Pytania konkursowe i właściwe odpowiedzi do testu dla Rodziców.

Te pytania (i odpowiedzi) dla uczestników naszej zabawy okazały się najłatwiejsze (od 87,5 % do 94,32% poprawnych odpowiedzi):

* Czy jesteśmy anonimowi w Internecie? (nie)
* Jaka metoda daje nam stuprocentowe bezpieczeństwo poruszania się po sieci? (Nie ma stuprocentowej pewności, w Internecie zawsze obowiązuje zasada ograniczonego zaufania.)
* Co zrobisz w podanej sytuacji, aby się upewnić, że nie jest to próba wyłudzenia danych?

***Wyobraź sobie, że dzwoni do Ciebie osoba, która mówi, że jest pracownikiem banku i chce ustawić lepsze zabezpieczenia. Dzwoniący zna twoje imię, nazwisko, podaje ostatnie cyfry Twojej karty. Prosi Cię o instalację "aplikacji bezpieczeństwa".*(**Przerywam rozmowę i dzwonię na infolinię banku, aby to wyjaśnić.)

* Co należy zrobić, jeśli otrzymasz z banku wiadomość tego typu:

***Drogi Kliencie, wykryliśmy problem z Twoim kontem. Nasz system wykrył nietypowy login do Twojego konta, musisz odblokować konto poprzez zweryfikowanie poprawnych informacji, aby uzyskać ponownie dostęp do konta. Otwórz poniższy plik pomocy technicznej, aby uzyskać pomoc od naszego zespołu pomocy.*(**Najpierw dzwonię do mojego banku)

* Czekasz na paczkę. Dostajesz sms o takiej treści: ***Dostawa twojego przedmiotu nie jest możliwa, powodem jest przekroczenie wymiaru paczki. Dodatkowa kwota 1,20 zł https://bit.ly/2H58267*  (**Dzwonię do firmy kurierskiej, aby dowiedzieć się, czy naprawdę mają problem z moją paczką)
* Wyobraź sobie, że dzwoni do Ciebie osoba, która mówi, że jest policjantem. Twierdzi, że nieuczciwy pracownik banku próbuje ukraść Twoje oszczędności. Na szczęście od jakiegoś czasu jest on na celowniku policji, która ma szansę złapać go na gorącym uczynku. Aby zabezpieczyć pieniądze i schwytać złodzieja, musisz wypłacić w pobliskim bankomacie pieniądze ze swojego konta i wpłacić je na specjalne „bezpieczne konto”. (Nie podaję dzwoniącemu żadnych danych. Proszę go o imię, nazwisko, numer jednostki. Po rozmowie idę na komisariat i wyjaśniam sprawę)
* Dostaniesz mailem ofertę sprzedaży sprzętu elektronicznego, który planujesz kupić. Cena jest bardzo dobra, bo właśnie trwa promocja. Wchodzisz na stronę sklepu, gdzie znajdujesz ofertę niższą o 30% od cen regularnych. (Przed zakupem w jakimkolwiek sklepie internetowym najpierw sprawdzam opinie na jego temat na niezależnych stronach oraz forach internetowych. Upewniam się też, czy w regulaminie znajduje się KRS, NIP oraz adres firmy, która oferuje produkty.)
* Dostajesz taką wiadomość od dobrego znajomego: ***Hej, masz może opcję szybkiego przelewu na telefon? Opłacisz mi zamówienie, a ja Ci oddam z nawiązką za pomoc.*(**Zanim wyślę kod, dzwonię do znajomego, aby potwierdzić, że naprawdę potrzebuje pomocy.)

Pytania o średnim stopniu trudności (od 44,32 % do 82,95 % poprawnych odpowiedzi):

* Aby skutecznie chronić swój komputer, należy zainstalować na nim program antywirusowy. (tak, należy tylko pamiętać, aby to był jeden program – jeśli zainstalujemy więcej mogą się wzajemnie „zwalczać”).
* Jak nazywamy fałszywe informacje pojawiające się w sieci, które najczęściej  mają za zadanie wywołać strach, panikę, sensację lub komuś zaszkodzić? (fake news)
* W którym miesiącu obchodzimy Dzień Bezpiecznego Internetu? (luty)
* Od którego roku obchodzony jest Dzień Bezpiecznego Internetu? (od 2004)
* Skąd możesz się dowiedzieć, co twoje dziecko robi w sieci? (odpowiedź: Wydaje mi się, że bliski kontakt z dzieckiem i częste rozmowy wystarczą.

Wyjaśnienie:

Bliski kontakt z dzieckiem i rozmowy to fundament zdrowej rodziny! Należy jednak mieć na uwadze, że dziecko może nawet nie wiedzieć, że to, co robi, potencjalnie stwarza dla niego ryzyko. Zalecamy, by od czasu do czasu poprosić o pokazanie listy znajomych i wyrywkowo zapytać, skąd się znają. Nigdy natomiast nie powinniśmy tego robić bez wiedzy dziecka – dziecko ma prawo do tajemnicy korespondencji. Warto również włączyć filtr rodzicielski w przeglądarkach – oczywiście przy udziale dziecka, objaśniając, co robimy i dlaczego.

(źródło: Projekt Cybernauci – materiały edukacyjne dla rodziców).

* Informacje o karcie kredytowej twojego znajomego zostały wykradzione, gdy kupował coś przez internet. Po czym możesz poznać, że twoje dane są bezpieczne podczas zakupów on-line? (odpowiedź: W pasku adresowym jest zamknięta kłódka, a adres strony zaczyna się od “https”.)

Wyjaśnienie:

Samo szyfrowanie nie wystarczy. Równie ważna jest renoma samego sklepu i to, czy obsługuje płatności poprzez przekierowanie na stronę banku. Większość sklepów internetowych nie wymaga dziś podawania danych karty. Obsługiwanie płatności poprzez przekierowanie oznacza, że dane karty nie są w ogóle nikomu udostępniane, a płatność przetwarza bezpośrednio nasz bank.

(źródło: Projekt Cybernauci – materiały edukacyjne dla rodziców).

* Twoja znajoma skorzystała z nowego serwisu umożliwiającego darmowe pobieranie muzyki i filmów. Po miesiącu okazało się, że musi zapłacić wysoką kwotę za pobieranie plików. Jak uniknąć takich przykrych niespodzianek? (odpowiedź: Należy czytać regulaminy i nie akceptować ich bez zrozumienia warunków korzystania z serwisów.)

Wyjaśnienie:

Akceptowanie regulaminu usługi często jest równoznaczne z zawarciem umowy z dostawcą tej usługi. Na treść tej umowy nie mamy jednak wpływu. Zapoznanie się z takim regulaminem ma szczególne znaczenie, jeżeli przed skorzystaniem z serwisu internetowego, aplikacji czy usługi musimy dokonać rejestracji, podając swoje dane osobowe (numer telefonu, numer karty kredytowej). Podanie takich danych usługodawcy może być potraktowane jako wyrażenie skutecznego oświadczenia woli, może więc wywołać skutki prawne i rodzić zobowiązania po stronie użytkownika. Dlatego warto dokładnie się zastanowić przed przystąpieniem do procesu rejestracji. Szczególną ostrożność należy zachować, podając dane karty: ma to sens tylko w przypadku, kiedy chcemy płacić za jakąś usługę, a i wtedy trzeba się dwa razy zastanowić i dokładnie przeanalizować punkty regulaminu dotyczące pobierania płatności. Lepszym wyjściem może być użycie tzw. karty wirtualnej (pre-paid) do płatności w internecie.

Kolejnym ważnym aspektem regulaminów są zawarte w nich oświadczenia o zgodzie na przetwarzanie danych użytkownika wprowadzanych do systemu usługodawcy. Warto dokładnie dowiedzieć się, jakie prawa do wprowadzanych treści rości sobie usługodawca, czy zamierza przekazać te informacje podmiotom trzecim. Chodzi tutaj zarówno o nasze dane osobowe i inne informacje wprowadzane do serwisu, które mogą naruszyć naszą prywatność, jak i wprowadzane do systemu utwory, których użytkownik jest autorem.

Warto zwrócić swojemu dziecku uwagę na czytanie ze zrozumieniem regulaminów i przemyślane podawanie swoich danych podczas korzystania z serwisów internetowych. Jeśli to możliwe, warto, by dziecko używało pseudonimu. Warto też przyjąć regułę, że każdy przypadek podawania danych osobowych albo akceptowania długiego, trudnego do zrozumienia regulaminu dziecko powinno konsultować z dorosłym.

W kontekście pobierania z sieci plików będących utworami w rozumieniu prawa autorskiego (np. filmy, muzyka, książki itp.) należy zastanowić się nad granicami legalności takiego działania. Zgodnie z art. 23 pkt 1) ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych „Bez zezwolenia twórcy wolno nieodpłatnie korzystać z już rozpowszechnionego utworu w zakresie własnego użytku osobistego”. W Polsce dozwolone jest zatem „ściąganie” plików na własny użytek. Należy tutaj zwrócić uwagę na warunek wcześniejszego rozpowszechnienia utworu (za zgodą autora). Jeśli więc pobieranie dotyczy utworów będących już oficjalnie w obrocie, to jest legalne w świetle polskiego prawa. Nielegalne jest natomiast ściąganie plików z muzyką, filmami czy książek z serwisów P2P, na których ściągając, jednocześnie automatycznie udostępniamy już ściągnięte fragmenty utworów (naruszenie zapisu o korzystaniu „na własny użytek”).

(źródło: Projekt Cybernauci – materiały edukacyjne dla rodziców).

* Jakie sposoby ochrony prywatności w sieci polecasz swojemu dziecku? (odpowiedź: Rozsądnie i świadomie korzystaj z sieci – używaj pseudonimów, ustawiaj opcje prywatności na serwisach społecznościowych, zastanów się nad tym, jakie konsekwencje może mieć publikowanie i ściąganie treści. Instaluj wszystkie zalecane aktualizacje bezpieczeństwa dla oprogramowania, którego używasz.

Wyjaśnienie:

Większość zasad bezpieczeństwa obowiązuje zarówno świecie prawdziwym, jak i wirtualnym. Tak jak nie zostawiamy na drzwiach kartki, że wyjechaliśmy na dwutygodniowy urlop, nie warto też ogłaszać tego w mediach społecznościowych. Dbamy, żeby zamki w naszym mieszkaniu były sprawne, dbajmy też o aktualność naszego oprogramowania i zainstalujmy programy antywirusowe (aktualizacje są nawet ważniejsze, to one łatają błędy oprogramowania wykorzystywane przez wirusy).

Ponieważ zdarzają się wycieki haseł z serwisów internetowych, bardzo ważne jest, aby nie używać wszędzie tego samego hasła. Jeśli takie hasło dostanie się w niepowołane ręce, grozi nam naruszenie naszej całej cyfrowej tożsamości. Jeśli udostępniasz jakieś informacje o sobie, rób to rozważnie. Używaj pseudonimów, gdzie to tylko możliwe. Ustaw odpowiednie opcje w serwisie społecznościowym, aby jak najmniej informacji widziały osoby spoza kręgu twoich znajomych. Jeśli chcesz coś udostępnić w internecie (np. zdjęcie), pomyśl, że to nieodwołana decyzja: bardzo trudno coś z internetu „usunąć”. Nie otwieraj podejrzanych plików, używaj mocnych haseł, różnych dla każdego serwisu.

(źródło: Projekt Cybernauci – materiały edukacyjne dla rodziców).

* Wystawiasz coś na jednej z popularnych platform ogłoszeniowych. Super! Udało Ci się sprzedać produkt. Teraz dostajesz od kupującego link do wygodnego przygotowania przesyłki do paczkomatu z wypełnionymi przez niego danymi. Co robisz? (Korzystam z informacji na głównej stronie portalu, aby się upewnić, czy to rzeczywiście kupujący powinien mi wysłać link do transakcji. )

Wyjaśnienie:

Zawsze upewnij się czy strona jest prawdziwa i jakie są zasady jej funkcjonowania. Dzięki temu rozpoznasz niestandardowe prośby i żądania. W tym przypadku – upewnisz się kto tak naprawdę wysyła link do wystawienia listu przewozowego. (https://www.ludziesaniesamowici.pl/test-bezpieczenstwa)

* Twoja córka jest aktywną użytkowniczką forum o zwierzętach „Mój pupil”. Skarży się, że od jakiegoś czasu za każdym razem, gdy napisze posta, zaczepia ją użytkownik o nicku „Gad1990”. Wysyła jej nieprzyjemne wiadomości i złośliwie komentuje każdy jej wpis. Ostatnio zapytał ją w prywatnej wiadomości o adres domowy. Co robisz? (Informuję o podejrzanym użytkowniku administratorów forum i sprawdzam, czy da się go zablokować.)

Wyjaśnienie:

Twoja córka ma do ciebie zaufanie i wie, że pomożesz jej znaleźć adekwatne rozwiązanie dla jej problemu. Fora internetowe powinny oferować różne środki służące zwalczaniu złośliwych zachowań użytkowników; skorzystanie z nich jest w tej sytuacji najlepszym wyjściem. Twoja córka powinna mieć możliwość zablokowania użytkownika tak, aby nie mógł się z nią kontaktować. Ponadto administratorzy mogą wysłać tej osobie ostrzeżenie, usunąć niepożądane treści, a w ostateczności usunąć jego konto. Czasami usunięcie konta nie wystarczy i istnieje konieczność zablokowania adresu IP użytkownika, co uniemożliwi mu zakładanie kolejnych kont. Porozmawiaj z córką o niepożądanych zjawiskach na forach internetowych i pokaż jej, jak może rozpoznać, czy forum jest w poprawny sposób moderowane i przyjazne dla kulturalnych użytkowników. Jednocześnie upewnij się, że córka wie, jak w bezpieczny sposób korzystać z sieci, i że nie przekazała nieznajomemu użytkownikowi swoich danych osobowych. (źródło: Projekt Cybernauci – materiały edukacyjne dla rodziców).

Pytanie trudne (tylko dwa pytania okazały się trudne dla naszych uczestników – dobrych odpowiedzi było od 4,55 % do 7,95 %):

* Pokazujesz swoim dzieciom, jak założyć konto w Internecie. Jesteście na etapie wybierania hasła. Twój syn ma kilka pomysłów – który jest najlepszy? (2żółsło!)

Wyjaśnienie:

Hasło „$@nToR1n1” jest bardzo mocne, ale też bardzo łatwo je zapomnieć, co oznacza, że zostanie pewnie zapisane na jakiejś kartce lub w widocznym miejscu. Hasła muszą być silne, ale i możliwe do zapamiętania. Najlepiej sprawdzają się więc hasła w postaci krótkich fraz (kilka słów). Łatwiej je zapamiętać niż losowe ciągi znaków, a są wystarczająco silne. Warto też korzystać z menedżerów haseł, jak KeePassX.

(źródło: Projekt Cybernauci – materiały edukacyjne dla rodziców).

* Kim jest haker? (odpowiedź: Jest to osoba, która ma dużą wiedzę z jakiejś dziedziny (np. informatyki, ale nie tylko) i potrafi twórczo tę wiedzę wykorzystać, np. stworzyć własne oprogramowanie czy samodzielnie zbudować lub naprawić potrzebne urządzenia; majsterkowicz. To m.in. dzięki hakerom powstało wolne oprogramowanie np. GNU/Linux, GIMP czy Mozilla Firefox.)

Wyjaśnienie:

Hakerów znaleźć można w [hackerspace’ach](https://pl.wikipedia.org/wiki/Hackerspace%22%20%5Ct%20%22_blank) na całym świecie. Hackerspace to swego rodzaju klub majsterkowicza, przestrzeń, w której hakerzy mogą wspólnie popracować nad swoimi projektami, znaleźć niezbędne narzędzia albo zwyczajnie spędzić trochę czasu w towarzystwie podobnych im ludzi. W każdym większym mieście w Polsce istnieje lub powstaje hackerspace; warto tam zajrzeć, nawet jeśli nie czujesz się hakerem! Więcej na ten temat możesz poczytać w serwisie [wiki.hackerspace.org](https://wiki.hackerspaces.org/) (materiał anglojęzyczny) oraz w artykule [Hacker Howto Erica Stevena Raymonda](http://rafa.eu.org/hacker-howto.html).

(źródło: Projekt Cybernauci – materiały edukacyjne dla rodziców).

Pytanie o hakera powtórzyło się z zeszłego roku i również sprawiło największą trudność.