PODSTAWOWE ZASADY BEZPIECZEŃSTWA W SIECI

Jeśli zachowamy zasady spisane poniżej, możemy śmiało powiedzieć, że zrobiliśmy dużo dla naszego bezpieczeństwa. Stuprocentowej ochrony mieć nigdy nie będziemy. W cyberprzestrzeni ona po prostu nie istnieje.

1. **Nie wchodź na podejrzane strony internetowe**

Używaj tylko bezpiecznych stron internetowych, czyli takich, które służą do edukacji lub kreatywnej zabawy

Jeśli nie jesteś pewny reputacji strony internetowej – nie wchodź na nią. Sprawdź wcześniej w wyszukiwarce jakie są opinie na jej temat. Skorzystaj z serwisów (np. www.virustotal.com), które przeskanują podejrzany adres. Trzeba pamiętać, że nawet samo odwiedzenie „zawirusowanej" strony może doprowadzić do zainstalowania złośliwego oprogramowania na naszych komputerach.

2. **Nie klikaj w linki, których nie znasz**

Nie klikaj w odnośniki (strony internetowe) jeżeli nie pochodzą od zaufanych źródeł (czyli rodzina, bliscy znajomi, nauczyciele). W ten sposób ograniczysz ewentualne wirusy komputerowe.

Jeśli ktoś przysyła Ci link – bądź czujny. Po pierwsze sprawdź nadawcę (czy go znasz i czy spodziewałaś się tej wiadomości). Pamiętaj, że ktoś mógł podszyć się pod nadawcę. Jeśli nie jesteś pewny – zadzwoń do nadawcy i się upewnij.

3. **Nie otwieraj podejrzanych załączników**

Nie odpowiadaj na "zaczepki" osób, których nie znasz realnie.

Jeśli dostałeś wiadomość e-mail z dziwnie wyglądającym załącznikiem, tzn. z dziwną nazwą, z rozszerzeniem, którego nie znasz (.js, .zip, .rar etc.) nie otwieraj! Jeśli dodatkowo w treści maila znajdziesz ponaglenia, żądania zrobienia czegoś jak najszybciej – bądź wyjątkowo czujny, możesz być ofiarą kampanii phishingowej. To znaczy, ktoś chce, żebyś koniecznie wykonał czynność kliknięcia w link lub otworzenia załącznika. Jeśli wiadomość jest napisana bez składu i ładu, z błędami gramatycznymi, bez polskich znaków – możesz być pewien, że jest to próba manipulacji.

4. **Nie klikaj w „Włącz obsługę makr", „Opcje", „Enable content" w dokumentach**

Jeśli postanowiłeś otworzyć załącznik Worda czy Excela (najczęściej spotykane)
i wyskakuje Ci informacja, by „włączyć obsługę makr" lub wyłączyć zabezpieczenia klikając „opcje" lub cokolwiek podobnego – nigdy nie klikaj! Klikasz, znaczy pozwalasz na wykonanie się dołączonego skryptu – przeważnie złośliwego.

5. **Nie wysyłaj swoich poufnych danych zwykłym mailem**

Ilekroć ktoś prosi Cię o przesłania danych osobowych, identyfikacyjnych, – odmawiaj.

6. **Instaluj programy z zaufanych źródeł**

Tak jak możesz zainstalować nieświadomie złośliwe oprogramowania wchodząc na skompromitowaną stronę, czy klikając w link dostarczony Ci wiadomością e-mail, tak możesz je sobie zainstalować, jeśli ściągasz programy z niezaufanych źródeł.

7. **Aktualizuj wszystko Bezpieczeństwo to wyścig.**

Kiedy tylko przestępca zauważy lukę (błąd) w dowolnym programie, od razu będzie chciał ją wykorzystać do przejęcia kontroli nad Twoim komputerem. Jednocześnie programiści odpowiedzialni za daną aplikację, tak szybko jak to możliwe, będą takie luki łatać, czyli dopisywać odpowiednie fragmenty kodu, aby niemożliwe było wykorzystanie zidentyfikowanego błędu. Zatem tak szybko jak to możliwe – instaluj aktualizacje wszystkich programów. Nigdy nie wiadomo, którędy przestępca będzie chciał się włamać – a będzie próbował wszystkiego.

8. **Używaj antywirusa**

To prawda, że oprogramowanie antywirusowe nie uchroni nas przed wyrafinowanym atakiem, ale spowoduje, że większość znanych już wirusów nie będzie dla nas problemem. Zdecydowana większość oprogramowania, które wykorzystują przestępcy jest stara, dlatego też antywirus ciągle pozostaje jedną z podstawowych form zabezpieczenia.

9. **Skonfiguruj zaporę sieciową (firewall)**

Zapora sieciowa musi być włączona. Zdecydowanie zwiększa ona bezpieczeństwo systemu i danych. Chroni komputer przed niepowołanym i niekontrolowanym dostępem zarówno w sieciach publicznych, jak i prywatnych.

Windows Defender całkiem skutecznie zabezpiecza komputer typowego użytkownika domowego. Wchodzi on w skład np. systemu Windows 10, który obecnie jest bardzo popularny na komputerach stacjonarnych i laptopach.

10. **Uważaj na sieci publiczne**

Sieci publiczne są słabo zabezpieczone i zazwyczaj jeden użytkownik może łatwo „podsłuchać” innego. Nie musisz – nie korzystaj. Musisz – szyfruj komunikację.

## 11. Pamiętaj, że danych z Internetu już nie usuniesz

Jeśli upublicznisz jakiekolwiek dane musisz zakładać, że zostaną one w Internecie już na zawsze. Internet też ma swoje archiwum. Zachowaj zasady netykiety w sieci.

## 12. Szyfruj dane swoje

Szyfrowanie to dzisiaj podstawa. Nie tylko w komunikacji (np. https, PGP). Powinieneś również zaszyfrować swoje dyski. Wtedy nawet po kradzieży sprzętu dostęp do danych nie będzie prosty.

## 13. Zadbaj o swoją przeglądarkę

Przeglądarka internetowa to Twoje okno na świat i podstawowe narzędzie pracy. Warto pomyśleć o jej bezpieczeństwie, korzystając zawsze z najbardziej aktualnej wersji.

## 14. Wykonuj kopie zapasowe

Należy liczyć się z tym, że prędzej czy później zostaniemy zaatakowani, utracimy nasze dane i naszym jedynym ratunkiem będzie sięgnięcie po kopię zapasową danych. Po prostu trzeba je mieć.

## 16. Ustal mocne hasło. Wszędzie.

O hasłach napisano już wiele, ale wciąż jest to najsłabsze ogniwo systemu zabezpieczeń. Dlatego przypominamy o nich jeszcze raz. Najłatwiejszą metodą włamań na cudze konto jest odgadnięcie hasła. Użytkownicy nie wykazują szczególnej inwencji w wymyślaniu haseł – najpopularniejsze to imiona (na dodatek pisane małymi literami: “monika”, “maciek”) i popularne kombinacje klawiszowe (“qwerty”, “12345”, “q1w2e3”). Za

szczyt przebiegłości uchodzi utworzenie prostej kombinacji słowno-liczbowej, na przykład “marysia123”. Ale złamanie takich haseł to “pestka”.