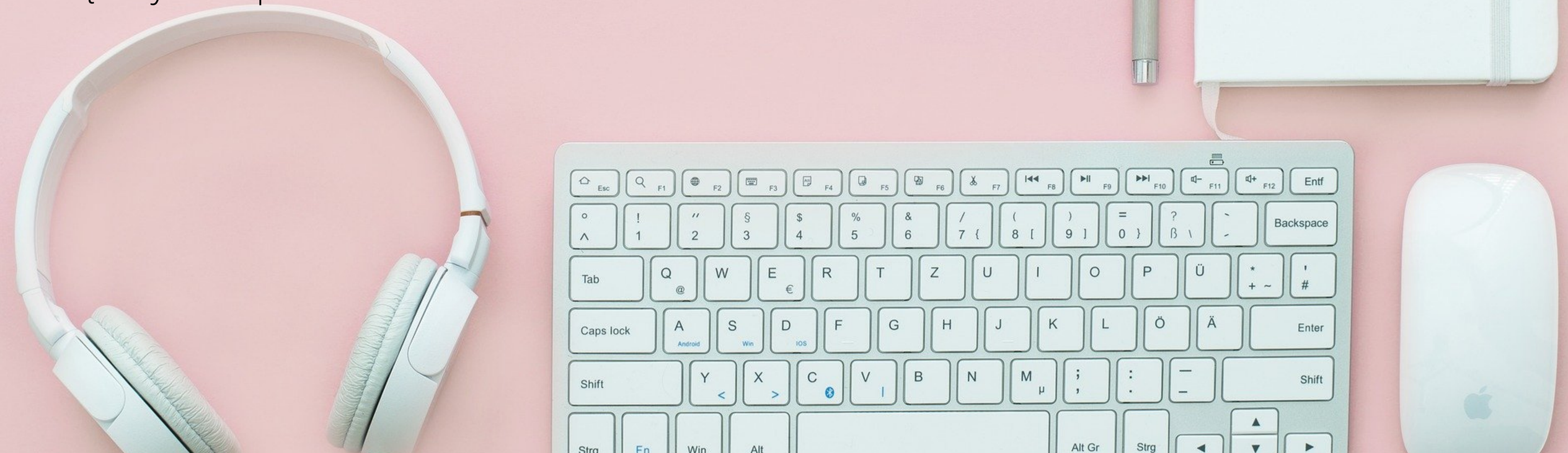
ZESPÓŁ SZKÓŁ
ZS
OSTRÓW LUBELSKI

Bezpieczeństwo w sieci – jakich zasad przestrzegać? O co zadbać?

Trudno wyobrazić dziś sobie życie bez internetu. Korzystamy z niego każdego dnia – w domu, pracy, szkole, restauracji czy na dworcu. Zawsze warto pamiętać o bezpieczeństwie w sieci, ponieważ na użytkowników czeka spora liczba zagrożeń, których istnienia nie każdy jest świadomy. Cyberprzestępcy posługują się różnymi technikami i narzędziami w postaci złośliwego oprogramowania. Przedstawiamy cenne zasady, które pomogą zwiększyć bezpieczeństwo w internecie.



Na jakie zagrożenia użytkownik jest narażony?

Do najpoważniejszych zagrożeń internetowych należy phishing – czyli podszywanie się pod zaufane osoby czy instytucje w celu wyłudzenia poufnych danych osobowych lub pieniędzy. Hakerzy mogą również przejąć dostęp do komputera i przeprowadzać różnego typu szkodliwe operacje. Użytkownikowi grożą m.in. bezpowrotna utrata plików, niestabilna praca systemu czy nawet brak możliwości jego uruchomienia.

Bezpieczny internet – 20 zasad, które warto znać

Poniżej znajduje się 20 porad, których zastosowanie pozwoli zwiększyć bezpieczeństwo w sieci. Zasady będą przydatne zarówno dla „początkujących” użytkowników, jak i osób korzystających z internetu od wielu lat, lecz niezwracających dotychczas większej uwagi na kwestię bezpieczeństwa.

1. Nie otwieraj maili od podejrzanych nadawców

Cyberprzestępcy mogą zainfekować komputer swojej ofiary nawet na skutek samego wyświetlenia przez nią grafik dołączonych do wiadomości mailowej. Warto zatem jak najszybciej usuwać maile od nieznanych i wzbudzających podejrzenie nadawców. Najczęściej będą to wiadomości przesłane z zagranicznej domeny, a ich treść napisana w niedbały sposób – z licznymi błędami gramatycznymi. Tematyka jest zazwyczaj typowa dla SPAM-u, np. powiadomienie o wygranej w konkursie. Pod żadnym pozorem nie należy klikać w linki,ani otwierać załączników znajdujących się w takich mailach.

2. Nie klikaj w reklamy pojawiające się na pulpicie czy w przeglądarce

Do infekcji wirusem, trojanem, oprogramowaniem szpiegującym i innymi szkodliwymi programami może także dojść na skutek kliknięcia w pojawiającą się reklamę. Dlatego warto ignorować tego typu wyskakujące okna i jak najszybciej przeskanować system programem antywirusowym.

3. Twórz trudne do odgadnięcia hasła

Chcąc zadbać o bezpieczeństwo w sieci, należy w jak największym stopniu utrudnić cyberprzestępcom proces rozszyfrowywania haseł – np. do systemu bankowości elektronicznej, poczty, routera czy sieci Wi-Fi. Przede wszystkim warto pamiętać, aby nie używać tych samych loginów i haseł w różnych miejscach sieci. Wyjątkowo łatwe do odgadnięcia są hasła w formie daty urodzenia, imienia czy innych krótkich słów. Znacznie więcej czasu zajmie hakerowi rozszyfrowanie hasła składającego się z wielu znaków – liczb, małych i wielkich liter oraz symboli specjalnych. W prosty sposób można je utworzyć, korzystając z darmowych generatorów online.

4. Pamiętaj o regularnych aktualizacjach

Bezpieczeństwo w internecie w ogromnym stopniu zależy od tego, jak często użytkownik aktualizuje system operacyjny, oprogramowanie antywirusowe, a także wszystkie zainstalowane aplikacje. Dzięki aktualizacjom możliwe jest bieżące usuwanie luk w zabezpieczeniach, które mogłyby cyberprzestępcom posłużyć do przeprowadzenia ataku. Jeżeli nie jesteś w stanie pamiętać o przeprowadzania aktualizacji w ręczny sposób, warto wtedy aktywować opcję ich automatycznego wgrywania.

5. Korzystaj z zapory sieciowej firewall

Zapora sieciowa, zwana również ogniową, to system chroniący komputer znajdujący się w sieci LAN przed nieuprawnionym dostępem z zewnątrz. Firewall monitoruje ruch sieciowy oraz filtruje niebezpieczne połączenia przychodzące i wychodzące. Stanowi więc barierę przed różnego typu zagrożeniami internetowymi.

6. Nie zapominaj o wylogowaniu się z serwisów

Po zakończeniu korzystania z serwisu wymagającego logowania się należy niezwłocznie skorzystać z opcji wylogowania. Jest to istotne zwłaszcza w przypadku korzystania z sieci współdzielonych z innymi użytkownikami – np. w szkole, pracy czy bibliotece. Dzięki wylogowaniu się zmniejszamy ryzyko, że poufne dane zostaną przejęte przez osobę trzecią.

7. Podawaj swoje poufne dane jedynie na stronach z certyfikatem SSL

Jeżeli podajesz w internecie swoje dane – np. rejestrujesz się, wypełniasz formularze elektroniczne czy kupujesz w sklepie online – upewnij się wcześniej, czy dany serwis został zabezpieczony za pomocą protokołu https. Sprawdzisz to, klikając w symbol kłódki, znajdujący się obok adresu strony w przeglądarce. Jeżeli serwis posiada certyfikat SSL, wtedy otrzymasz komunikat „Połączenie jest bezpieczne”.

8. Korzystaj z weryfikacji dwuetapowej w systemach bankowości

Jeżeli logujesz się do banku przez internet, wtedy warto zadbać o bezpieczeństwo w sposób szczególny. Chodzi przecież o twoje pieniądze. Jeżeli strona jest zabezpieczona za pomocą protokołu https, to świetnie, ale możesz jeszcze bardziej utrudnić hakerom zadanie. Przykładem dwuetapowej weryfikacji danych jest konieczność wpisania po zalogowaniu dodatkowo kodu przesłanego na numer telefonu.

9. Pobieraj pliki i programy jedynie z zaufanych źródeł

Jednym z najczęstszych powodów infekcji komputera szkodliwym oprogramowaniem jest pobieranie plików z nielegalnie działających stron. Jeżeli zastanawiasz się, jak być bezpiecznym w internecie, to w żadnym wypadku nie korzystaj z serwisów typu torrent do pobierania filmów. Ściągaj pliki jedynie z zaufanych i legalnych źródeł, których wiarygodności jesteś pewien.

10. Sprawdź, czy razem z programem nie instalujesz dodatkowych narzędzi

Często się zdarza, że podczas instalowania legalnego i przydatnego programu można w pakiecie zainstalować szkodliwe narzędzia firm trzecich, które okazują się być złośliwym oprogramowaniem – np. koniem trojańskim, spyware czy rootkitem. Dlatego zalecamy dokładnie czytać wyświetlane przez kreator instalacji komunikaty i nie godzić się na wgrywanie dodatkowych komponentów.

11. Korzystaj z różnych adresów e-mail

W celu zwiększenia bezpieczeństwa w sieci warto używać kilku adresów mailowych. Najlepiej założyć nową skrzynkę przeznaczoną do zakupów internetowych oraz rejestracji w różnych serwisach. Nie należy takich operacji dokonywać ze swojego głównego konta, ponieważ użytkownik naraża się w ten sposób na przejęcie poufnych danych.

12. Zabezpiecz swój router

Hakerzy mogą przeprowadzić atak poprzez włamanie się do routera. Dlatego warto zmienić w panelu administracyjnym urządzenia domyślne dane. Najczęściej są one bardzo proste do odszyfrowania, gdyż przyjmują formę taką jak np. „admin”.

13. Nie działaj pod wpływem emocji

Cyberprzestępcy przeprowadzają często ataki, próbując wywołać w swoich ofiarach poczucie strachu czy wzbudzić presję czasu. Dlatego posługują się technikami phishingu, np. wymuszając pieniądze czy poufne dane osobowe. Szczególnym przykładem takiego działania są programy typu ransomware, blokujące dostęp do systemu na komputerze. Hakerzy podszywają się pod zaufane instytucje – np. policję, sąd czy biuro bezpieczeństwa, wyświetlając na ekranie monitora komunikat o rzekomym złamaniu prawa przez użytkownika. Obiecują odblokowanie komputera po wpłaceniu okupu w określonym terminie. Warto więc pamiętać, że policja i inne legalnie działające instytucje nigdy nie postępują w ten sposób. Nie należy więc wpłacać pieniędzy ani podawać żadnych poufnych danych.

14. Twórz kopie zapasowe i zapisuj je w różnych miejscach

W wyniku działań cyberprzestępców możesz bezpowrotnie utracić wszystkie cenne dane zapisywane na dysku komputera. Dlatego warto pamiętać o systematycznym wykonywaniu kopii zapasowych. Plików backup nie należy przechowywać na komputerze, lecz na zewnętrznych nośnikach danych (np. pendrive) oraz w wirtualnej chmurze.

15. Nie wchodź na strony o złej renomie i chroń przed nimi swoje dzieci

Niebezpieczne skrypty znajdują się najczęściej na stronach o tematyce erotycznej, hazardowej czy związanej z podejrzanymi transakcjami finansowymi. W związku z tym warto unikać ich odwiedzania oraz chronić przed nimi swoje dzieci – np. za pomocą funkcji ochrony rodzicielskiej.

16. Korzystaj z dobrego pakietu antywirusowego

Aby uchronić swoje urządzenie przed atakami hakerów, warto regularnie skanować system pod kątem obecności wirusów oraz innego typu złośliwego oprogramowania. Powinien być to program monitorujący w trybie rzeczywistym oraz usuwający różnego typu zagrożenia internetowe.

17. Unikaj korzystania z publicznych sieci Wi-Fi

Jeżeli nie musisz, to nie łącz się z internetem poprzez publiczne, ogólnodostępne sieci Wi-Fi. W żadnym wypadku nie podawaj wtedy swoich poufnych danych – nie loguj się do systemów bankowości elektronicznej, poczty
czy różnego typu serwisów transakcyjnych.

18. Używaj oryginalnego systemu operacyjnego oraz legalnych wersji programów

Tylko legalnie działające oprogramowanie jest bieżąco udoskonalane przez producentów i możliwe jest jego uaktualnianie do nowszych wersji. Dzięki temu mogą być usuwane luki w bezpieczeństwie, które umożliwiają hakerom przeprowadzanie niebezpiecznych ataków.

19. Nie otwieraj plików zapisanych na zewnętrznych nośnikach przed ich przeskanowaniem

Zanim otworzysz plik otrzymany na płycie CD, pendrive czy innym zewnętrznym nośniku, pamiętaj o jego przeskanowaniu programem antywirusowym. Pozwoli to uniknąć infekcji komputera rootkitem, koniem trojańskim czy innym szkodliwym oprogramowaniem.

20. Chroń nie tylko komputer, lecz także pozostałe urządzenia

Jeżeli logujesz się do sieci na różnych urządzeniach – nie tylko komputerze, lecz jednocześnie na laptopie czy tablecie – wtedy ochrona samego komputera może okazać się niewystarczająca.

Bibliografia:

- https://www.netia.pl/pl/blog/bezpieczenstwo-w-sieci-jakich-zasad-przestrzegac
- https://www.saferinternet.pl/dbi/o-dbi.html
- https://www.gov.pl/web/edukacja-i-nauka/dzien-bezpiecznego-internetu-2021
- https://epodreczniki.pl/a/bezpieczenstwo-w-sieci/DLcH59Wno
- https://www.telepolis.pl/wiadomosci/bezpieczenstwo/dzien-bezpiecznego-internetu-bezpieczenstwo-w-mediach-spolecznosciowych
- https://www.policja.pl/pol/kreci-mnie-bezpieczenst-1/31098,Dzien-Bezpiecznego-Internetu.html