

**Інструкція:**

**ПРАВИЛА ВИКОРИСТАННЯ ТА ЗМІНИ ПАРОЛІВ**

**Ознаки надійного пароля**:

1. Понад вісім символів.
2. Не містить поширених поєднань літер та слів.
3. Не містить символів, які повторюються або йдуть один за одним (11111, 12345, QQQQ тощо).
4. Не містить вашого імені, прізвища, дати народження та інших персональних даних.
5. Не містить імені, прізвища чи дати народження ваших батьків, дітей, чоловіка, дружини.
6. Такого слова немає в англійській, українській мовах та бажано інших теж.
7. Містить спеціальні символи, цифри, великі та маленькі літери.
8. Створено за допомогою сервісу генерування паролів.
9. Використовуєте його лише на одному сервісі.
10. Ви не зберігаєте пароль у себе на смартфоні або ноутбуці у нотатках.
11. Його немає на сайті [Have I Been Pwned](https://haveibeenpwned.com/).
12. Його немає на наклейці вашого ноутбука, що стоїть посеред офісу.
13. Його не знають ваші рідні, кохані, друзі, колеги та випадкові знайомі.
14. Ваш пароль має суттєво відрізнятись від попереднього, який ви використовували на цьому сервісі.

**Чого не можна робити з паролем**:

Надсилати комусь повідомленням.

1. Дублювати на інших сервісах.
2. Залишати у вільному доступі, наприклад, на папірці в офісі.

**Як легко використовувати складні паролі:**

1. Користуйтеся генератором паролів – щоб не вигадувати їх щоразу.
2. Зберігайте складні комбінації у менеджері паролів.
3. Використовуйте парольні фрази – їх легко запам'ятовувати.
4. Придумайте систему генерування паролів, щоб щоразу не доводилося вигадувати комбінації та дублювати на різних ресурсах.
5. Використовуйте пристрій для безпечної аутентифікації на підтримуючих сервісах (наприклад, для електронних підписів).