**Jak tworzyć bezpieczne hasła?**

Hasła, które tworzymy do naszych internetowych kont mają za zadanie chronić nasze dane i zapewnić nam bezpieczeństwo w sieci. Jednak według badań 50 proc. Polaków nie zmienia regularnie pin-u i hasła do bankowości internetowej. Tworzymy też hasła bardzo łatwe do złamania przez przestępców internetowych. A jak tworzyć bezpieczne hasła?

**Ustaw silne hasło**

- Silne hasła to takie, które składają się z wielkich i małych liter, cyfr i znaków specjalnych.

- Trudne do wykrycia są hasła nie związane z charakterystycznymi danymi, które można przypisać do danej osoby, np. miejscem urodzenia, imieniem bliskiej osoby itd.

**Jakie hasła nie są bezpieczne?**

- Hasła poniżej 8 znaków

- Hasła będące imieniem lub nickiem

- Zbiór samych cyfr

- Hasło bez znaków specjalnych

- Hasło wykorzystane w wielu serwisach

Kiedy użytkownik proszony jest o wymyślenie hasła zawierającego DUŻĄ literę - w 90% przypadków będzie to pierwsza litera wyrażenia.

Jeśli poproszony jest o zastosowanie w swoim haśle cyfr:

* zazwyczaj użyje dwóch cyfr - pewnie będzie to rok urodzenia,
* kolejnym częstym wyborem jest zastosowanie na końcu wyrazu czterech cyfr – często jest to aktualny rok kalendarzowy,
* popularne zakończenie hasła to jedna cyfra – często 1, a następnie w kolejności są 3 cyfry.

Gdy potrzebujemy użyć znaku specjalnego – to chętnie wybieramy **!**

Takie przyzwyczajenia pozwalają przewidzieć hakerom jakiej struktury hasła używamy.

**Jak stworzyć bezpieczne hasło?**

- Powinno się ono składać z przynajmniej 8 znaków

- Powinno zawierać małe i wielkie litery (Aa, Bb, Cc...), cyfry (1234567890) oraz znaki specjalne (!@#$%^&\*)

Niektóre znaki specjalne i cyfry są podobne do liter i można ten fakt wykorzystać przy tworzeniu silnego hasła, np.:

I = !

a = @

E = 3

S = $

O = 0

Do budowy hasła może posłużyć ulubione zdanie, np.:

ŻYRAFY WCHODZĄ DO SZAFY, PAWIANY WCHODZĄ NA ŚCIANY

Następnym krokiem jest wybranie pierwszych liter do stworzenia hasła:

**Ż**YRAFY **W**CHODZĄ **D**O **S**ZAFY, **P**AWIANY **W**CHODZĄ **N**A **Ś**CIANY

Na koniec zamieniamy litery na znaki specjalne, dodajemy cyfry oraz inne elementy bezpiecznego hasła:

ZWDSPWNS → 29Zwd$Pwn$85

Dodane cyfry są zmodyfikowanym i rozdzielonym rokiem (1985), gdzie cyfra 1 została zastąpiona cyfrą 2.

Alternatywnym rozwiązaniem jest manager haseł, który jest programem komputerowym tworzącym i przechowującym mocne hasła (składające się z przypadkowych znaków).

**Regularnie zmieniaj hasło**

- Zrób z tego nawyk (zmieniaj je np. pierwszego dnia każdego miesiąca razem z opłacaniem rachunków)

- Jeśli masz problemy z zapamiętaniem hasła, nie musisz zmieniać całego hasła - wystarczy, że w jakiś sposób je zmodyfikujesz

**Stosuj różne hasła do różnych serwisów**

- Nie używaj tego samego hasła do wielu serwisów (np. do bankowości internetowej, poczty e-maila czy serwisów społecznościowych). Jeśli któreś z kont zostanie przejęte przez hackera, pozwoli to uchronić twoje pozostałe dane.

- Profiluj trudność hasła do tego, jak ważne dla Ciebie informacje ono chroni.

- Wyłącz automatyczne zapamiętywanie haseł w swojej przeglądarce internetowej.

- Nie zapisuj nigdzie swoich haseł i numerów

pin.

Dbajmy o swoje bezpieczeństwo w sieci!



Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Zapraszamy na stronę www.bde.wib.org.pl