BEZPIECZEŃSTWO W SIECI
I OCHRONA SWOJEGO KOMPUTERA

Sposoby na zabezpieczenie swojego komputera

Wiele osób martwi się o bezpieczeństwo danych przesyłanych przez sieci. Szczególnie niebezpieczne są sytuacje, gdzie nasze komputery / smartfony dostępne są dla innych (niepowołanych) osób.

1. Wyłącz automatyczne logowanie

Jeśli włączono automatyczne logowanie, podczas uruchamiania Maca pomijany jest etap sprawdzania hasła użytkownika. Oznacza to, że każdy może uruchomić nasz komputer i uzyskać dostęp do wszystkich plików. Aby tego uniknąć, wystarczy przejść do panelu preferencji Accounts, kliknąć opcję Login Options i usunąć zaznaczenie opcji Automatically Log In As.

2. Wstaw pytanie o hasło po obudzeniu komputera

Wygaszacz ekranu świetnie chroni zawartość ekranu przed wścibskimi oczami, ale wystarczy poruszać myszą lub nacisnąć dowolny klawisz, aby ta zasłona zniknęła.

3. Zablokuj pęk kluczy

Większość aplikacji może zapisywać różnego rodzaju hasła i klucze w pęku kluczy (Keychain); obejmuje to programy pocztowe, przeglądarki internetowe i wiele innych programów. Keychain potrafi także automatycznie wypełniać pola formularzy w przeglądarce Safari.

4. Zapisz poufne dane na zaszyfrowanym obrazie dysku

Jeśli poufne są tylko niektóre pliki znajdujące się na dysku twardym, można umieścić je na zaszyfrowanym obrazie dysku z ochroną hasłem. Zamontowanie takiego obrazu w systemie wymaga podania hasła. Po zakończeniu pracy z plikami wystarczy „odmontować" plik z biurka, aby dane znów stały się całkowicie bezpieczne.

5. Wymazuj poufne pliki

Nawet usunięte pliki można odzyskać po pewnym czasie. Dzieje się tak, gdyż poszczególne fragmenty pliku w dalszym ciągu znajdują się na dysku. Istnieją programy, które umożliwiają odtwarzanie takich usuniętych plików. Aby całkowicie skasować poufne dokumenty, należy wybrać polecenie Finder: Secure Empty Trash. Spowoduje to kilkakrotne nadpisanie usuwanych plików, przez co ich odzyskanie będzie praktycznie niemożliwe.

6. Aktualizuj oprogramowanie zabezpieczające

Regularne instalowanie aktualizacji oprogramowania antywirusowego zabezpiecza przed większością ataków.

7. Nie klikaj łączy w spamie

Spam sam w sobie nie jest niebezpieczny - problemy powstają dopiero w zależności od tego, co użytkownik zrobi po jego otrzymaniu. Na przykład jeśli spam zachęca użytkownika do kliknięcia łącza w celu uzyskania dalszych informacji, mogą zacząć się kłopoty. Nigdy nie klikaj łączy zawartych w takiej wiadomości, a unikniesz ataków typu phishing i pobrania szkodliwego oprogramowania.

(Nie)bezpieczny Internet

W dzisiejszych czasach młoda osoba przestaje interesować się wyłącznie aplikacjami czy grami, a zaczyna powoli poznawać różne zakątki świata Internetu. W tym miejscu zaczyna się problem, a zagrożenia w sieci stają się realne.

Cyberkradzież

Dzisiaj niektórzy szybko uczą się, jak osiągnąć swój cel – zarówno w realu, jak i w świecie wirtualnym. Takie zachowanie staje się problemem, gdy ktoś wyznaczy sobie niewłaściwy cel.

W Polsce i na świecie znane są przypadki kradzieży wirtualnych dóbr, których finał znalazł miejsce w sądzie.

W przypadku, o którym piszę, chodziło o włamanie się na konto jednego z graczy i przejęcie z tego konta wirtualnych dóbr w postaci zdolności i wyposażenia postaci, jaką stworzył w grze okradziony gracz.

Sprawa była potraktowana poważnie, włączając w to zaangażowanie policji. Podczas dochodzenia wyceniono, że zakup tych wirtualnych dóbr na platformie z grą stanowił równowartość paru tysięcy złotych. A to oznacza, że taka kradzież traktowana jest jak przestępstwo, a nie jak wykroczenie. A wiadomo, że od 2017 r. kradzież czegokolwiek o wartości powyżej 400 zł jest traktowane właśnie jak przestępstwo.

Nałogowe online

Z badań UNICEF (źródło: Raport UNICEF: 1 na 3 użytkowników Internetu to dziecko) wynika, że 71% młodzieży jest online. Dla porównania, dorośli online stanowią tylko 48% społeczeństwa. W Europie tylko 4% dzieci nie ma dostępu do sieci, reszta uzyskuje dostęp na różne sposoby - począwszy od wykupionej przez rodziców usługi dostępu, przez darmowe hotspoty (miastowe lub w hotelach czy restauracjach), na włamywaniu się do istniejących sieci Wi-Fi skończywszy.

Potrzeba bycia „online" prowadzi do chorobowego uzależnienia u dzieci i młodzieży. Niektórzy są tak zaangażowani w gry, poświęcają im tyle godzin na dobę, że zaburzają sobie prawidłowy rytm dnia i nocy. Przyczyną niewyspania jest ciągłe granie lub monitorowanie sieci społecznościowych. W skrajnych przypadkach, dłuższy stan niesypiania może być przyczyną powstawania depresji czy innych zaburzeń psychicznych.

Kto może Ci udzielić pomocy?

- Bursa,
- Szkoła,
- Policja,
- Zespoły pomocowe, np. helpline.org.pl,

- www.bezpiecznyinternet.org – projekt realizowany przez Fundację Kidprotect.pl, która jest organizacją pozarządową o charakterze non-profit. Jej celem jest szeroko pojęta ochrona dzieci i młodzieży przed zagrożeniami czyhającymi na nie w świecie realnym, jak i w Internecie. Fundacja prowadzi najstarszy w Polsce hotline, do którego można zgłosić incydenty związane z pornografią dziecięcą oraz pedofilią.

Dbajmy o nasz komputer czy smartfon oraz bezpiecznie korzystajmy z zasobów sieci ☺

Pozdrawiam
Mateusz Czepek