

Zabawa: Niebezpieczne wiadomości, czyli jak nie dać się nabrać w internecie

Co będzie potrzebne?

- Komputer/ smartfon (z połączeniem do internetu)
do odtworzenia filmu pt. „Owce w sieci: Dziewięćdziesiąt dziewięć”
- oraz do rozwiązywania quizu „Prześlij dalej...”

Liczba uczestników: minimum 2 osoby

Zabawa przeznaczona dla dzieci w wieku: 10 - 11 lat

Czego dowie się Twoje dziecko?

- jakie mogą być konsekwencje spełniania próśb nieznanym osobom w internecie
- dlaczego nie warto bezkrytycznie wierzyć w internetowe prezenty i promocje (i groźby)

Opis zabawy

Internetowe łańcuszki, prośby o rozestanie wiadomości lub zdjęć do znajomych – pewnie o nich słyszeliście nie raz. Wydają się być niewinną zabawą, podczas gdy w rzeczywistości mogą sprawić wiele kłopotów. Łańcuszek internetowy to tak naprawdę spam, który zawiera polecenie lub prośbę o rozestanie danej wiadomości do jak największej liczby odbiorców. Często zawiera groźbę, że jeśli nie wyślemy go dalej, zgodnie z zapisaną informacją, może na przykład się nam coś stać. Niektóre łańcuszki bywają jedynie irytującą grą (jeśli nie jesteśmy ich zwolennikami), inne niestety niosą za sobą poważne zagrożenia – mogą prowadzić do przeciążenia łączy internetowych oraz blokady serwerów czy zarażenia wirusem naszego komputera.

Jak na nie reagować? Dowiedzie się z kolejnego odcinka serii „Owce w sieci”.

Zadanie 1.

Obejrzyj razem z dzieckiem film pt. „Owce w sieci: Dziewięćdziesiąt dziewięć” (otwórz poniższy adres internetowy lub widoczny obok QR-kod).
<https://youtu.be/ORtdAkOg4fM>



Zajmie Wam to tylko trzy minuty. Spróbujcie podsumować morał tego odcinka, układając zdanie z samych emotikoniek i przesyłając je sobie nawzajem. Koniecznie sprawdźcie, czy dobrze zrozumieliście swoje wiadomości.

Przykład:



(Jeśli uwierzę w groźby nadawcy wiadomości i roześlę ją do wszystkich znajomych, będą bardzo niezadowoleni lub przestraszą się, jak ja, a cyberprzestępca osiągnie swój cel).

Zadanie 2.

Rozwiąż ze swoim dzieckiem szybki quiz pt. „Prześlij dalej...” (otwórz poniższy adres internetowy lub widoczny obok QR-kod).
<https://forms.gle/LRm3h13RpgUm53AE9>



Pogratuluj dziecku wszystkich poprawnych odpowiedzi, ale też spróbuj się dowiedzieć, jakie ma wrażenia i przemyślenia po obydwu zadaniach.

Zapytaj je:

- Jak myślisz, dlaczego odbiorcy takich wiadomości „nabierają się” na nie?

I Jasiak, i wszystkie owce w kreskówce uwierzyły, że jeśli nie wykonają zaleceń z e-maila, to stanie się coś BARDZO ZŁEGO. I o to chodzi. Nadawcy tego rodzaju wiadomości chcą skłonić nas do wykonania ich polecenia, więc stosują różne sztuczki. Czasami pojawia się w nich groźba (np. usunięcia konta lub utraty jakiejś wyjątkowej okazji). To oczywiste, że nikt nie lubi czegokolwiek tracić, więc często reagujemy w takich sytuacjach bez zastanowienia. Bywa też tak, że kusi nas bardzo przyjemna obietnica – np. prezent, który otrzymamy, jak tylko... no właśnie, zrobimy to, czego oczekuje nadawca. Emocje w takiej

sytuacji nie są dla nas dobrym doradcą, najlepiej więc, jeśli poradzimy się kogoś dorosłego i dokładnie sprawdzimy, o co w takiej podejrzanej wiadomości chodzi.

- Czym może grozić spełnienie próśb (lub gróźb) nadawcy?

Bardzo często nadawcy takich wiadomości nie mają dobrych intencji. Mogą to być cyberprzestępcy, którzy próbują uzyskać dostęp do wszystkich Twoich kontaktów. Pamiętaj, aby nigdy nie podawać kontaktów do innych osób bez ich zgody. Zachęty do pobrania załącznika albo kliknięcia w link zamieszczony w wiadomości to najczęściej nic innego, jak próba zainfekowania Twojego komputera złośliwym oprogramowaniem, wirusami, albo programem, który zaszyfruje wszystkie dane na komputerze lub smartfonie i sprawi, że staną się bezużyteczne. W takiej sytuacji cyberprzestępcy mogą zażądać dużej sumy pieniędzy za „odszyfrowanie” Twojego sprzętu. Nigdy nie ściągasz nieznanymi załącznikami i nie klikaj w linki w wiadomościach od nieznanymi nadawców. Najlepszą ochroną przed cyberprzestępcami jest Twój zdrowy rozsądek (z małą pomocą programu antywirusowego 😊).

- Co najlepiej zrobić, jeśli dostanie się taką wiadomość?

Na wiadomości, w których ktoś nam grozi, obiecuje „złote góry”, albo zachęca do pobrania załącznika (np. kuponu w quizie) lub kliknięcia w link, nie powinniśmy nigdy reagować! Najlepiej, jeśli od razu wykasujemy taką wiadomość. Jeśli budzi nasz duży lęk, pokażemy ją komuś dorosłemu. Nie przesyłamy jej do innych, nawet dla żartu, ponieważ możemy wtedy narazić ich komputer lub smartfona na atak cyberprzestępców.