ЛАБОРАТОРНА РОБОТА №2. КЕРУВАННЯ ПАРОЛЯМИ.

Мета вивчення: ознайомитися з різними методами та правилами створення надійних паролів. Отримати практичні навички утворення паролів та їх перевірки на стійкість. Налаштувати двохфакторну автентифікацію акаунту в Google.

Обсяг навчального часу: 1 година.

Обладнання: комп'ютер (планшет, смартфон), наявність підключення до мережі Інтернет.

План заняття:

1. Створити паролі різними методами та різної довжини.
2. Перевірити створені паролі на стійкість та в базах, що містять скомпрометовані паролі.
3. З'ясувати, чи впливають довжина й складність паролю на його стійкість.
4. Налаштувати двохфакторну автентифікацію акаунту в Google.

Інформаційні джерела:

генератори паролів:

- https://www.avast.ua/random-password-generator,
- https://1password.com/password-generator/,
- https://axcrypt.net/information/password-generator;

створення карти паролів: https://www.savernova.com/;

перевірка надійності паролів:

- https://exploit.in/passcheck/,
- https://www.security.org/how-secure-is-my-password/,
- https://zillya.ua/check-password;

бази паролів, які були скомпрометовані:

- https://breachalarm.com/?,
- https://pwnedlist.com/query,
- https://haveibeenpwned.com/Passwords;

підтримка Google: https://support.google.com/mail/?hl=uk.

ЗАВДАННЯ:

1. Створити паролі наступними методами: цифровим методом, за допомогою парольної фрази (слова), генератором паролів (використайте не менше двох відповідних онлайн-сервісів), за допомогою карти паролів, надайте приклад майстер-пароля. Занести створені паролі у перший стовпчик вашого звіту.

2. Перевірити створені паролі на стійкість та наявність у базах паролів, що були скомпрометовані. Результати занести у звіт.

3. Додайте до таблиці-звіту принаймні два «легких» пароля, але різної довжини: 8-10 символів та 14-16. виконайте для цих паролів завдання 3. Зробіть висновки.

4. виконайте налаштування двохфакторної автентифікації на прикладі акаунту в Google.

ВИМОГИ ДО ЗВІТУ:

1. Таблиця зі створеними паролями та результати їх перевірки.

2. Висновок, щодо залежності стійкості паролю від його довжини та складності.

ХІД РОБОТИ.

1. Онлайн-генератор паролів AxCrypt завдяки використанню статистичного аналізу фактичного тексту створює надійні паролі, які не є безглуздим набором символів, отже їх легко запам’ятати. Вам буде запропоновано три паролі різного рівня складності.

Скористайтеся генератором паролів від Avast для перевірки залежності стійкості паролю від його довжини та знаків, що використовуються.

Приклад таблиці зі звітом:

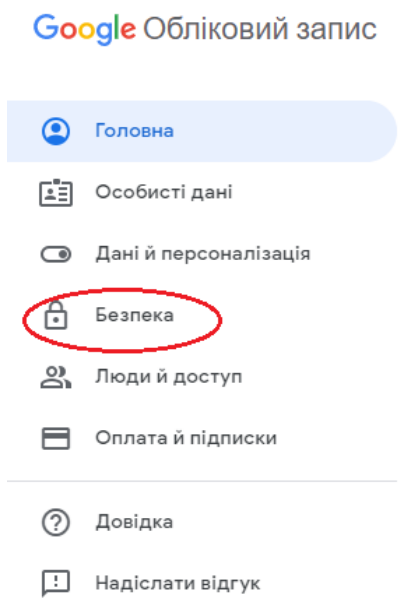
Пароль та метод утворення	Результати перевірки на стійкість		Чи був пароль скомпрометовано
	zillya.ua	**security.org**	**haveibeenpwned.com**
ghjatcjhcmrj-dbrkflfwmrbq метод парольної фрази	Ваш пароль має високий рівень надійності. Зламати такий пароль практично неможливо	16 sextillion years	—
12345678910 елементарний пароль	Якщо Ваш пароль настільки простий, то у вас проблеми! На злам такого паролю хакерам знадобиться зовсім мало часу.	2 seconds	+ This password has beenseen 170 284 times before

2. Двохфакторна автентифікація в Google. Акаунти найпопулярніших сервісів типу Google та Facebook використовуються для авторизації на інших онлайн-ресурсах. Отже, якщо зловмисники отримують доступ до одного акаунту, вони автоматично заволодівають інформацією з багатьох сервісів.

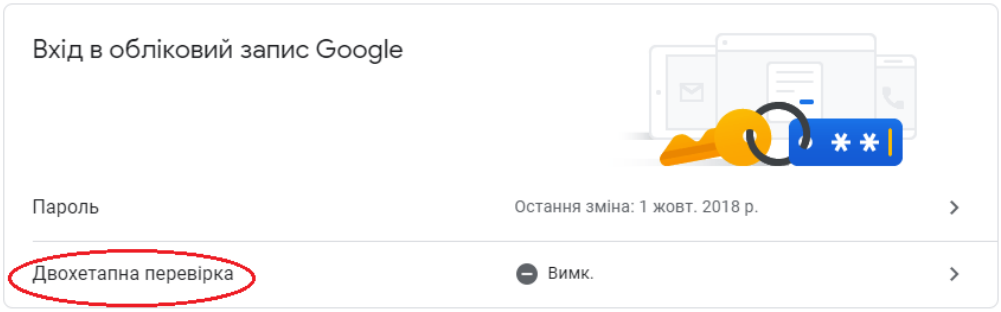
При налаштованій двофакторній авторизації система не надасть доступ до сервісу без додаткової ідентифікації, навіть якщо буде введений правильний пароль. Таким чином, якщо Ваш пароль буде викрадений, і хтось спробує ним скористатися, ви отримаєте про це сповіщення й зможете оперативно зреагувати (змінити пароль).

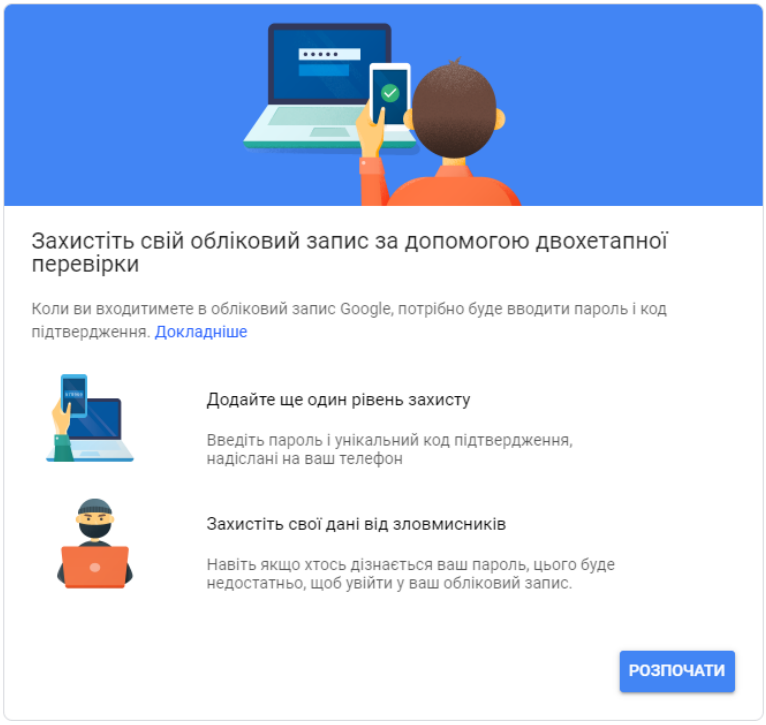
Єдиним мінусом є те, що користувач змушений надавати додаткову персональну інформацію, наприклад, реальний номер свого телефону. Але цей недолік є досить відносним. Створення та підтримка двофакторної авторизації потребує значних фінансових ресурсів, тому запроваджують її лише великі компанії (Google, соціальні мережі, банки, великі торгові платформи тощо), яким користувачі і так надають достатньо приватної інформації, оскільки це передбачено умовами їх використання.

Для налаштування двофакторної авторизації акаунту Google авторизуйтесь та перейдіть на вкладку «Безпека».

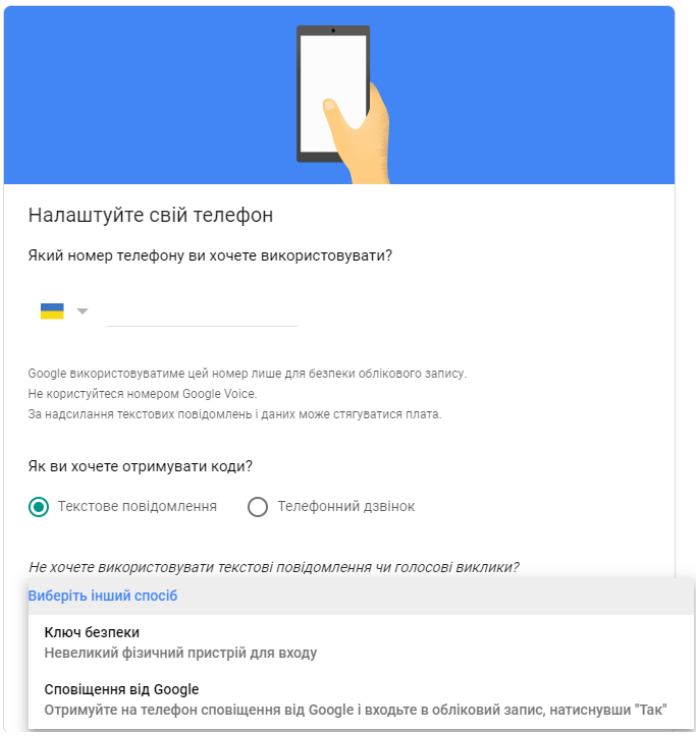


У параметрах входу в обліковий запис оберіть «Двохетапна перевірка», щоб розпочати налаштування.





Додайте номер телефону та оберіть, в який спосіб ви бажаєте отримувати сповіщення.



Для використання варіанту «Сповіщення від Google» Вам буде необхідно додатково увійти в свій акаунт Google зі свого мобільного пристрою. Цей спосіб не вимагає надання номеру мобільного телефону. Його перевага в тому, що якщо сім-картка з якоїсь причини заблокована, доступ до Google-акаунту зберігається й залишається недоступним зловмисникам. Недоліком є те, що для входу в акаунт телефон повинен мати підключення до Інтернету. При виборі опції «Текстове повідомлення» або «Телефонний дзвінок» зверніть увагу, що код країни вказаний в форматі +380, тому номер телефону необхідно вводити в 9-значному форматі (без першого нуля).