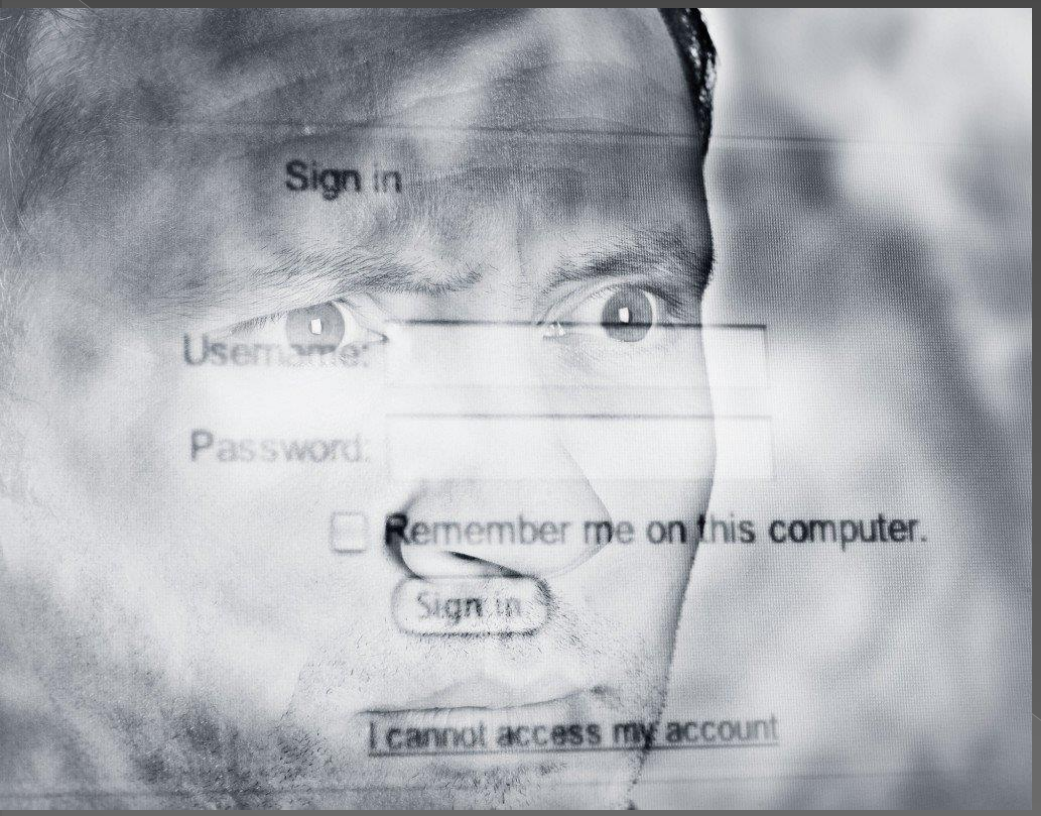
"Поради щодо правильного вибору пароля"

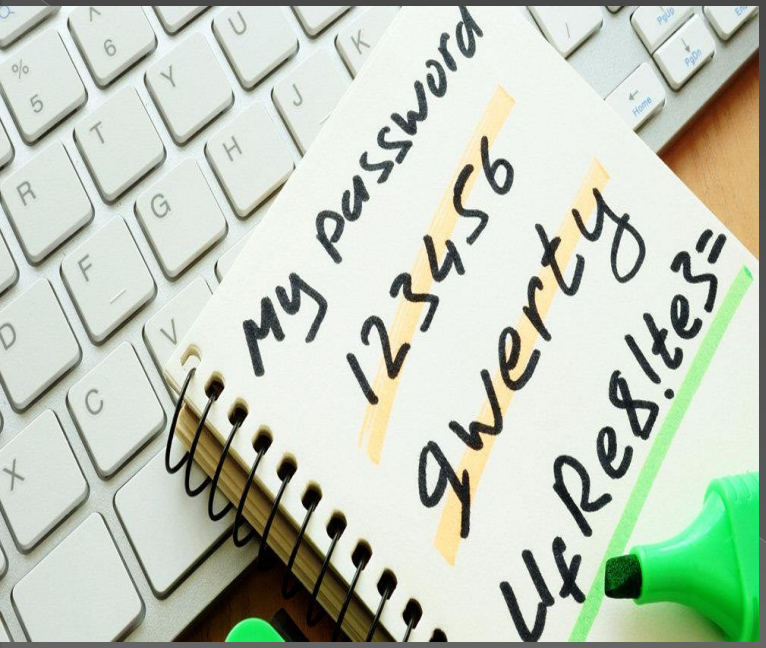
Підготував
учень !0 –А класу
Бондарєв Микита



Придумувати складні паролі

Паролі досить часто критикують, як з точки зору безпеки, так і зручності, що робить їх менш ідеальним методом аутентифікації. Однак саме вони в комбінації з іменами користувачів залишаються найпоширенішою формою аутентифікації на різних сайтах.

Паролі як ключі до онлайн-профілів справедливо вважаються першим і, на жаль, часто єдиним способом захисту, який забезпечує безпеку цифрових даних користувачів. Однак прості та неунікальні дані входу для кожного пристрою та облікового запису не здатні захистити конфіденційну інформацію від зловмисників.



Найгірші паролі 2019 року

Цей список було складено на основі понад 5 мільйонів паролів, які потрапили у вільний доступ.

Перше місце порівняно з минулим роком не змінилося – воно належить паролю "123456".

Друге місце у пароля "123456789". До трійки лідерів також увійшов традиційний пароль "qwerty".

Список 25 найбільш популярних найгірших паролів виглядає так:

1 - 123456
2 - 123456789
3 - qwerty
4 - password
5 - 1234567
6 - 12345678
7 - 12345
8 - iloveyou
9 - 111111
10 - 123123
11 - abc123
12 - qwerty123
13 - 1q2w3e4r
14 - admin
15 - qwertyuiop
16 - 654321
17 - 555555
18 - lovely
19 - 7777777
20 - welcome
21 – 888888
22 - princess
23 - dragon
24 - password1
25 - 123qwe

За оцінками експертів, близько 10% усіх користувачів в світі хоча б раз використовували один із 25 найгірших паролів в цьому році, а близько 3% використовували пароль "123456". Найчастіше гіршими паролями було захищено акаунти північноамериканських і західноєвропейських користувачів.

Правила створення паролів

Довший пароль забезпечує більший рівень безпеки.

Використовуйте **щонайменше вісім символів**. Це можуть бути **комбінації літер, цифр і символів.**

Уникайте простих слів, фраз і шаблонів, які легко вгадати.
Наприклад:
- очевидні слова та фрази, як-от "пароль" або "дозволити_вхід"
- послідовності, як-от "abcd" або "1234"
- шаблони клавіатури, як-от "qwerty" або "qazwsx"
приклади, як-от "sPo0kyH@ll0w3En" або "uP@8cCe!"

Не використовуйте особисту інформацію

Уникайте використання інформації, яку можуть знати й легко вгадати інші.

Наприклад:

назва вулиці

ім’я домашньої тварини

назва вулиці

ваш псевдонім

Поєднуйте різні типи символів

Використовуйте комбінації буквено-цифрових символів і знаків.

Великі літери. Наприклад, A, E, T
Малі літери. Наприклад, a, e, т
Цифри. Наприклад, 2, 6, 7
Спеціальні символи. Наприклад, ! @ & *

Оберіть фразу, яка асоціюється у Вас з даним ресурсом, та трансформуйте її

Попри свою довжину, такі фрази легко запам'ятовуються користувачем. Однак під час їх вибору слід уникати очевидних варіантів, таких як відомі цитати з фільмів або книг. Для підвищення рівня безпеки варто додавати до ключової фрази знаки пунктуації, цифри, верхні або нижні підкреслювання та пробіли.

Замініть літери на цифри та символи.

Виберіть слово або фразу та вставте цифри й символи замість деяких літер. Наприклад:

"Spooky Halloween" можна змінити на "sPo0kyH@ll0w3En"
"Later gator" можна змінити на "L8rg@+0R“

Створіть абревіатуру з речення.

Придумайте довге речення та створіть пароль із перших літер кожного слова. Наприклад:

"Uncle Peter always ate chocolate-covered everything" стане "uP@8cCe!"

Створіть свою власну схему перетворення

Замість пробілів між словами використовуйте дефіси чи нижні підкреслення;
заміняйте останню літеру цифрою, яка відповідає кількості слів у цьому слові;
нехай друга літера кожного слова буде великою;
заміняйте кожну літеру «е» на решітку «#»
… або придумайте будь-який інший, зручний для вас спосіб.

Регулярно змінюйте паролі, особливо у разі потреби в захисті важливих даних. Чим більш важливіша інформація, тим частішими мають бути оновлення даних входу.

Мати один і той самий замок на дверях будинку протягом багатьох років – це все одно, що запрошувати до себе злодія. У якийсь момент замок руйнується; а код піддається.

Використовуйте унікальний пароль для кожного окремого сервісу

Використовувати той самий пароль небезпечно. Якщо хтось дізнається пароль для одного облікового запису, то зможе ввійти в інші й отримати доступ до вашої електронної пошти, адреси та навіть грошей. Необхідно мати різні ключи для різних замків.

Зроби правильний вибір