

**BEZPIECZNE I ODPOWIEDZIALNE
KORZYSTANIE Z MEDIÓW
SPOŁECZNOŚCIOWYCH
I BEZPIECZNE UMIESZCZANIE
INFORMACJI W INTERNECIE**

CZYM SĄ MEDIA SPOŁECZNOŚCIOWE?

Media społecznościowe (ang. Social Media) to wirtualne miejsca, gdzie ludzie mogą dodawać (wpisy, wideo, obrazy), a inni to oglądają komentują i odpowiadają. To jak rynek miejski, na którym ludzie się spotykają, tylko przeniesiony do Internetu. Albo jak oglądanie rodzinnych albumów, ale w Internecie. Ludzie robią to codziennie.

ZASADY BEZPIECZNEGO KORZYSTANIA Z SOCIAL MEDIÓW

- Utwórz silne hasło,
- Korzystaj tylko z oficjalnych aplikacji sieci społecznościowych,
- Używaj programu antywirusowego,
- Nie odpowiadaj na wiadomości jeśli nie znasz nadawcy,
- Prywatne informacje pozostaw prywatnymi,
- Nie używaj wulgaryzmów,
- Ogranicz dostęp do konta;

UTWÓRZ SILNE HASŁO

Konto w serwisie społecznościowym zabezpiecz niepowtarzalnym i odpowiednio długim hasłem. Każde hasło powinno być nie tylko silne, ale też niepowtarzalne. Hasło nie powinno zawierać twojego imienia lub nazwiska ani daty urodzenia, ponieważ jest wtedy łatwe do odgadnięcia. Bezpieczne hasło powinno zawierać co najmniej 8 znaków, w tym małe i duże litery, cyfry, znaki specjalne oraz znaki specyficzne dla danego języka. Hasło do każdego konta powinno być inne.



KORZYSTAJ TYLKO Z OFICJALNYCH APLIKACJI SIECI SPOŁECZNOŚCIOWYCH

Aplikacje pobieraj wyłącznie z oficjalnych sklepów — np. Google Play dla Android, App Store dla iOS i Microsoft Store dla Windows.



UŻYWAJ PROGRAMU ANTYWIRUSOWEGO

Dobry program antywirusowy zatrzyma złośliwe oprogramowanie, zanim jeszcze zostanie ono pobrane do systemu. Najpopularniejsze przeglądarki internetowe ostrzegają o podejrzanych stronach internetowych – poważnie traktuj takie ostrzeżenia i nie odwiedzaj tych stron. Mogą zawierać złośliwe oprogramowanie, które umożliwi przestępcom przejęcie kontroli nad Twoim urządzeniem.



NIE ODPOWIADAJ NA WIADOMOŚCI JEŚLI NIE ZNASZ NADAWCY

Serwisy społecznościowe to doskonałe narzędzie dla hakerów próbujących wyłudzić cenne informacje od nieświadomych użytkowników. Jeśli więc otrzymałeś wiadomość od nieznanego najlepiej zwyczajnie ją zignoruj.



NIE UŻYWAJ WULGARYZMÓW

Jeżeli widzisz, że ktoś pisze w sieci wulgaryzmy powinienes to zgłosić do odpowiednich osób.



OGRANICZ DOSTĘP DO KONTA

Uaktywnij dwuskładnikowe uwierzytelnianie na wszystkich swoich kontach. Można z niego korzystać w większości serwisów społecznościowych. To nic trudnego.

PRYWATNE INFORMACJE POZOSTAW PRYWATNYMI

Różnice między „realnym” życiem, a rzeczywistością wirtualną coraz bardziej się zacierają. Możliwość nawiązania kontaktu poprzez social media jest bardzo ważna – obecnie korzystają z tego nawet firmy rekrutujące pracowników. Pamiętaj jednak, by prywatnych informacji kontaktowych nie oferować nikomu, kogo dobrze nie znasz w „realu”.



ODPOWIEDZIALNE UMIESZCZANIE INFORMACJI W INTERNECIE

Zaczynamy udostępniamy jakieś zdjęcie, wiadomość powinniśmy zastanowić się czy to komuś nie zaszkodzi i nie narusza kogoś prywatności, ponieważ jest to karalne. Pamiętajmy, że to co trafi do sieci już na zawsze tam zostanie nawet jeżeli to usuniemy.

ZA JAKIE ZACHOWANIE W INTERNECIE MOŻEMY ZOSTAĆ UKARANI?

Możemy zostać ukarani np. za

- Kradzież cudzej pracy,
- Za hejt
- Za opublikowanie nie swojej pracy/zdjęcia bez zgody autora;



CO JEŻELI UŻYJEMY KOGOŚ PRACY?

Jeżeli pobieramy czyjeś zdjęcie lub prace
powinniśmy podać jego źródło, wykupić licencje lub
skontaktować się z autorem.

Źródła informacji:

https://pl.wikipedia.org/wiki/Media_spo%C5%82eczno%C5%9Bciowe

<https://steemit.com/polish/@entuir/jak-stworzyc-trudne-do-zlamania-i-latwe-do-zapamietania-haslo>

<https://www.iobit.com/pl/online-password-generator.php>

<https://www.gov.pl/web/baza-wiedzy/bezpieczni-w-mediach-spolecznościowych--praktyczne-wskazowki>

<https://rootblog.pl/sklep-play-sie-zmienia-google-rezygnuje-z-dawnego-menu/>

<https://imagazine.pl/2021/08/27/apple-placi-100-milionow-dolarow-i-zgadza-sie-na-wiele-zmian-w-app-store/>

<https://teamnet-software.pl/kategoria/licencje/antywirus-dla-instytucji/antywirus-dla-urzedow/>

<https://androidbeztajemnic.wordpress.com/2017/05/11/samsung-rozpoczyna-wspolprace-z-mcafee-antywirus-ten-bedzie-preinstalowany-na-urzadzeniach-producenta/>

<https://wiadomosci.onet.pl/poznan/pila-wpadl-haker-szantazujacy-firmy-energetyczne/hkth7cI>

<https://hunters.pl/7-zasad-bezpieczenstwa-w-mediach-spolecznościowych/>

<https://lozbjn.edu.pl/bi/prawo.html>

<https://salwowski.net/2016/02/13/dlaczego-winnismy-sie-strzec-wulgaryzmow/>

<https://spolecznosc.ing.pl/-/Blog/7-sposob%C3%B3w-jak-chroni%C4%87-swoj%C4%85-prywatno%C5%9B%C4%87-w-sieci/ba-p/4850>

DZIĘKUJE ZA UWAGĘ