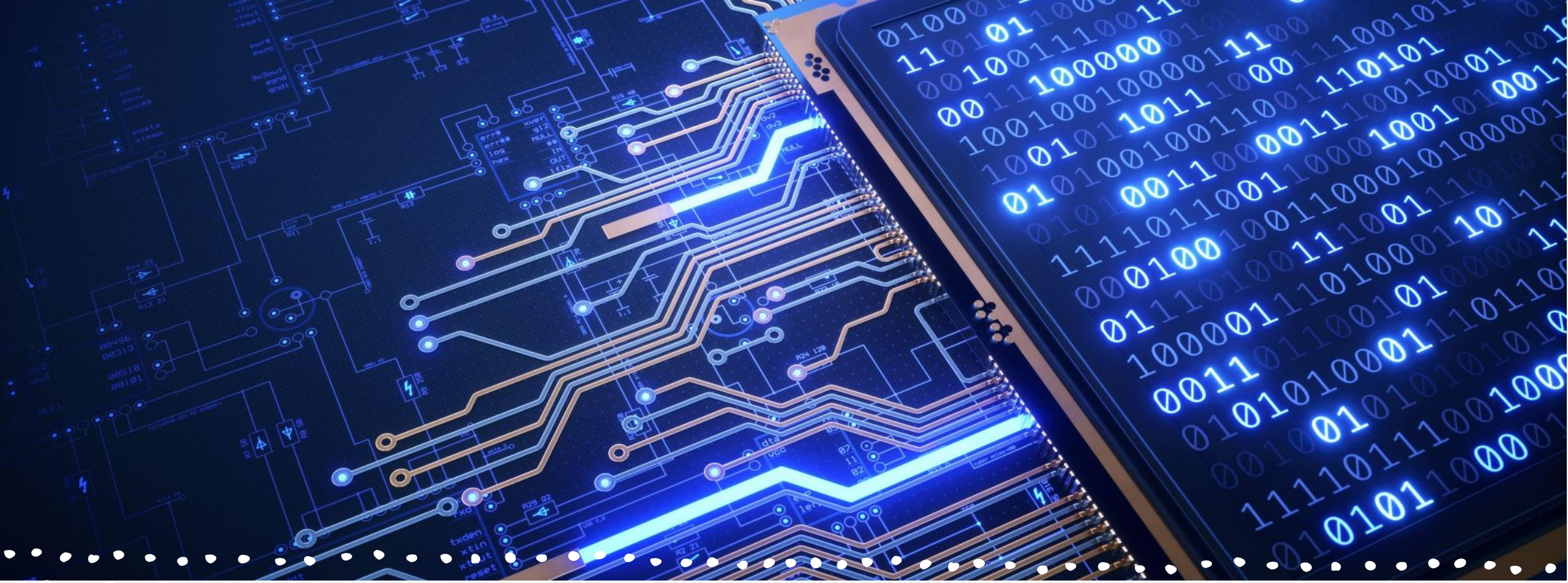

Bezpieczeństwo w internecie

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.

Zachowaj szczególną ostrożność wchodząc w linki

- Bardzo częstym sposobem atakowania prywatności i wyciągania danych są rozsyłane na skrzynki pocztowe wiadomości e-mail, zawierające dziwne załączniki lub proszące o kliknięcie w jakieś linki. To tak zwany **phishing.** Nie istnieje jeden i do tego 100-procentowo pewny sposób na obronę. Najlepiej po prostu uważać i nigdy ich nie otwierać. Znacznie bezpieczniejsze jest samodzielne wchodzenie na interesującą Cię stronę.

W internecie nic nie ginie

- Bądźcie dyskretni. Informacje, które publikujecie, stają się publiczne i widoczne dla wszystkich. Nie wstawiajcie informacji lub obrazków, których nie chcecie udostępniać całemu światu. Uważajcie – mogą zostać przekazane dalej!
- Bądźcie anonimowi. Nie dzielcie się prywatnymi lub bardzo osobistymi informacjami. Nigdy nie zamieszczajcie lub wysyłajcie czegokolwiek, co może posłużyć do zlokalizowania was lub innej osoby (na przykład imienia i nazwiska, adresu e-mail, czy też adresu domowego lub numeru telefonu).

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.

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.

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.

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. Użytkownicy Netii mogą korzystać z usługi Bezpieczny Internet, w ramach której korzystają z oprogramowania antywirusowego z funkcją ochrony sieciowej i kontroli rodzicielskiej. System ten pomaga skutecznie zadbać o bezpieczeństwo w sieci.

Szyfrowanie plików na dysku

- Dysk Twojego komputera to mnóstwo cennych danych i informacji na Twój temat. Aby dobrze go zabezpieczyć, konieczne jest jego szyfrowanie (na przykład funkcja Bitlocker czy VeraCrypt).
-

Jak możesz dowiedzieć, czy mój komputer został zhackowany

1. **Wiesz, że Twój komputer został zhackowany i naruszony, jeśli zobaczysz następujące znaki:**
2. Twoje hasła lub ustawienia online zostały zmienione
3. Hasła do konta lokalnego komputera zostały zmienione lub zobaczysz nowe konta użytkowników
4. Widzisz dziwne posty "zrobione przez ciebie" w swoich kanałach społecznościowych. A może Twoi znajomi otrzymują nieodpowiednie wiadomości, rzekomo od Ciebie.
5. Twoi znajomi zgłaszają otrzymywanie od Ciebie dziwnego spamu lub wiadomości e-mail.
6. Nowe programy lub paski narzędzi zostały zainstalowane na komputerze.
7. Otrzymujesz wiadomości z fałszywego oprogramowania antywirusowego lub innego nieuczciwego oprogramowania

Zmiana haseł online

- Jeśli zauważysz jedną lub więcej Twoich haseł online zmieniło się na sud denly, najprawdopodobniej zostałeś zhackowany. Zazwyczaj dochodzi do tego, że ofiara bezwiednie reaguje na autentycznie wyglądający e-mail phishingowy, rzekomo rzekomo pochodzący z usługi, kończący się zmienionym hasłem. Haker zbiera informacje logowania, loguje się, zmienia hasło i używa usługi do kradzieży pieniędzy od ofiary lub znajomych ofiary. Zobacz, jak możesz uniknąć ataków i ataków polegających na wyłudzaniu informacji. i podejmij kroki, aby zapobiec kradzieży tożsamości w Internecie.

Kwota brakująca na koncie bankowym

- W razie nieszczęścia możesz stracić wszystkie swoje pieniądze jeśli haker uzyska dostęp do Twoich danych osobowych (karta kredytowa, dane bankowości internetowej itp.). Aby tego uniknąć, włącz powiadomienia o transakcjach, które wysyłają alerty tekstowe, gdy wydarzy się coś niezwykłego. Wiele instytucji finansowych pozwala na ustalanie progów kwot transakcji, a jeśli próg zostanie przekroczony lub trafi do obcego kraju, zostaniesz ostrzeżony. Dobrym pomysłem byłoby zastosowanie się do wskazówek dotyczących bankowości internetowej.
-

Fałszywe komunikaty antywirusowe

- Fałszywe komunikaty ostrzegawcze antywirusowe są jednymi z najpewniejszych śladów po zaatakowaniu systemu. Kliknięcie przycisku Nie lub Anuluj w celu zatrzymania fałszywego skanowania antywirusowego nie przynosi żadnych korzyści, ponieważ uszkodzenie już zostało zrobione. Programy te często wykorzystują niezałatane oprogramowanie, takie jak Java Runtime Environment, aby wykorzystać system.

Częste losowe wyskakujące okienka

- Ten problem jest w większości związany z przeglądarkami i wskazuje, że na Twoim komputerze zainstalowano niechciane oprogramowanie lub złośliwe oprogramowanie, ponieważ witryny nie generują generowania szkodliwych wyskakujących okienek.

Dziękuję za obejrzenie mojej prezentacji 😀😀😀

- Źródła:
- https://pl.joecomp.com/how-do-i-know-if-my-computer-has-been-hacked-and-what-to-do-next
- https://www.google.com/search?q=wikipedia&oq=wiki&aqs=chrome.1.69i57j0i433j46i433j0i433j0i131i433j69i60l3.3054j0j7&sourceid=chrome&ie=UTF-8
- Prezentacje przygotowała: Anna Hanejko