Cyberbezpieczeństwoto ogół technik stosowanych w celu obrony sieci informatycznych, struktur wewnętrznych oraz danych. A tak konkretnie, chodzi w nim o obronę swojej sieci, prywatnych danych i bezpieczeństwo w Internecie. Ma na celu jak najlepiej zadbać o to, aby dostarczać rozwiązania dostosowane do potrzeb ludzi, ale w sposób uniemożliwiający wykorzystanie ich przeciwko użytkownikom.

### A czy nas to cyberbezpieczeństwo dotyczy?

<https://threatmap.checkpoint.com>

Na tej stronie można zobaczyć mapę cyberataków aktualizowaną na żywo. Takie mapy zbierają dane z założonych pułapek, rejestrów danych, systemów monitorowania i wielu innych. Zebranie informacje są przetwarzane, a później przedstawiane graficznie. Pozwalają zobaczyć co się wokół nas dzieje, jak często i z jaką intensywnością. A dzieje się dużo. W zeszłym (2022) roku do cyberataku dochodziło co około 40 sekund.

### Ile informacji jest o nas w sieci i skąd się tam biorą?

Zacznę od odrobinkę łatwiejszego pytania, czyli skąd w ogóle w Internecie biorą się nasze dane? Po pierwsze i najważniejsze – sami je tam umieszczamy. Piszemy znajomym, co właśnie robimy, udostępniamy rolki na Instagramie, wchodzimy na przeróżne strony i ślepo klikamy wszędzie akceptuj, aby tylko uniknąć czytania i w końcu dostać do tego, co nas interesuje. To nas gubi. Wiele serwisów w takich umowach wymaga pozwolenia na zbieranie i przetwarzanie danych. Tutaj scenariuszy może być kilka: albo te dane są nieprawidłowo przechowywane i przetwarzane, przez co wyciekają. Taka firma może stać się celem cyberataku, a nasze dane zostaną skradzione i wykorzystane. Najczęściej jednak nasze dane są sprzedawane mniejszym firmom, w celu podsyłania nam reklam i treści dopasowanych do naszego profilu wyszukiwań.

## Na jakie ataki jesteśmy narażeni?

Zdecydowanie najpopularniejszym atakiem jest phishing. Przygotowanie go potrafi zająć od kilku minut aż do wielu dni. Sam atak polega na tym, że cyberprzestępca podszywa się pod znaną osobą lub organizację i grając na naszych emocjach (przede wszystkim strachu, poczuciu niepewności, czasami też możliwości otrzymania nagrody) wyłudza nasze dane osobiste.

Kolejnym popularnym atakiem jest ransomware. Tutaj przez nieumyślne kliknięcie lub ściągnięcie szkodliwego oprogramowania na czyimś prywatnym sprzęcie szyfrowany jest dysk. Hackerzy zazwyczaj kontaktują się z ofiarą przez mail i proszą o niewielki okup w zamian za odszyfrowanie dysku. Ten atak również nie jest trudny w przygotowaniu, raczej nie żąda się dużych pieniędzy, dlatego biorąc pod uwagę skalę jest bardzo opłacalny dla atakujących.

Jeszcze innym zagrożeniem są ataki na infrastrukturę IoT. Zazwyczaj jest kiepsko zabezpieczona, używa domyślnych haseł lub wcale nie używa szyfrowania. Przez to jest stosunkowo łatwym celem dla hackerów.

Więcej na temat ataków można przeczytać tutaj:

<https://www.websiterating.com/pl/research/cybersecurity-statistics-facts/>

## Jak chronić swoje dane?

### **HASŁA. To prawdziwy fundament**

Wszyscy mówią, że trzeba mieć długie i trudne hasło. Na każdej stronie odpowiednia wymagana jest odpowiednia długość, ilość cyfr, małych oraz dużych liter, znaków specjalnych. Dodatkowo każde powinniśmy pamiętać, zmieniać co miesiąc i nigdzie nie zapisywać. Nie oszukujmy się, w normalnym życiu jest to trudne. Jednak da się mieć dobre hasła i nie zwariować!

Można używać zasady pełnych zdań. Wybieramy cytat, powiedzenie, krótką rymowankę, zmieniamy tam jakiś wyraz albo po prostu się inspirujemy i tworzymy własny krótki ciąg znaków. Jeśli będzie się składało z około 5 wyrazów, zapewne jest silnym hasłem!

Świetną opcją jest użycie swojej wyobraźni i stworzenie jakiejś sceny, jaką będziecie mogli skojarzyć z danym serwisem. Do logo Facebooka sama skojarzyłam *niebieskieLADOWISKOdla2malychSAMOLOTOW*. To hasło zawiera duże i małe litery, cyfry, a do tego jest długie! Zawiera też elementy abstrakcyjne.

Dobrze jest nie tworzyć haseł odnoszących się do rzeczy jakie mamy pod ręką. Po pierwsze dlatego, że takie wymyślne są fajniejsze, po drugie pod ludzi można tworzyć słowniki, a jak mamy z czymś styczność na co dzień to łatwiej na to postawić i jest większa szansa, że ktoś też na to wpadnie.

Kolejna świetna opcja to mieszanie języków. Zazwyczaj podczas przygotowywania ataku bierze się pod uwagę jeden język, dlatego użycie wyrazów spoza zakresu języka jest zabiegiem wymykającym się większości ataków słownikowych.

*I$mDANCINGsobieWdeszczu*

Siłę hasła i przybliżoną ilość czasu potrzebną do jego złamania można sprawdzić tutaj:

<https://www.passwordmonster.com>

### **Największe zagrożenie - phishing**

Problemem, z którym borykamy się aktualnie najbardziej jest właśnie phishing. W tych wiadomościach tendencję do wywierania na nas presji, grania na emocjach. Mamy mieć poczucie, że coś się dzieje i MUSIMY DZIAŁAĆ TERAZ. Nie zastanawiać się, a ratować swoje dane i rzeczy. To dlatego, że celem phishingu nie jest sprzęt, a my sami.

Warto sprawdzić swoją wiedzę o phishingu na tej stronie:

<https://kwestiabezpieczenstwa.pl/phishing/>

Jak rozpoznać taką wiadomość phishingową? Przede wszystkim należy na spokojnie i z chłodną głową zastanowić się, czy dana firma ma w zwyczaju zachowanie, o jakim nas informuje. Normalnym jest otrzymanie powiadomienia o wykorzystaniu limitu danych w telefonie, ale informacja o wygraniu nowego iPhone’a powinna budzić podejrzliwość. Zawsze należy zwracać uwagę na poprawną polszczyznę i emoji w wiadomościach, od poważnych firm. Wszelkie linki należy sprawdzać wpisując w innym oknie przeglądarki na przykład „rzekoma\_nazwa\_organizacji strona” lub „rzekoma\_nazwa\_organizacji mail”. W ten sposób łatwo zweryfikować, czy ktoś podsyła nam prawidłowe linki. Tak samo sprawdzić można podejrzany numer telefonu.

**Warto mieć też w pamięci kilka zasad postępowania z podejrzanymi wiadomościami:**

* Przede wszystkim należy zachować spokój!
* Adresy email oraz linki do stron należy sprawdzić na wyszukanych samodzielnie stronach, za które podaje się nadawca wiadomości
* Logować się na swoje konta tylko z zakładek
* Uważać na wszelkie błędy ortograficzne i językowe
* Zastanowić się, czy dana firma rzeczywiście mogłaby przysłać taką wiadomość

## Bezpieczna przeglądarka i komunikator

Bezpieczne, to znaczy jakie? Dla mnie to znaczy zapewniające szyfrowanie przesyłanych danych, wspierane przez dos Na nasze szczęście twórcy przeglądarek to całkiem solidne firmy. Pod warunkiem, że aktualizujemy przeglądarkę, a najlepiej też nie pozwalamy na ciasteczka, to same w sobie powinny być dla nas bezpieczne.

Podobnie sytuacja ma się z komunikatorami. Zbyt wielu ludzi na nich polega, żeby ich dostawcy mogli pozwolić sobie na błąd. Pamiętając o aktualizacjach i uważając na potencjalnie niebezpieczne wiadomości możemy z nich korzystać spokojnie!

# Jak żyć, czyli co i kiedy warto udostępniać w sieci?

Zawsze warto 3 razy zastanowić się, czy faktycznie chcemy podzielić się czymś ciekawym, a także czy za 5 lat chcielibyśmy, aby to latało sobie po sieci. Nigdy nie dzielmy się nowym sprzętem, ani dłuższą nieobecnością w domu, ponieważ tylko tworzymy komuś okazję do tego, aby nas okraść.

Nie mamy pojęcia, do kogo trafią nasze zdjęcia, dlatego powinno się kasować nasze metadane (dane o danych, związane ze szczegółami technicznymi i lokalizacją utworzenia) ze zdjęć. Pamiętajmy, że nieraz w tle zdjęcia (szukając danego krajobrazu czy charakterystycznego budynku) znajdują się informacje o naszych ulubionych miejscach lub aktualnej lokalizacji!

Przed udostępnieniem czegokolwiek należy też zadać sobie pytanie, czy to dobry pomysł? Nie jesteśmy w sieci anonimowi, a skojarzone z nami treści już nigdy z internetu nie uciekną. Przez to nie warto umieszczać tam żadnych obraźliwych ani kompromitujących kogokolwiek informacji.

W dzieleniu się sukcesami, ciekawymi wydarzeniami z życia czy fajnymi miejscami nie ma nic złego! Ważne jednak, aby umieszczać w nich żadnych wrażliwych informacji o sobie oraz dodawać je po powrocie do domu.

Na koniec artykuł na temat publikowania w sieci:

<https://sergiuszdiundyk.pl/jak-bezpiecznie-publikowac-zdjecia-w-internecie>

Opracowała:

Paulina Kołodziejczyk