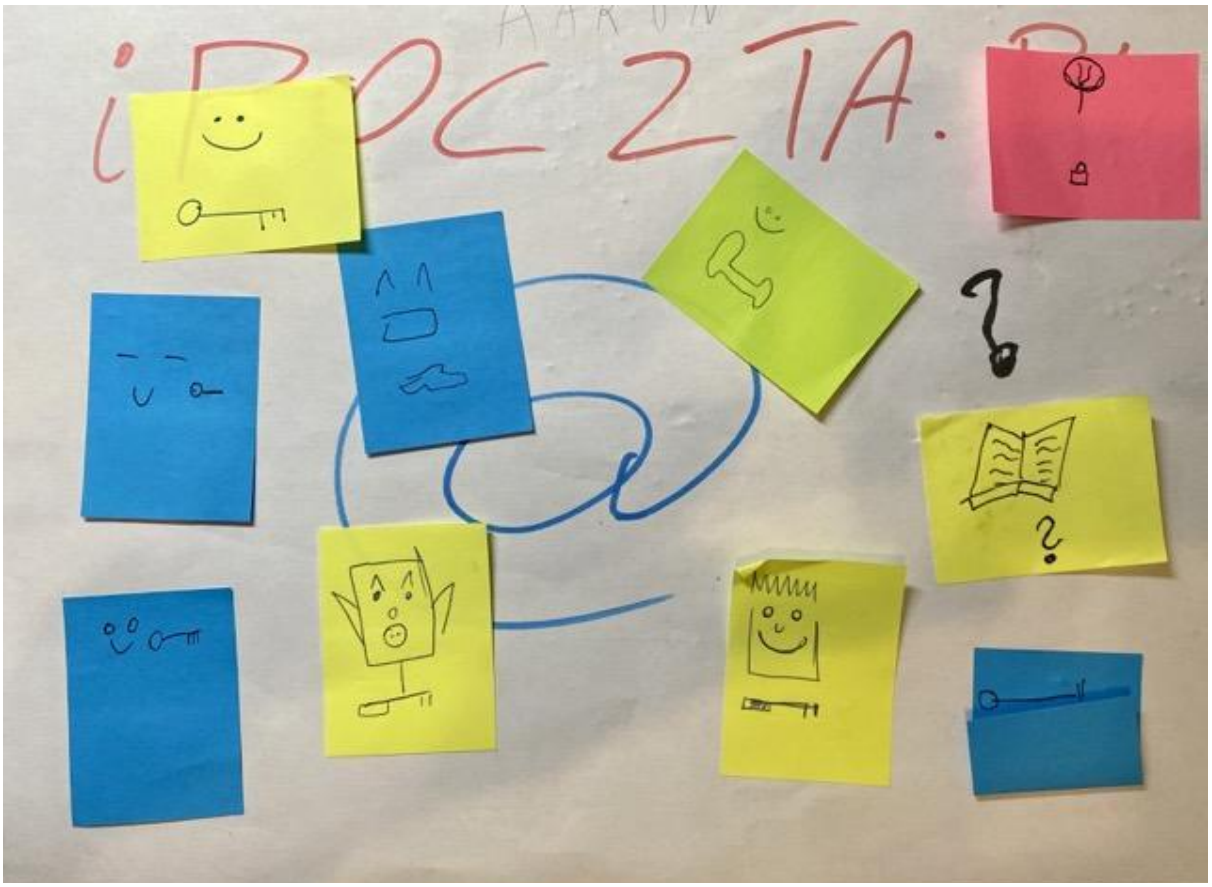
Poducha cyberbezpieczeństwa – dla najmłodszych*

*najmłodszych tj. od 2. klasy SP



Poducha pokazuje jak wielki wpływ na ochronę swojej tożsamości w sieci mają sami użytkownicy Internetu. Pokazuje także na co nie mają oni wpływu.

Poducha cyberbezpieczeństwa jako produkt Cyfrowego Skauta ma na celu:

- pokazać, że do edukacji najmłodszych zbędne są rzeczy na prąd;
- zrobić łatwy scenariusz, który pozwoli adeptowi IT przeprowadzić warsztat;
- nauczyć dzieci jak wiele zależy od nich, a co od nich w sieci jednak nie zależy;
- pokazać jak wiele rzeczy nie zależy od nas i dlatego musimy sami zatroszczyć się o bezpieczeństwo danych logowania (uwierzytelniających);
- przedstawić temat w sposób dynamiczny;
- nakreślić cel posiadania różnych haseł do różnych miejsc i pokazać praktyczną siłę ochrony w postaci dwuskładnikowego logowania;
- pobudzić ciekawość dzieci do szukania kolejnych sposobów zachowanie cyberbezpieczeństwa w sieci.

Sposoby zwiększenia zaangażowania:

1. nagrody (drobiazg);
2. docenienie dobrych odpowiedzi.

Potrzebne wyposażenie:

1. kartki A4, A3,
2. kredki, pisaki,
3. karteczki samoprzylepne,
4. drobne nagrody,
5. #Skaucik – naklejka projektu.

Nauczyciel otrzyma podstawowe kroki w formie skróconej instrukcji, a w niej:

- jak pokazać stronę www (lub grę);
- jak wyjaśnić, co to są tzw. kredki i gdzie je nakleić;
- kiedy haker ma zabrać kredki;
- jakie mają paść pytania i wokół jakich ma zostać poprowadzona dalsza dyskusja:

    Co się właśnie wydarzyło?
    Co może zrobić haker?
    Czy haker może się teraz zalogować na twoje konto?
    Czy uda mu się zalogować na inną stronę www?
    Co musi się zadziać lub być, żeby mu się nie udało?

Słownik definicji:

1. ***haker/kraker/oszust/przestępca*** – dokonuje przestępstw w Internecie;
2. ***dane uwierzytelniające, credentials*** – dane logowania, poświadczenia, login i hasło – **kredki – symbol** 😀 i 🗝️ **(kluczyk)**;
3. ***dwuskładnikowe uwierzytelnienie*** – metoda wymagająca dodatkowego składnika logowania (kod z SMS lub z mail, kliknięcie w link w mailu, klucz sprzętowy Yubico);
4. ***haszowanie haseł*** – sposób na bezpieczne przechowywania haseł przez stronę internetową. W grze z założenia strony nie mają tego elementu. Użytkownik nigdy nie wie czy strona to ma, czy stronę łatwo okraść z haseł. Nawet haszowane hasła da się złamać. To kwestia czasu, szczęścia i mocy "komputera" przestępcy (od godziny do 1000 lat). Przestępca zgaduje każdą kolejna możliwą kombinację hasła i porównuje do danych zahaszowanych;
5. ***itemki, skiny*** – przedmioty w grach. Wymagają pracy, szczęścia lub są kupowane za prawdziwe pieniądze. Itemki mogą trafić na czarny rynek w Internecie;
6. ***robux*** – waluta w środowisku gier Roblox. Cena to 800 sztuk za 9,99$;
7. ***Metaverse*** – wirtualny świat, do którego wchodzi się poprzez gogle 3D;
8. ***chat*** – komunikator w grze.

Poducha cyberbezpieczeństwa – gra dla najmłodszych

Instrukcja

1. Prośba: **narysuj swoją ulubioną stronę www lub grę – *strona***
    a. tam, gdzie się logujesz lub masz już swoje konto;
    b. narysuj tak, abyśmy zgadli, co to za strona – masz 10 min.
2. W międzyczasie wybieramy ucznia **hakera** i tłumaczymy mu zadanie z pkt 7.
3. Zadanie: rozpoznajemy te ***strony***, kto co namalował.
4. Nauczyciel pokazuje ***strony*** i pyta uczniów czy tu mają konto?
5. Tłumaczymy, co to są dane uwierzytelniające (inaczej zwane credentials – **kredki** – czyli po prostu login i hasło).

    Przygotuj kartkę z uśmieszkiem 😀 (synonim nicka/loginu) **i poniżej symbol kluczyka**.

    a. Na karteczkach samoprzylepnych zapiszcie kredki.
    b. UWAGA!: Nie używamy prawdziwych kredek, prawdziwego hasła.
    c. Loginem niech będzie 😀 (synonim nicka/loginu).
    d. Hasło niech będzie w formie obrazka kluczyk 🗝️ (synonim hasła).
6. Polecenie: *Teraz przyklejcie swoje **kredki** na **stronach**, których używacie.*

7. Haker kradnie karteczki ze strony, gdzie jest najwięcej **kredek** – uczeń odgrywa tą rolę:
    a. zabiera z wybranych ***stron*** wszystkie lub wybrane karteczki.
8. Nauczyciel pyta:
    a. Zobaczcie co się stało? Kto wie?
    b. Co może zrobić haker?
    c. Czy haker może teraz się zalogować na twoje konto?
9. Spośród odpowiedzi, w dyskusji szukamy informacji o konsekwencjach takiego zdarzenia. Przykładowe konsekwencje po przejęciu tożsamości. Haker teraz może:
    a. pisać w naszym imieniu;
    b. zapłacić naszymi walutami;
    c. hejtować z naszego konta;
    d. czytać korespondencję;
    e. sprzedać postać z gry, itemki.

Tutaj katalog konsekwencji zagrożeń Katalog konsekwencji zagrożeń

UWAGA: odpowiedzi, sugestie, których brak w Katalogu – spisać i przesłać do Skauta.
Skaut odpowie.

10. Pokazując przykładową karteczką na przyklejoną inną ***stronę***, nauczyciel pyta:
    a. *Czy haker może teraz zalogować się tym samym hasłem na inne konta?* Nauczyciel wraz z uczniami sprawdzają czy te kredki się nie powtarzają na innych stronach.
    b. *Czy uda mu się zalogować na inną stronę tymi danymi?*
    c. *Co musi się zadziać lub być, żeby mu się **nie** udało?*
    d. Pożądane odpowiedzi:
        i. *dwuskładnikowe uwierzytelnianie;*
        ii. *różne hasła;*
        warto docenić, bo to realne zabezpieczenie na taki atak hakera.
11. Nauczyciel pyta i podsumowuje:
    a. *Na co mamy wpływ w ochronie swojej tożsamości?*
        i. różne hasła do różnych miejsc;
        ii. dwuskładnikowe logowanie.
    b. *Na co nie mamy wpływu zakładając gdzieś konto?*
        i. jak chronione są nasze dane.
    c. *Co możemy zrobić, żeby nie ponosić konsekwencji kradzieży naszych danych uwierzytelniających?*
12. Polecenie:
    a. zróbmy jeszcze raz dane logowania na karteczkach, teraz z innym kolorem kluczyka i jeszcze raz załóżmy konto.