

Bezpieczne
i odpowiedzialne
korzystanie z mediów
społecznościowych

Media społecznościowe

Media społecznościowe to rozwiązania wykorzystujące technologie internetowe i mobilne, umożliwiające komunikowanie się poprzez interaktywny dialog. W dzisiejszych czasach wiele ludzi z nich korzysta. Według danych Hootsuite „Digital 2020” jest to aż 19 milionów Polaków. Social media „zabierają” nam średnio dwie godziny życia dziennie. Należy pamiętać aby używać ich odpowiedzialnie, ponieważ możemy trafić na wiele zagrożeń.





Zagrożenia w mediach społecznościowych



- Spośród wielu zagrożeń należy zwrócić uwagę na to co publikujemy w sieci. Wiadomo, że w Internecie nie ginie żadna informacja. Nasz przyszły pracodawca może ocenić naszą osobę po tym co wstawiamy np. na Facebooka.
- Problemem w social mediach jest też to, że nigdy nie wiemy kto jest po drugiej stronie. Spotykanie się z nowo poznanymi osobami w Internecie może mieć poważne konsekwencje.
- Musimy brać pod uwagę fakt, że publikowane przez nas treści są poddawane ocenie innych osób. Konsekwencją tego może być hejt.

Jak bezpiecznie odpowiedzialnie korzystać z mediów społecznościowych?

Większość działań na platformach społecznościowych opiera się o nasze prywatne dane, począwszy od rejestracji, udostępniania zdjęć, postów, aktualności z życia, dołączania do wydarzeń i różnego rodzaju grup. Nasze dane są bardzo atrakcyjne dla cyberprzestępców – mówi minister Marek Zagórski. Aby być bezpiecznym należy się stosować do kilku zasad.





Złote zasady



1. **Utwórz silne hasło.** Konto w serwisie społecznościowym zabezpiecz niepowtarzalnym i odpowiednio długim hasłem. Wiele użytkowników korzysta z tego samego hasła do wielu kont. To niedobrze. Każde hasło powinno być nie tylko silne, ale też niepowtarzalne.
2. **Ogranicz dostęp do konta.** Uaktywnij dwuskładnikowe uwierzytelnianie na wszystkich swoich kontach. Można z niego korzystać w większości serwisów społecznościowych.

Złote zasady

3. **Tylko prawdziwi znajomi.** Dodawaj do listy znajomych wyłącznie osoby, które rzeczywiście znasz i którym ufasz. Pamiętaj, że przyjmując nową osobę do grupy swoich znajomych najczęściej domyślnie udostępniasz jej swoje prywatne zdjęcia oraz informacje o sobie.
4. **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.

Złote zasady

5. **Dbaj o prywatność.** Praktycznie wszystkie serwisy społecznościowe posiadają rozwiązania zwiększające prywatność – aktywuj je!
6. **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.

Funkcjonowanie Internetu i wynikające z tego zagrożenia



Nie każdy użytkownik sieci wie, czym jest cyberprzestrzeń. Definicja jasno mówi, że jest to przestrzeń wirtualna służąca do gromadzenia, wymiany i udostępniania informacji. Powinniśmy pamiętać, że każda informacja umieszczona w Internecie powinna być traktowana jako informacja publiczna. Dlatego zanim zdecydujesz się podzielić jakimikolwiek informacjami, odpowiedz sobie na pytanie, czy ich ujawnienie Ci nie zaszkodzi. Wszystkie dane umieszczone w Internecie prędzej czy później mogą bowiem zostać ujawnione.



Bezpieczeństwo informacji w Internecie

Mimo największej ostrożności niektórych sytuacji mających wpływ na bezpieczeństwo informacji w Internecie nie da się jednak uniknąć. Do podstawowych zagrożeń można zaliczyć:

- **błędy człowieka** – kiedy do wycieku informacji dochodzi ze względu na zaniechanie, brak wiedzy albo umyślne działanie administratorów systemu lub ich użytkowników,
- **awarie** – problemy techniczne ze sprzętem czy oprogramowaniem, które uniemożliwiają jego normalne funkcjonowanie,
- **katastrofy** – wszystkie zdarzenia mające charakter losowy, takie jak powódzie, trzęsienia ziemi, pożary oraz wypadki, w których zawinił człowiek, jak np. katastrofy budowlane czy komunikacyjne, prowadzące do zakłóceń funkcjonowania systemów,
- **celowe działania** – ataki ukierunkowane na kradzież sprzętu i zasobów informacji.

Czy wysłanie zdjęć przez Internet jest bezpieczne?

Oczywiście że nie! W większości wypadków, zdjęcie, zrobione kamerą telefonu, pozwoli zidentyfikować którym telefonem zostało zrobione. Można wykryć nie tylko model telefonu, opierając się o dane EXIF i IPTC, ale dokładnie zidentyfikować że to akurat Twój telefon, a nie inny. Zwykłą lustrzankę też da się zidentyfikować. Ale pod kątem nielegalnej (bo, najprawdopodobniej, nie wyraziłeś świadomie i wyraźnie zgody na handel Twoją prywatnością) sprzedaży poufnych danych telefon jest o wiele cenniejszy od kamery dlatego że z niego już dawno są pozyskane Twoje kontakty, inne zdjęcia i inne poufne dane.



Kilka kroków jak bezpiecznie wysyłać zdjęcia do Internetu:

1. Nigdy nie wysyłamy surowych zdjęć.
2. W oryginalnej rozdzielczości wymazujemy wszystkie defekty kamery i defekty skóry.
3. Lekko zaszumiamy i rozmywamy zdjęcie.
4. Poprawiamy kontrast, ewentualnie wyostriamo zdjęcie.
5. Pomniejszamy zdjęcie do minimalnie niezbędnej rozdzielczości.
6. Pilnujemy żeby obraz nie skompromitował nas w przyszłości, w razie czego edytujemy.
7. Zapisujemy zdjęcie do pliku JPG o jakości nie przekraczającej 85%.
8. Otwieramy obrobione zdjęcie w programie do wyświetlania zdjęć.

Autor:
Martyna Pączyńska

Źródła

- <https://pixabay.com/pl/illustrations/medi%c3%b3w-spo%c5%82ecznych-spo%c5%82eczny-5187243/>
- <https://www.gov.pl/web/baza-wiedzy/bezpieczni-w-mediach-spolecznosciowych--praktyczne-wskazowki>
- <https://www.digitalamiga.com/2021/11/24/why-is-social-media-an-important-part-of-digital-marketing/>
- <https://www.fulex.com/successful-social-media-tips-for-ecommerce/>
- <https://zadbajobezpieczenstwo.pl/bezpieczenstwo-sieci-informatycznej-hotelu/>
- <https://nadnoteckibank.pl/dla-rolnictwa/oszczednosci-i-inwestycje/>
- <http://pngimg.com/image/10964>
- <https://www.orange.pl/poradnik/twoj-internet/na-czym-polega-bezpieczenstwo-informacji-w-internecie/>
- <https://sergiuszdiundyk.pl/jak-bezpiecznie-publikowac-zdjecia-w-internecie>
- <https://wallpapersden.com/anonymous-hacker-caught-by-police-artistic-wallpaper/1920x1080/>
- <https://www.egospodarka.pl/137041,Zagrozenia-internetowe-w-2017-roku-wg-Kaspersky-Lab,1,12,1.html>
- <https://hdqwalls.com/wallpaper/1920x1080/internet-technology>
- <https://bitdefender.pl/portale-spolecznosciowe-i-zagrozenia-jakie-generuja/#:~:text=Kradzie%C5%BC%20danych%20do%20logowania%20i%20innych%20poufnych%20informacji,kt%C3%B3re%20mo%C5%BCemy%20natkn%C4%85%C4%87%20si%C4%99%20zw%C5%82aszcz%C5%82a%20w%20mediach%20spo%C5%82eczno%C5%9Bciowych.>