**Pytania konkursowe i właściwe odpowiedzi do testu dla Rodziców.**

Te pytania (i odpowiedzi) dla uczestników naszej zabawy okazały się najłatwiejsze (od 85,51 % do 96,38% poprawnych odpowiedzi):

* W którym miesiącu obchodzimy Dzień Bezpiecznego Internetu? (luty)
* Czy jesteśmy anonimowi w Internecie? (nie)
* Czy należy zasłaniać kamerkę w swoim laptopie? (tak)
* Pytanie dotyczące reakcji na wiadomość mailową z banku (nigdy nie klika się w linki, które otrzymujemy w mailu – to może być podstawiona, sklonowana przez oszustów strona; można natomiast skontaktować się z bankiem i powiadomić go o sytuacji, używając jednak informacji kontaktowych podanych na stronie banku, a nie w mailu).
* Pytanie dotyczące najbezpieczniejszego hasła spośród podanych. (jo@7LAN#5ta - zawiera litery, liczby i znaki specjalne)
* Co oznacza symbol kłódki w pasku adresu przeglądarki internetowej? (To szyfrowana wersja protokołu komunikacji między przeglądarką a danym serwerem. Oznacza, że połączenie jest bezpieczne).
* Jaka metoda daje nam stuprocentowe bezpieczeństwo poruszania się po sieci? (Nie ma stuprocentowej pewności, w Internecie zawsze obowiązuje zasada ograniczonego zaufania.)
* Pytanie: Dostajesz maila od nieznanej firmy, która twierdzi, że nie opłaciłeś/-aś faktury. Faktura jest w załączniku. Co robisz? (To podejrzane. Słyszałam o przestępcach internetowych. Jeśli informacja nie pochodzi ze znanego mi adresu e-mail, a tytuł wiadomości nie dotyczy sprawy, którą kojarzę, kasuję mail wraz z załącznikiem, bez otwierania.)
* Jak nazywamy cyberprzestępstwo polegające na wysyłaniu maili w celu wyłudzenia pieniędzy lub informacji? (phishing)

Pytania o średnim stopniu trudności (od 48,55 % do 84,78 % 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”).
* Jutro Twoje dziecko idzie na urodziny do koleżanki. Właśnie sobie przypomniałeś/-aś, że nie kupiłeś/-aś jej prezentu. Jeśli zamówisz go teraz on-line, powinien przyjść następnego dnia. Co robisz? (odpowiedź: Dopiero po powrocie do domu zamawiam prezent on-line z urządzenia (komputera, laptopa) w sieci domowej. Zwracam uwagę na bezpieczeństwo połączenia HTTPS.)

Wyjaśnienie:

Transakcje, nawet najbezpieczniejsze, zawsze wiążą się z jakimś ryzykiem. Dbanie o bezpieczeństwo połączenia HTTPS i korzystanie z własnej, bezpiecznej sieci skutecznie to ryzyko minimalizuje. Większość banków w Polsce wspiera też uwierzytelnienie wielopoziomowe (np. prócz hasła trzeba również podać kod uwierzytelniający przesłany SMS-em lub wygenerowany przez specjalny token) – zdecydowanie warto z niego korzystać!

(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).

* Zakładasz nowe konto w banku. Czytając umowę, zauważasz zapis o konieczności wyrażenia zgody na przetwarzanie danych osobowych w celach marketingowych. Co robisz?

(odpowiedź: Nie zgadzam się na podpisanie umowy. Zgodnie z Ustawą o ochronie danych osobowych mam prawo do wyrażenia zgody na przetwarzanie i udostępnianie swoich danych. Mam też prawo dostępu do tych danych, zmieniania ich i żądania ich usunięcia. To jest klauzula niedozwolona – bank nie może nikogo zmuszać do udostępniania swoich danych. Zgłaszam sprawę do GIODO.)

Wyjaśnienie:

Zgodę na przetwarzanie swoich danych w celach innych niż konieczne do realizacji umowy możesz wyrazić jedynie dobrowolnie, oddzielnie od oświadczenia o chęci zawarcia umowy z bankiem. Masz rację – ten zapis jest klauzulą niedozwoloną. Dobrym rozwiązaniem jest zgłoszenie sprawy do Generalnego Inspektora Ochrony Danych Osobowych w celu zapobiegania rozpowszechnianiu się nieuczciwych praktyk w zakresie gromadzenia danych osobowych. Pamiętaj, że jeżeli zostałaś kiedyś zmuszona do wyrażenia zgody na przetwarzanie danych osobowych z naruszeniem przepisów ustawy, możesz zażądać ich usunięcia.

(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).

* Co przedstawia ten obrazek?



(odpowiedź: To oprogramowania typu ransomware, polegające na szyfrowaniu plików użytkownika i odszyfrowaniu ich po zapłaceniu okupu.)

(źródło: Czy potrafisz zadbać o swoje bezpieczeństwo w sieci? Krzysztof Majdan „Bussines Insider”)

* Od którego roku w Polsce obchodzony jest Dzień Bezpiecznego Internetu? (od 2004) (źródło: strona szkoły, dbi.pl)
* Jak brzmi tegoroczne hasło realizowane w ramach Dnia Bezpiecznego Internetu? (odpowiedź: Działajmy razem!)(źródło: strona szkoły, dbi.pl)
* 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).

* Córka twojego kolegi 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).

Pytanie trudne (tylko jedno z pytań okazało się trudne dla naszych uczestników – dobrych odpowiedzi było 8,7 %, czyli tylko 12 osób odpowiedziało na to pytanie dobrze):

* 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).