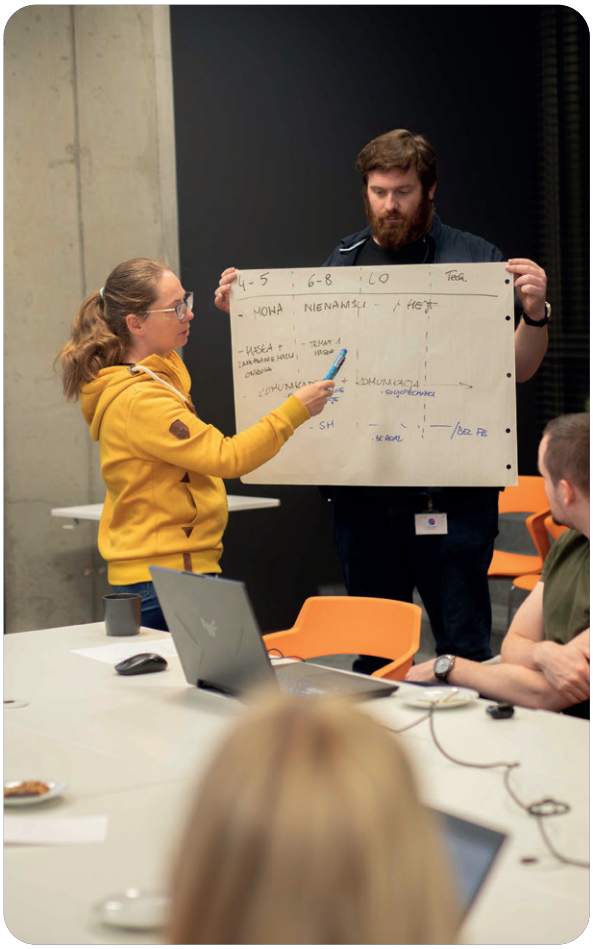
Fundacja realizuje szereg inicjatyw edukacyjnych, a największą z nich jest Centralny Dom Technologii, czyli unikatowy w skali kraju projekt, łączący świat nauki, technologii i biznesu. Centralny Dom Technologii tworzy zespół edukatorów i ekspertów nowoczesnej edukacji opartej na metodologii STEAM. W Centralnym Domu Technologii, mieszczącym się w Warszawie, organizowane są wydarzenia, projekty partnerskie, ale głównym i najważniejszym obszarem działalności są zajęcia warsztatowe stacjonarne i online dla dzieci, młodzieży i dorosłych, w tym także dla osób starszych.

Dodatkowe obszary działalności Fundacji to wspieranie innowacyjności, przedsiębiorczości, motywowanie do zwiększania kompetencji przez całe życie, budowanie postaw prospołecznych i aktywizacja zawodowa. Podstawowe grupy odbiorców działań realizowanych przez Fundację to dzieci, młodzież oraz osoby starsze, jednakże naszym celem jest stworzenie całego ekosystemu dobrych praktyk i zaangażowanych instytucji, tak aby realizowane projekty miały realny wpływ na życie beneficjentów Fundacji. W ramach realizacji swoich celów statutowych Fundacja PFR tworzy własne autorskie projekty, ale także przystępuje do Partnerstw, dzięki którym ma możliwość realizacji projektów społecznych, edukacyjnych i kulturalnych.

Więcej informacji na temat Fundacji PFR znajduje się na stronie: **www.fundacjapfr.pl**

Centralny Dom Technologii

PFR Fundacja



Opracowanie:

Marek Grzywna
Zbigniew Bujak
Cyberbezpieczni

Projekt jest finansowany ze środków **Kancelarii Prezesa Rady Ministrów** w ramach ogólnopolskiego programu rozwoju kompetencji uczniów i nauczycieli **„Cyberbezpieczni”.**