BEZPIECZEŃSTWO W SIECI

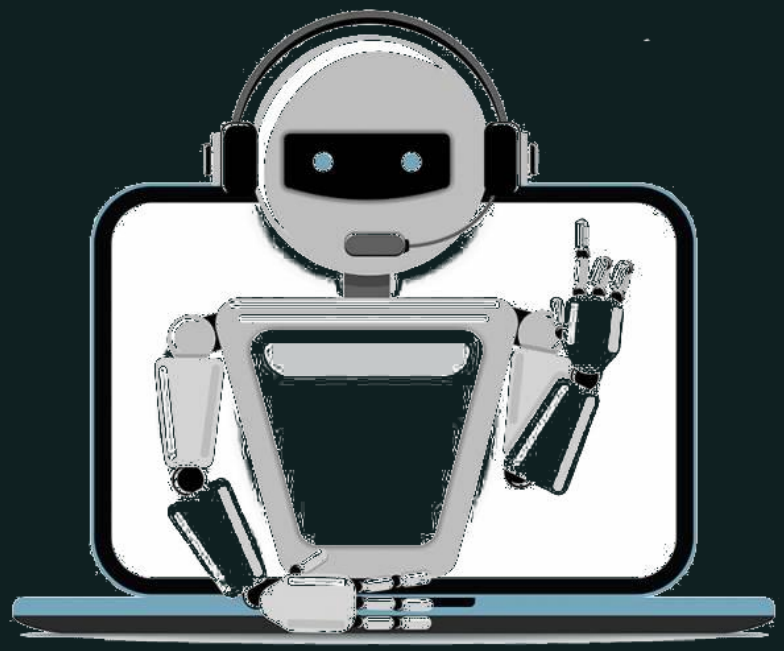
Internet jest miejscem rozrywki, zdobywania wiedzy i informacji. Za jego pośrednictwem załatwiamy ważne sprawy i udostępniamy prywatne dane. Dlatego też powinniśmy dbać o to, aby nie uzyskały do nich dostępu niepowołane osoby.

Słownik ważnych pojęć

1. **HAKER /CRACKER**
   Osoby dokonujące komputerowych włamań nazywane są hakerami.

2. BOT

Program wykonujący czynności w zastępstwie człowieka. Może służyć do przejmowania kontroli nad komputerami, przeprowadzania ataków czy też kradzieży danych.



3. SPAM

Niechciane wiadomości, na których otrzymanie odbiorca nie wyraził uprzedniej zgody. Kliknięcie na link w takiej wiadomości może uruchomić procedurę instalacji szkodliwego oprogramowania.

4. FIREWALL

Zapora sieciowa – jeden ze sposobów zabezpieczania sieci i systemów przed intruzami. Powstrzymuje hakerów przed włamywaniem się do komputera z zewnątrz.

5. PHISHING

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań

6. RANSOMWARE

Złośliwe oprogramowanie, które po zainfekowaniu systemu szyfruje na nim pliki i foldery, uniemożliwiając dalsze z nich korzystanie. Następnie użytkownik otrzymuje żądanie okupu, którego opłacenie nie daje jednak żadnej gwarancji, że komputer zostanie odszyfrowany.

7. MALWARE

Każde złośliwe oprogramowanie, które stara się zainfekować komputer, telefon lub tablet. Wykorzystywane jest m.in. do rozprzestrzeniania wirusów, przejęcia kontroli nad komputerem i kradzieży poufnych danych.

JAK BEZPIECZNIE KORZYSTAĆ Z INTERNETU

1. AKTUALNE OPROGRAMOWANIE

Każdy system operacyjny i oprogramowanie posiada błędy bezpieczeństwa.

Są one odnajdowane i łatane na bieżąco, ale to użytkownik musi zainstalować aktualizację lub wyrazić zgodę na aktualizacje automatyczne. Jest to jedna z najskuteczniejszych metod na zabezpieczenie urządzenia, za pomocą którego łączymy się z siecią, przed niepowołanym dostępem.

2. FIREWALL I ANTYWIRUS

Zainstaluj oprogramowanie typu firewall, które pozwala ustawić blokadę wszystkich połączeń przychodzących do twojego komputera. Antywirus nie daje stuprocentowej gwarancji bezpieczeństwa, ale skutecznie odsiewa stare i masowe zagrożenia.

3. SILNE I UNIKATOWE HASŁA

Twórz hasła niesłownikowe, nieszablonowe i skomplikowane – każdy dodatkowy znak zwiększa trudność jego złamania. Kiedy to możliwe, korzystaj z dwuetapowej weryfikacji – aby się zalogować nie wystarczy podanie hasła, trzeba jeszcze wpisać kod przesłany na telefon lub maila.

4. OSTROŻNIE Z ZAŁĄCZNIKAMI

Nie otwieraj załączników z niespodziewanymi wiadomościami np. spadek po wujku w Afryce.

5. TRYB PRYWATNY (INCOGNITO)

Jeżeli korzystasz z internetu na czyimś komputerze, włącz tryb prywatny, w który wyposażona jest każda nowoczesna przeglądarka. Po aktywowaniu tej funkcji użytkownik ma pewność, że wszystkie dane wytworzone od tego momentu zostaną usunięte natychmiast po przejściu w normalny tryb lub zamknięciu przeglądarki.

6. W INTERNECIE NIC NIE GINIE

Wszystko, co umieszczasz w sieci lub udostępniasz nawet jednej zaufanej osobie, traktuj jako publicznie dostępne. Prywatna galeria zdjęć może nagle stać się dostępna dla każdego internauty na skutek błędu w serwisie.

7. SIEĆ WI-FI Z NIEZNANEGO ŹRÓDŁA

Nie korzystaj z publicznie dostępnych sieci wi-fi. Hakerzy mogą rozmieszczać hotspoty w różnych miejscach, aby przechwytywać dane. Zdarza się, że tworzą fałszywe sieci, które udają zaufane.

8. SZANUJ SWOJE DANE OSOBOWE

Gdy zakładasz maila lub rejestrujesz inne konto, nie podawaj adresu zamieszkania. Żadna internetowa usługa nie ma prawa wymagać od ciebie podania danych, które nie są niezbędne do jej działania. Ustal z rodzicami, którymi danymi możesz dysponować, a które chcą chronić.

9. RÓB CZĘSTE KOPIE BEZPIECZEŃSTWA

Rób często kopie bezpieczeństwa swoich plików, można bowiem paść ofiarą przestępców komputerowych. W ostatnim czasie popularnym atakiem jest szyfrowanie dysku przez hakerów, którzy w zamian za odszyfrowanie żądają wysokiego okupu. Nawet jego zapłacenie nie gwarantuje odzyskania plików. Najlepiej mieć aktualną kopię istotnych danych.

Źródła:

https://pixabay.com/pl/vectors/wy%c5%82udzanie-informacji-referencje-6573326
https://pixabay.com/pl/vectors/ostrze%c5%bcenie-alarm-wykryte-2168379/
https://pixabay.com/pl/vectors/atak-niezabezpieczone-laptop-haker-6806140
https://pixabay.com/pl/vectors/bezpiecze%c5%84stwo-internet-haker-dane-5000785
https://pixabay.com/pl/illustrations/bezpiecze%c5%84stwo-profesjonalny-sekret-5199239
https://pixabay.com/pl/illustrations/w%c5%82ama%c4%87-si%c4%99-haker-elita-hakerstwo-813290
https://pixabay.com/pl/illustrations/e-mail-poczta-przep%c5%82ywu-4009691
https://s3-eu-west-1.amazonaws.com/media-wp-tomhrm/wp-content/uploads/2017/09/05173216/password.png
https://www.gov.pl/photo/format/260b9610-f36e-4098-9fb6-c1e96c5c00bd/resolution/729x308
https://jaklatwo.pl/wp-content/uploads/2020/08/incognito-2231825_1920-696x380.png
https://i.ytimg.com/vi/xyvmCi-VkoY/maxresdefault.jpg
https://kapitanhack.pl/wp-content/uploads/2020/02/wifite-wifi-hacking-tool.gif
https://www.backupacademy.pl/wp-content/uploads/2013/06/Backup-And-Recovery-Services.jpg
https://hejdom.pl/images/2019/10/07/backuphassio.png
https://pixabay.com/pl/vectors/aktualizacja-internet-sie%c4%87-97888
https://biblioteka.pl/artykul/Bezpieczenstwo-w-internecie/9692