

Bezpieczeństwo w sieci

Prywatność online

Kto z was korzysta z serwisów społecznościowych? Z jakich?



Jakie prywatne informacje o was znajdują się w tych serwisach?

- Prywatne zdjęcia i filmy
- Nasze opinie – komentarze
- Numer telefonu i inne dane osobowe
- Informacje nt z kim? jak? i gdzie? spędzamy wolny czas
- Inf. o tym kogo znamy, kogo lubimy
- Prywatna korespondencja
- Informacja z jakich stron korzystamy

Czy wiążą się z tym jakieś zagrożenia?

Zastanówcie się, jak zagrożona jest wasza prywatność w sieci?

- ◉ ktoś niepożądany może mieć dostęp do informacji, które podajemy,
- ◉ ktoś może zrobić użytek z naszych zdjęć lub filmów,
- ◉ ktoś może włamać się na nasze konto i zapoznać się z prywatną korespondencją.



Niestety, takie sytuacje zdarzają się bardzo często. Zakładając profile w portalach społecznościowych dbajmy o to, żeby były one prywatne, a nie publiczne i dostępne dla każdego. Tymczasem podstawą korzystania z serwisów społecznościowych takich jak choćby Facebook jest skonfigurowanie ustawień prywatności tak, żeby dostęp do informacji na wasz temat miały tylko osoby, które znacie i z którymi chcecie się tymi informacjami dzielić. Warto też pamiętać, że nawet najlepiej zabezpieczone konto nie zwalnia od myślenia o tym, jakie informacje na swój temat zamieszczamy w sieci i czy przypadkiem nie są one zbyt szczegółowe.

A czy wy macie podobne doświadczenia albo słyszeliście takie historie?

*Jak myślicie, jakie są
najważniejsze zasady
bezpieczeństwa związane
z takimi sytuacjami?*

- Skonfiguruj ustawienia prywatności w serwisie społecznościowym tak, żeby do twojego profilu miały dostęp tylko osoby, które znasz i którym ufasz.
- Uważaj, jakie wiadomości na swój temat podajesz w sieci – nie podawaj dokładnego planu dnia ani informacji o wszystkim, co robisz.

Komentarze innych mogą być bardzo nieprzyjemne i obraźliwe. To jedna z form przemocy, ktoś, kto ją stosuje, chowa się za pozorną anonimowością, jaką stwarza internet. Filmy z naszym udziałem lub zdjęcia na których jesteśmy, mogą stać się przedmiotem drwin i wyśmiewania. Nie jesteśmy w stanie kontrolować tego, co myślą lub piszą inni, dlatego zawsze dobrze jest się zastanowić, zanim coś opublikujemy w sieci – komu to udostępniamy i czy jesteśmy gotowi na ewentualne negatywne komentarze. Z drugiej strony, jeżeli to my coś komentujemy pamiętajmy, żeby nie sprawiać innym przykrości, a siebie nie narażać na nieprzyjemności.

***Słyszeliście może o podobnych
historiach związanych z
zamieszczaniem w sieci swojej
twórczości albo z komentarzami?***

***A może sami mieliście takie
doświadczenia?***



Teraz opracujemy zasady, które dotyczą zamieszczania w sieci filmów oraz komentowania. Co to mogą być za reguły?

- Zastanów się dwa razy zanim coś opublikujesz w sieci – zdjęcie lub film z twoim udziałem mogą narazić cię na kpiny albo przykre komentarze ze strony innych internautów.
- Bierz odpowiedzialność za swoje komentarze w sieci – nie pisz o kimś tego, czego nie powiedziałbyś mu w twarz.

Włamanie na konta lub profile, podszywanie się pod kogoś i działanie na jego szkodę to częste sytuacje. Łatwo w ten sposób kogoś skrzywdzić, bo co można zrobić, kiedy wszyscy myślą, że to my piszemy jakieś nieprzyjemne rzeczy, podczas gdy robi to ktoś w naszym imieniu? Takich sytuacji można jednak uniknąć. Jednym ze sposobów jest „mocne” hasło – czyli takie, którego nikt nie zgadnie.

Czy wiecie, że najpopularniejszym hasłem wśród internautów jest ciąg liczb „12345” oraz „123456”?

Wśród popularnych wyrazów i kombinacji, jakimi internauci zabezpieczają dostęp do swoich kont znajdują się również: słowo „hasło”, własne imię, imiona zwierzaków, kombinacje typu „abc123” oraz „QWERTY” (sąsiadujące ze sobą litery na klawiaturze).

Najprostszym sposobem na wymyślenie trudnego hasła jest stworzenie go z pierwszych liter jakiegoś zdania na nasz temat.

Na przykład:

Mam na imię Ojek, mam 15 lat i uwielbiam grać w Counter Strike'a –

MniOm15liugwCS



Przestrzegając zasad bezpieczeństwa online, można uniknąć tego typu sytuacji. Jak myślicie, jakie to są zasady?

- Zabezpieczaj hasłem dostęp do telefonu i wszystkich serwisów internetowych, z których korzystasz. Nikomu nigdy tego hasła nie udostępniaj. Pamiętaj też, żeby hasło było wystarczająco skomplikowane oraz że warto je systematycznie zmieniać.

- Pamiętaj, żeby kończąc pracę na komputerze albo innym urządzeniu z dostępem do internetu, zawsze wylogować się ze swojego konta/profilu.



Co robić w sytuacji zagrożenia, jak się zachować?

- ◉ W sytuacji zagrożenia reaguj jak najszybciej i staraj się zabezpieczyć dowody nieprzyjemnych zdarzeń
- ◉ Zawsze w sytuacji zagrożenia szukaj pomocy u zaufanych osób dorosłych
- ◉ Możesz też skorzystać z pomocy konsultantów Telefonu zaufania dla dzieci i młodzieży 116 111,
www.116111.pl

Dziękuję za uwagę !

Paulina Janowicz

- Źródło: Fundacja Dajemy Dzieciom Siłę