Bezpieczeństwo w sieci zaczyna się od podstaw - czyli od hasła. Hasło to pierwsze, podstawowe zabezpieczenie, które chroni dostępu do Twoich kont. Każda aplikacja to swego rodzaju sejf, który zawiera mnóstwo Twoich danych, o których może nawet nie masz pojęcia. Dlatego, aby nie dostał się do nich nikt niepożądany, pamiętaj o ustawieniu silnego hasła!

1. Zasady zabezpieczeń:

1. Pamiętaj, aby ustawić zabezpieczenia na każdym ze swoich urządzeń! Twój komputer i Twój telefon mogą być ze sobą połączone, więc jeśli odpowiednio nie zabezpieczysz jednego z nich, ktoś może zdobyć dostęp do wszystkich plików z obu urządzeń.

2. Nie powtarzaj haseł, dla każdego konta stosuj inne. Jeśli będziesz stosować wszędzie takie samo hasło, a na jednej z witryn dojdzie do wycieku danych, nieodpowiednie osoby będą mieć dostęp do wszystkich serwisów, na których się logowałeś.
Tak, problemem może się okazać zapamiętanie wszystkich haseł - dlatego warto skorzystać z menadżera haseł, który szyfruje Twoje hasła i udziela dostępu tylko po uwierzytelnieniu, że to właśnie Ty próbujesz się do niego dostać.

3. Nie zapisuj swoich haseł w widocznych miejscach - w zeszytach czy na karteczce przyklejonej do komputera! I oczywiście - nikomu nie podawaj swojego hasła.

4. Stosuj uwierzytelnianie dwuskładnikowe - zależnie od aplikacji, to zabezpieczenie może nazywać się „Uwierzytelnianie dwuskładnikowe”, „Weryfikacja dwuetapowa”, 2FA lub Two-Factor Authentication. Możliwość aktywacji tego zabezpieczenia znajdziesz w ustawieniach aplikacji, strony bądź urządzenia. Stosuj 2FA gdzie tylko się da, dzięki temu, nawet po wpisaniu prawidłowego hasła, będziesz musiał potwierdzić, że próbujesz się zalogować, za pomocą sposobu, do którego masz tylko Ty - np. SMSa, powiadomienia w innej aplikacji, specjalnie wygenerowanego kodu czy odebraniu połączenia.

5. Skorzystaj z zabezpieczeń biometrycznych - większość telefonów, tabletów, a także wiele komputerów pozwala na ustawienie dodatkowych zabezpieczeń biometrycznych. Dzięki nim, łatwo i szybko odblokujesz swoje urządzenie za pomocą odcisku palca czy skanowania twarzy. Biometria jest nie do podrobienia, dlatego warto ustawić ją jako pierwsze zabezpieczenie.

6. Zwracaj uwagę na powiadomienia o logowaniu - wiele serwisów wysyła maile bądź powiadomienia push-up za każdym razem, gdy zalogujesz się do swojego konta na nowym urządzeniu. Dzięki temu, jeśli ktoś zaloguje się na Twoje konto, możesz szybko zareagować i skorzystać z opcji „Wyloguj ze wszystkich urządzeń”. Pamiętaj, aby po takiej sytuacji, natychmiast zmienić hasło!

2. No dobrze, ale jakie w ogóle powinno być to silne hasło?

- **Musi być trudne do odgadnięcia dla innych osób, a także zaawansowanej technologii.**
- **Powinno zawierać minimum 12 znaków (im dłuższe, tym lepsze). Za silne hasła uznaje się takie, które mają co najmniej 16 znaków**
- **Powinno składać się z kombinacji wielkich liter, małych liter, symboli oraz cyfr**
- **Jeśli ustawiasz konkretne słowo - zastąp kilka liter losowymi symbolami bądź celowo zapisz je niepoprawnie, np. zamiast królpopiel, napisz: krulp0p!3L?**
- **Jeśli strona na to pozwala - zastosuj polski znak, zminimalizuje to ryzyko odgadnięcia hasła przez osoby niekorzystające z polskiego alfabetu, np. lub!ępl@ck!16**
- **Unikaj cyfr i liter następujących po sobie, np. qwerty, 987654321**
- **Nigdy nie używaj w haśle swoich danych osobowych, np. imienia, nazwiska, daty urodzenia czy miejscowości, z której pochodzisz, np. macieksosnowiec**
- **Nie używaj także słów, które łatwo skojarzyć osobom z Twojego otoczenia, np. imienia Twojej dziewczyny, chłopaka czy swojej ksywki**

3. Dobre rady:

Jeśli masz problem z zapamiętaniem hasła numerycznego (które zazwyczaj wymagane są przy logowaniu do banków), spróbuj pomyśleć o słowie, które charakterystyczne jest tylko dla Twoich dalekich wspomnień - np. imię Twojego pierwszego kota z dzieciństwa albo ulubionej maskotki, a następnie „napisz je" za pomocą klawiatury numerycznej. Dzięki temu, wystarczy, że zapamiętasz słowo i przed logowaniem napiszesz je ponownie na klawiaturze numerycznej, np. Bonifacy = 26643229.

Ciekawostka: Najczęściej stosowanym hasłem w Polsce jest... 123456! Na 9 miejscu natomiast plasuje się słowo „mateusz". Najczęściej używane hasło na świecie to „password" w różnych wersjach językowych - czyli po prostu „hasło".

4. Co robić, gdy ktoś wykradnie Twoje hasło?

1. Jeśli masz nawet najmniejsze podejrzenie, że ktoś wykradł Twoje hasło, od razu je zmień! Pamiętaj, aby nie było podobne do poprzedniego! Jeśli użyłeś tego hasła również w innym miejscu – koniecznie zmień je na wszystkich profilach!
2. Jeśli posiadasz konto w banku, przede wszystkim sprawdź, czy nie zniknęły z niego żadne pieniądze. Jeśli masz podejrzenie, że ktoś mógł już na nie wejść lub skorzystać z Twojej karty, jak najszybciej skontaktuj się z infolinią swojego banku i podążaj za instrukcjami pracownika.
3. Sprawdź, czy na Twoich profilach nie pojawiły się żadne posty opublikowane przez osobę, która mogła włamać się na Twoje konto i czy nie zostały wysłane żadne wiadomości do Twoich znajomych. Jeśli tak – poinformuj ich o tej sytuacji, aby wiedzieli, że to nie Ty do nich piszesz.
4. Jeśli nie możesz odzyskać dostępu do konta – skontaktuj się z administratorem.

Pytania do młodzieży:

1. **Podaj przykłady 2-3 silnych haseł - oczywiście, nie stosuj ich potem w swoich profilach!**
2. **Spotkałeś się kiedyś z sytuacją, w której nieodpowiednie zabezpieczenia doprowadziły do naruszenia prywatności czyichś danych? Opowiedz.**
3. **Czy wiesz jak ustawić weryfikację dwuskładnikową? Zaprezentuj na przykładzie dowolnej aplikacji lub urządzenia.**
4. **Przetestuj zabezpieczenia biometryczne na swoich koleżankach i kolegach w klasie. Czy możliwe będzie włamać się do Twojego telefonu?**
5. **Jakie masz sposoby na zapamiętywanie skomplikowanych haseł?**