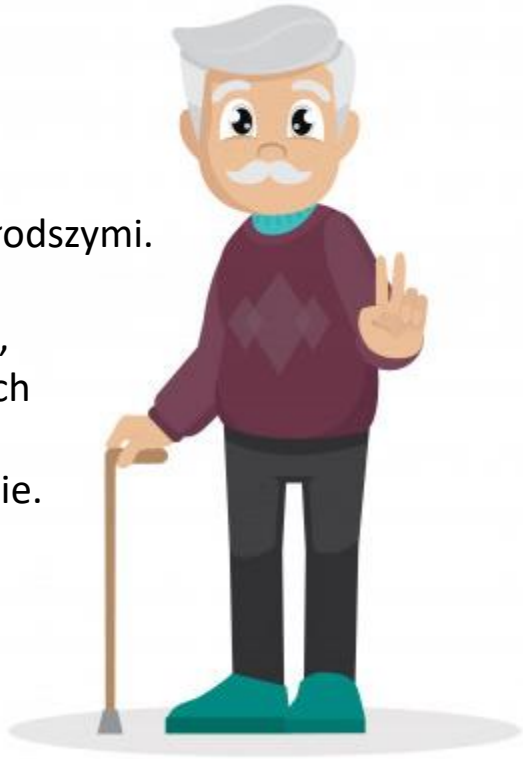
Bezpieczny Internet dla dzieci i seniorów.

Jak rozmawiać z najbliższymi o cyberbezpieczeństwie?

Ten poradnik podzieliliśmy na dwie części. Dzieli je wiek adresatów, łączy troska o ich bezpieczeństwo. Z poradnika dowiesz się, jak rozmawiać z 8-latkiem o bezpieczeństwie w sieci oraz jak wytłumaczyć seniorowi zagrożenia, które czyhają na niego w Internecie.

Wyjaśnij dziecku, z jakimi zagrożeniami może mieć do czynienia i naucz je podstawowych zasad bezpieczeństwa. Sprawdź jakie tematy możesz podjąć z najmłodszymi.



Porozmawiaj z seniorem o zabezpieczeniach, bezpiecznych zakupach w Internecie, mediach społecznościowych i spamie. Jeśli sądzisz, że seniorzy nie korzystają z sieci, jesteś w błędzie. Dowiedz się jaki procent jest aktywny z tego ebooka.

Spis treści

Tłumaczymy 8-latkowi jak być bezpiecznym w Internecie

A gdyby tak kultowe „Załóż czapkę, bo się przeziębisz” i „Nie biegaj, bo się przewrócisz” zamienić na „Nie klikaj gdzie popadnie, bo złapiesz wirusa” i „Nie rozmawiaj z nieznajomymi w sieci”? Sprawy mają się tak: w realnym świecie chronimy dzieci przed następstwami nieodpowiedzialnych zachowań. Natomiast w świecie wirtualnym instalujemy kontrolę rodzicielską i na tym kończymy temat. Bo przecież dziecko jest za małe, aby zrozumieć. Czyżby?

Wyjaśnij dziecku z jakimi zagrożeniami może mieć do czynienia
Zanim posadzisz swoją pociechę przed komputerem i rzucić hasło „serfuj, masz godzinę”, porozmawiajcie. Nie martw się, że dziecko nie zrozumie. Nie chodzi o to, abyś zagłębiał się w skomplikowane definicje. Wystarczy wyjaśnienie przez analogię.

Co grozi Twojemu dziecku w Internecie? Przede wszystkim różne typy szkodliwego oprogramowania, linki do złośliwych stron internetowych oraz witryny automatycznie otwierające nowe okienka i zaczynające pobieranie niechcianych przez nas plików (tzw. drive-by downloads). Zagrożenia jak widać dla każdego są te same, ale nieświadome niebezpieczeństw dziecko może narobić więcej szkód niż wyedukowany dorosły.

Naucz dziecko podstawowych zasad cyberbezpieczeństwa

Rozmowa powinna przebiegać dokładnie tak samo, jak każda pogadanka o bezpieczeństwie w „realu”. Po prostu wyjaśnij, że także w Internecie są ludzie, którzy próbują wykorzystać innych, kradnąc ich prywatne dokumenty lub pieniądze. Ludzie Ci używają różnych metod, aby oszukać – namawiają do przejścia na stronę www lub kliknięcia w jakiś link, obiecując świetną zabawę albo darmową muzykę i bajki. Podkreśl, że chociaż dziecko widzi tylko ekran swojego komputera, sieć łączy różnych (dobrych i złych) realnych ludzi, którzy również zasiadają za monitorami i wszyscy razem tworzą ten wirtualny świat. Dlatego należy być bardzo ostrożnym. Jeśli ktoś nieznajomy próbuje z dzieckiem porozmawiać przez Internet, powinno zareagować tak samo, jak wobec obcego na ulicy. Jeśli usiłuje wręczyć prezent w postaci darmowej bajki, dziecko musi przyjąć analogiczną postawę do tej, gdy nieznajomy chce je poczęstować cukierkiem. Wyjaśnij, że dla własnego bezpieczeństwa, po prostu nie może ulegać takimi pokusom. I sam nie twórz pokus, bo to pierwszy krok do kliknięcia w niewłaściwy link. Jeśli dziecku na czymś bardzo zależy, powinniście wspólnie ustalić co z tym zrobicie (może zakupicie dostęp do platformy z bajkami albo znajdziecie jakąś alternatywę?).

Tematy, które warto podjąć:

- Polityka haseł (jak klucz do kuferka ze skarbami, z nikim się nie dziel).
- Instalacja aplikacji bez zezwolenia (jak wpuszczanie obcego do domu pod nieobecność rodziców).
- Nieznajomi na portalach społecznościowych (jak rozmowa z nieznajomym na ulicy).
- Zamieszczanie w sieci zdjęć swoich i innych osób (jak dzielenie się zawartością wspomnianego kuferka z osobami, których nie znamy).

Kilka wskazówek dotyczących bezpieczeństwa:

- Zamiast zakazywać różnych aktywności w Internecie, pokaż dziecku alternatywy (na przykład w zastępstwie standardowego YouTube'a – YouTube Kids albo zamiast Facebooka (przypominamy, aby korzystać z FB trzeba mieć ukończone 13 lat) – Lego Life).
- Zainstaluj przeglądarkę przyjazną dziecku dzieci (Kiddle, KidRex, Safe Search Kids).
- Na wszelki wypadek zaszyfruj wszystkie dokumenty, do których dziecko nie powinno mieć dostępu oraz te o poufnej treści (zabezpiecz się w razie wycieku).
- Zrób kopię zapasową najważniejszych plików.
- Czytaj o zagrożeniach w sieci i omawiaj je ze swoim dzieckiem.
- Pamiętaj, że tylko poprzez edukację możesz nauczyć je bezpiecznego korzystania z Internetu.

Chroń dziecko w sieci, ale najpierw sam się do tego dobrze przygotuj

Jeśli zdecydowałeś, że Twoje dziecko będzie miało dostęp do komputera podłączonego do Internetu, dobrze się do tego przygotuj.

Załóżmy, że cała rodzina korzysta z jednego urządzenia. Na początku **wydziel konta dla każdego użytkownika**. Możesz to zrobić w panelu sterowania (konta użytkowników). Twoje konto powinno mieć typ „administrator", pozostałe są „standardowe". **Zabezpiecz je hasłami**. Także konto Twojego dziecka powinno być chronione hasłem, bo to dobry pretekst do kształtowania właściwych postaw dotyczących polityki haseł w przyszłości. Wymyślcie je wspólnie zgodnie z obowiązującą regułą: ciąg małych i wielkich liter oraz cyfr, co najmniej 8 znaków. Żadnego „Radzio7" albo „Anulka6". Od razu przejdźcie do konkretów jak Inspektor Gadżet. To może być fragment

ulubionego wierszyka albo piosenki, ale w żadnym wypadku imię Waszego psa 😉 Na przykład (choć to z pewnością nie jest bajka na topie): „KotWbutach07”. Banalne? Według „How secure is my password?” złamanie takiego hasła zajęłoby 3 tysiące lat!

Na tym etapie ważna jest jeszcze jedna kwestia. **Wejdź w ustawienia kontroli konta użytkownika i zmień ustawienia domyślne na „powiadamiaj zawsze”**. W ten sposób, jeśli aplikacje będą próbowały instalować oprogramowanie albo wprowadzać zmiany w systemie lub na koncie Twojego dziecka, jako administrator zostaniesz poproszony o wyrażenie na taką aktywność zgody.

Następnie **sprawdź jak konto Twojego dziecka jest chronione**. Windows ma wbudowanego firewalla, ale dla pewności rzuć okiem na „system i zabezpieczenia”. **Firewall** będzie uzupełniał Ciebie jako administratora, tzn. wyśle komunikat w przypadku, gdy dziecko będzie chciało pobrać jakąś podejrzaną aplikację. Jeśli jednak coś się przez zaporę przedrze, dobrze mieć aktywnego **antywirusa** (pamiętaj, że antywirus działa jak szczepionka: tylko wtedy, gdy posiada danego wirusa w swojej bazie). Dlatego dbaj o to, aby baza była zaktualizowana i nie polegaj tylko na antywirusie, bo atakujący wirus może być nowy, a tym samym nieznany dla Twoich systemów zabezpieczeń.

Oprócz tych wszystkich czynności **zainstaluj ochronę rodzicielską**, co pozwoli Ci kontrolować odwiedzane strony internetowe, blokować dostęp do wskazanych aplikacji (także do mediów społecznościowych) czy nadzorować czas spędzony przez dziecko przed komputerem. Tu pomocy może okazać się także **Adblock** czyli rozszerzenie dla przeglądarek internetowych, które umożliwia blokowanie wyświetlania reklam. Dopiero wyposażony w taki oręż możesz rozpocząć operację „dziecko w sieci” 😉 Powodzenia!

Internet dla seniora

Seniorzy nie korzystają z Internetu? Błąd. Liczba osób 55+ używających sieci stale rośnie. Według danych Gemius/Polskie Badanie Internetu w 2016 roku było ich 15,3%, natomiast pod koniec 2018 już 18,5%.

Internet dla seniora w liczbach

Przyjrzyjmy się aktywność osób 55+ w sieci. Według badań CBOS 39% użytkowników korzystających z Internetu w wieku 55-64 lat posiada konto w social mediach. Na samym Facebooku jest ich nawet 2 miliony. To ponad 13% wszystkich użytkowników tego narzędzia. Z kolei według danych raportu „E-commerce w Polsce 2018" 27% seniorów dokonuje zakupów online. Najczęściej kupują odzież i dodatki, kosmetyki i perfumy oraz książki, płyty, filmy.

Czy Internet jest bezpiecznym miejscem dla seniora?

Technologia nie jest dla osób starszych chlebem powszednim. Niektórzy z nich urodzili się zanim zbudowano pierwszy komputer. Byli nastolatkami, gdy zrodziła się koncepcja globalnej sieci komputerów i dorosłymi ludźmi, gdy powstała pierwsza strona www. Dlatego prawdopodobnie o cyberbezpieczeństwie mają pojęcie nikłe (jeśli w ogóle jakieś mają). Równocześnie należy zwrócić uwagę na to, że to seniorzy padają ofiarom licznych oszustw w życiu codziennym. Tylko w 2018 roku metodą na policjanta albo na wnuczka wyłudzono od nich ponad 60 milionów złotych.

Porozmawiajmy o bezpieczeństwie w sieci

Jeśli masz w swoim środowisku aktywnego w Internecie seniora, koniecznie porozmawiaj z nim o cyberbezpieczeństwie. Kluczowy dla tej rozmowy będzie właściwy dobór słownictwa. Nigdy nie używaj skomplikowanej terminologii. Tłumacz używając prostych zwrotów i analogii. Bądź cierpliwy 😉

Od czego zacząć? Od słuchania. Dowiedz się jak korzysta z Internetu: czy kupuje online i jak płaci za zakupy, w jakich serwisach jest zalogowany, czy używa poczty elektronicznej. Dopiero znając jego potrzeby i zachowania możesz doradzić konkretne działania.

Jeszcze jedno. Nie polecamy przeprowadzać tej rozmowy w jednym ciągiem. Najlepiej podzielić ją na etapy. Traktuj swojego ucznia poważnie. Tłumacz wszystko, ale miej świadomość, że Twój rozmówca może nie przyswoić całej wiedzy lub nie zrozumieć niektórych wątków. Dlatego przygotowaliśmy króciutkie podsumowanie pod koniec każdego omówionego problemu, które senior powinien zapamiętać obowiązkowo. Reszta jest dla Ciebie, abyś nie zapomniał poruszyć żadnego istotnego wątku.

Po pierwsze odpowiednie zabezpieczenia

Podstawa to dobrze zabezpieczony komputer. Co senior musi wiedzieć na pewno? Że jeśli haker się uprze, to i tak narobi szkód, bo nie ma żadnej 100% ochrony przed cyberatakami. Prywatny komputer dobrze zabezpieczyć w dwojaki sposób. Po pierwsze firewallem, po drugie antywirusem. Wyjaśnij, że firewall to zapora przed atakami z zewnątrz. Windows ma wbudowaną taką zaporę. Pokaż gdzie można sprawdzić czy jest aktywna i jak ona działa (na przykład spróbuj pobrać jakąś aplikację, aktywny firewall powinien Cię zapytać czy na pewno chcesz wykonać taką operację).

Podkreśl kilka razy, że niezaktualizowany antywirus nie spełnia swojej funkcji. Powiedz jak działa. Użyj analogii ściany – firewall to mur zabezpieczający przed nieproszonymi gośćmi, a antywirus jest strażnikiem, który zaczyna działać, gdy uda mu się jednak wprosić. W tym przypadku właściwe jest także porównanie antywirusa do szczepionki. Szczepionka działa tylko przeciw wirusom, które zna. Tak samo antywirus nie obroni komputera, jeśli atakujący wirus jest nowy.

Zapytaj seniora, czy posiada jakieś pliki (zdjęcia czy dokumenty), które są poufne. Jeśli tak, zastanówcie się wspólnie czy ich wyciek mógłby mieć nieprzyjemne konsekwencje. Być może uznacie, że warto zaszyfrować wybrane foldery po to, aby tych konsekwencji uniknąć.

Senior powinien być także świadomy, że pliki można bezpowrotnie utracić. Wyjaśnij mu czym jest kopia zapasowa. Jeśli to konieczne, wybierzcie wspólnie miejsce, gdzie będzie gromadził backupy, na przykład w usłudze chmury albo na dysku zewnętrznym typu pendrive.

Co senior powinien zapamiętać z tej części rozmowy? Nie wolno pomijać aktualizacji antywirusa. Jeśli przechowujemy poufne dokumenty na komputerze powinniśmy je szyfrować i wykonywać kopię zapasową.

Bezpieczna przeglądarka internetowa dla seniora

Przeglądarka przeglądarce nie jest równa. Wybierzcie taką z podniesionym bezpieczeństwem i ustawieniami prywatności. Wielu ekspertów poleca przeglądarkę Chrome, ponieważ posiada ona tzw. mechanizm piaskownicy. W uproszczeniu mówiąc, Chrome bada co dzieje się w Internecie, szuka złośliwych kodów, sprawdza je i jeszcze z tego wszystkiego wyciąga wnioski, bo rejestruje skutki działania. Czyli ta przeglądarka szybciej wykrywa, że dzieje się coś niedobrego i udaremnia próby ataków. Oczywiście nie jest to jedyna bezpieczna przeglądarka na rynku. Ważne, żeby senior miał świadomość, że wybór przeglądarki ma znaczenie.

Przy okazji porusz temat zbierania przez Chrome'a informacji o użytkownikach. Przejrzyjcie wspólnie ustawienia konta Google, zwracając szczególną uwagę na zakładki: dane osobowe, dane i personalizacja, bezpieczeństwo, osoby i udostępnianie oraz płatności i subskrypcje.

Co senior powinien zapamiętać z tej części rozmowy? Wybór przeglądarki ma znaczenie. Należy korzystać tylko i wyłącznie z bezpiecznych przeglądarek internetowych.

Aktualizacje łatają dziury bezpieczeństwa

Przypilnuj seniora, aby nigdy nie bagatelizował aktualizacji. Powiedz, że nikt nie jest nieomylny, nawet twórcy oprogramowania. Każde posiada dziury czyli błędy bezpieczeństwa. Na szczęście twórcy oprogramowania cały czas ich szukają i łatają. Gdy tak się stanie, wysyłają informację użytkownikowi, aby przystąpił do aktualizacji. Niezaktualizowane oprogramowanie to dziurawe oprogramowanie, które zagraża bezpieczeństwu seniora w Internecie.

Co senior powinien zapamiętać z tej części rozmowy? Nie wolno pomijać aktualizacji.

Bezpieczne zakupy i płatności online

Jeżeli korzystamy z bezpiecznej przeglądarki, powinna nas ona ostrzegać przed podejrzanymi witrynami. Ale przezorny zawsze ubezpieczony, dlatego wejdź na stronę popularnego sklepu internetowego i pokaż seniorowi, jak powinien wyglądać „bezpieczny sklep". Zwróć uwagę na pasek adresu strony. Bezpieczne połączenie rozpoczyna się od symbolu kłódki i przedrostka „https", który poprzedza adres witryny (nie „http"!). Oczywiście to nie daje nam gwarancji, że strona jest na pewno bezpieczna. Kliknijcie w kłódkę, aby zobaczyć więcej informacji. Sprawdźcie ważność certyfikatu.

Polecamy stronę „bezpieczne przeglądanie" (znajdziecie ją pod tym linkiem: https://transparencyreport.google.com/safe-browsing/search?hl=pl). Można tam rzucić adres danej witryny i sprawdzić czy nie zawiera niebezpiecznych materiałów.

Sprawdzajmy, czy każda podstrona na której jesteśmy, rozpoczyna się od wspomnianego symbolu kłódki i przedrostka „https", a **szczególnie strona płatności**.

W stopce strony muszą znajdować się wszystkie informacje o firmie. Dobrym sposobem na sprawdzenie wiarygodności strony są także opinie na temat sklepu na niezależnych stronach zewnętrznych takich jak opineo czy ceneo.

Co senior powinien zapamiętać z tej części rozmowy? Bezpieczne połączenie rozpoczyna się od symbolu kłódki i przedrostka „https", który poprzedza adres witryny. Zawsze sprawdzamy, czy takie symbole posiada strona płatności.

Poczta elektroniczna: porozmawiajmy o spamie

Jeśli senior się zgodzi, przejrzyjcie jego skrzynkę w celu poszukania przykładu spamu. Usuńcie wszystkie niechciane reklamy i porozmawiajcie o szczególnych rodzajach spamu czyli phishingu i scamie. Nie musisz używać obcobrzmiących nazw, po prostu opowiedz o tych groźnych zjawiskach.

Rozpoznanie phishingu może być dla seniora szczególnie trudne, dlatego zaproponuj, aby nigdy nie klikał w linki i załączniki przesłane od nieznanych odbiorców. Jeśli posiada choć odrobinę wątpliwości co do prawdziwości danego maila, najlepiej przed otwarciem skontaktować się z jego nadawcą i ustalić, czy taki mail został rzeczywiście wysłany. Żadne instytucje zaufania publicznego nie wysyłają maili z prośbą o udostępnienie loginu i hasła do konta, ani podania jakichkolwiek poufnych danych.

Klikanie w nieznane linki najczęściej prowadzi do zainfekowania komputera wirusem lub złośliwym typem oprogramowania, które szyfruje wszystkie pliki, a następnie w zamian za ich odszyfrowanie, żąda okupu.

Scam jest łatwiejszy do rozpoznania, ale ponieważ zawsze wiąże się z nim obietnica otrzymania bardzo dużej ilości pieniędzy, często się na niego nabieramy. Jeśli mail nie jest napisany poprawną polszczyzną, a jego treść dotyczy pomocy w odzyskania ogromnego majątku i wysokiej nagrody pieniężnej w zamian za udzielenie wsparcia w sprawie, od razu go usuwamy. Nie ma odstępstw od tej reguły.

Jakie są konsekwencje rozpoczęcia „współpracy” z oszustami? Utrata niemałych pieniędzy.

Co senior powinien zapamiętać z tej części rozmowy? Nigdy nie wolno klikać w podejrzane linki (także od zaufanych instytucji) ani odpisywać na wiadomości od nieznanych nadawców oferujących wysoką nagrodę pieniężną w zamian za pomoc w załatwieniu jakiejś sprawy. ***Takie maile należy od razu kasować.***

NiechzyjeB@l1955: o bezpiecznych hasłach

Zacznij od tego, że hasło do każdego serwisu lub usługi musi być inne. Jasno zaznacz, że gdy wyciekają dane z jakiegoś popularnego serwisu, hakerzy w pierwszej kolejności sprawdzają, czy użytkownicy, których dane wyciekły używają tego samego hasła do logowania się w innych miejscach. To bardzo ważne, bo wiele z tych osób w ten sposób traci oszczędności życia. Jeśli senior używa pytania pomocnicze do resetu hasła, przypilnuj aby nie było to imię wnuczka. Warto zadać sobie trochę trudu, stawka jest wysoka: tu chodzi o bezpieczeństwo. Podpowiedz, że niektóre serwisy posiadają funkcję dwuskładnikowego uwierzytelnienia (np. Gmail, Facebook, Twitter). O co chodzi?

Aby zalogować się na konto należy podać nie tylko login i hasło, ale także kod, który otrzymujemy smsem na nasz numer telefonu. Można tak ustawić tę funkcję, aby kod sms był niezbędny tylko wówczas, gdy logujemy się na nowym urządzeniu. Nie zapomnij wspomnieć o kodach awaryjnych. Należy je posiadać na wypadek zgubienia telefonu, bo jeśli masz aktywne dwuskładnikowe uwierzytelnienie i nie podasz kodu sms, nie zalogujesz się na swoje konto. Poradź, aby wygenerowane kody awaryjne trzymać w kliku kopiach w postaci zaszyfrowanej.

A same hasła? Muszą być unikatowe, trudne i długie. Dobre hasło to ciąg przypadkowych małych i wielkich liter oraz cyfr i znaków specjalnych. Podpowiedz jak zrobić to najłatwiej. Na przykład niech senior wybierze tytuł swojej ulubionej piosenki, a następnie pozamienia niektóre litery na znaki specjalne i doda swoją datę urodzenia (hasło NiechzyjeB@l1955 jest praktycznie nie do złamania 😉). Podkreśl wyraźnie: hasła nie wolno NIKOMU udostępniać.

Co senior powinien zapamiętać z tej części rozmowy? Hasło powinno zawiać małe i wielkie litery, cyfry oraz znaki specjalne i być inne do każdego posiadanego konta. Nie wolno go nikomu udostępniać.

Media społecznościowe też mogą być niebezpieczne

Próby oszustwa zdarzają się również w mediach społecznościowych. Należy się ich szczególnie obawiać gdy wymieniamy wiadomości ze znajomymi korzystając z wewnętrznych komunikatorów. Jeśli konto Twojego znajomego zostanie przejęte przez hakera, prawdopodobnie roześle on do wszystkich kontaktów zawirusowaną wiadomość. Treść takiej wiadomości zachęca do kliknięcia w podany link, np. „mam dla Ciebie niespodziankę”, „dobrze wyszedłeś na tym

zdjęciu” etc. Pod żadnym pozorem nie wolno klikać w takie załączniki. Oszuści podejmują także próby wyłudzenia pieniędzy, najczęściej prosząc o pożyczenie pewnej niewielkiej kwoty na jakiś ważny cel. Jeśli otrzymasz taką prośbę, skontaktuj się ze znajomym telefonicznie zanim prześlesz mu jakiekolwiek pieniądze. Warto przestrzec seniora przed przyjmowaniem do grona znajomych obcych osób. W mediach społecznościowych powinna obowiązywać dokładnie taka sama zasada, jak w „realu” – nie przyjmujemy w domu nieznajomych, bo może się okazać, że mają takie same zamiary jak przestępcy wykorzystujący „metodę na wnuczka”.

Co senior powinien zapamiętać z tej części rozmowy? Należy być wyczulonym na formy oszustwa w mediach społecznościowych. Przy pomocy komunikatora haker może rozsyłać wirusy lub podjąć próbę wyłudzenia pieniędzy.

Pamiętaj o tym, że nie chodzi o to, aby zniechęcić seniora do korzystania z sieci, ale by uczynić go świadomym użytkownikiem Internetu. Pokaż mu kilka fajnych stron, na przykład sprawdźcie razem jak może wyglądać Ziemia w przyszłości (projekt Earth2050), przejrzyjcie zasoby Muzeum Sztuki Nowoczesnej w Warszawie (http://syrena.artmuseum.pl) albo zróbcie wirtualną wycieczkę dookoła świata korzystając z Google Street View. Sprawdźcie też czy nauka nie poszła w las. Rozwiążcie quiz o bezpieczeństwie w Internecie: https://testbezpieczenstwa.specfile.pl/quiz.