**Міністерство освіти та науки України**

**Державний торговельно-економічний університет**

***Кафедра інженерії програмного забезпечення та кібербезпеки***

**ЗВІТ**

***З ЛАБОРАТОРНОЇ РОБОТИ № 9***

*з дисципліни*

**«ОСНОВИ КІБЕРБЕЗПЕКИ»**

**НА ТЕМУ:**

СТВОРЕННЯ ТА ЗБЕРЕЖЕННЯ НАДІЙНИХ ПАРОЛЕЙ

(назва теми)

**Виконала:** студентка факультету інформаційних технологій

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Ковальова Людмила Ігорівна

Київ 2024

**Лабораторна робота №9**

**Тема:** Створення та збереження надійних паролей

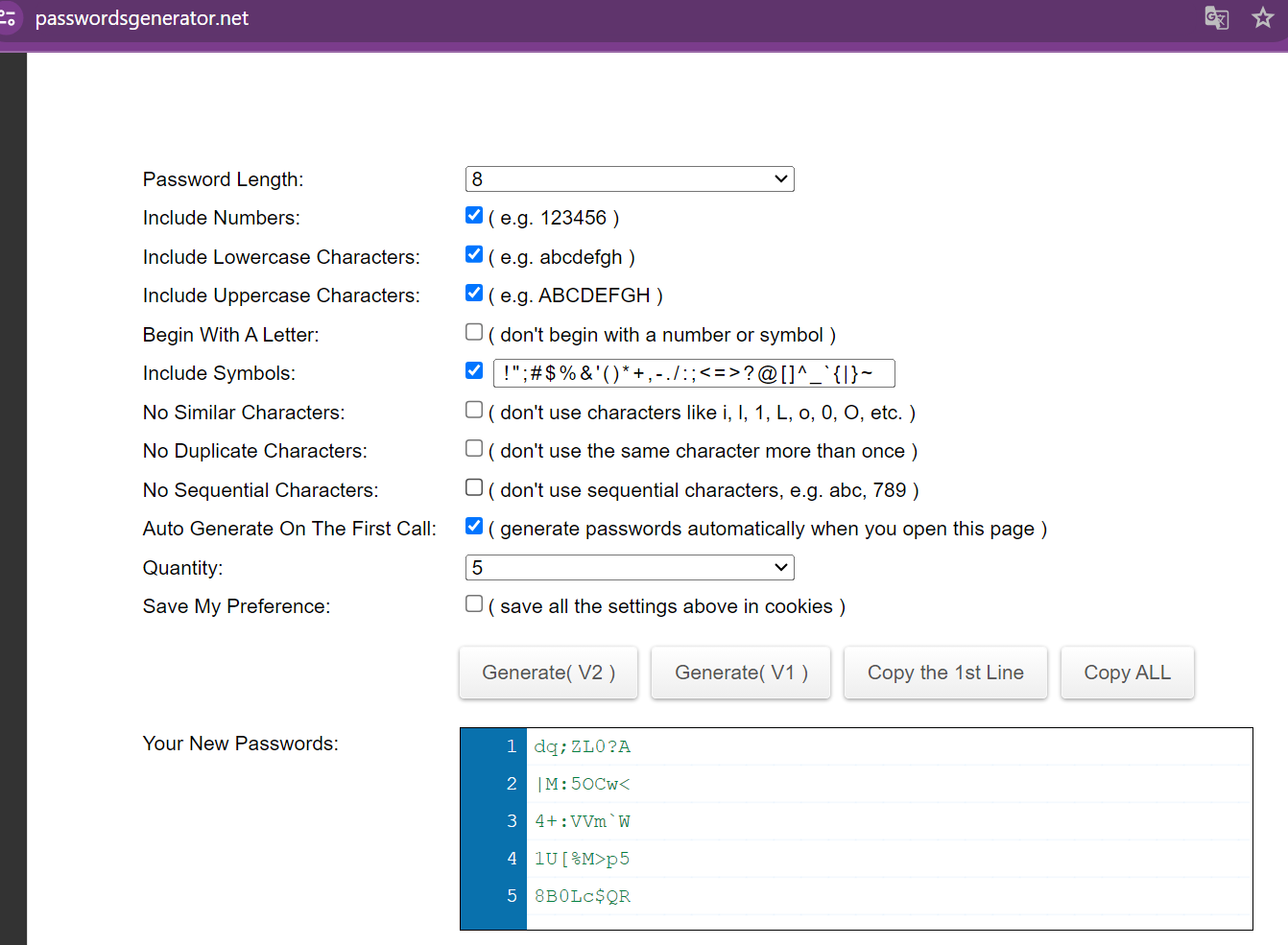
**Цілі та задачі:** Зрозуміти концепцію надійного пароля.

**Хід роботи:**

1. Створення надійного пароля
   1. Проаналізуйте характеристики надійного пароля та загальну політику вибору паролів, наведену вище. Чому в політиці не враховуються перші два пункти? Поясніть.

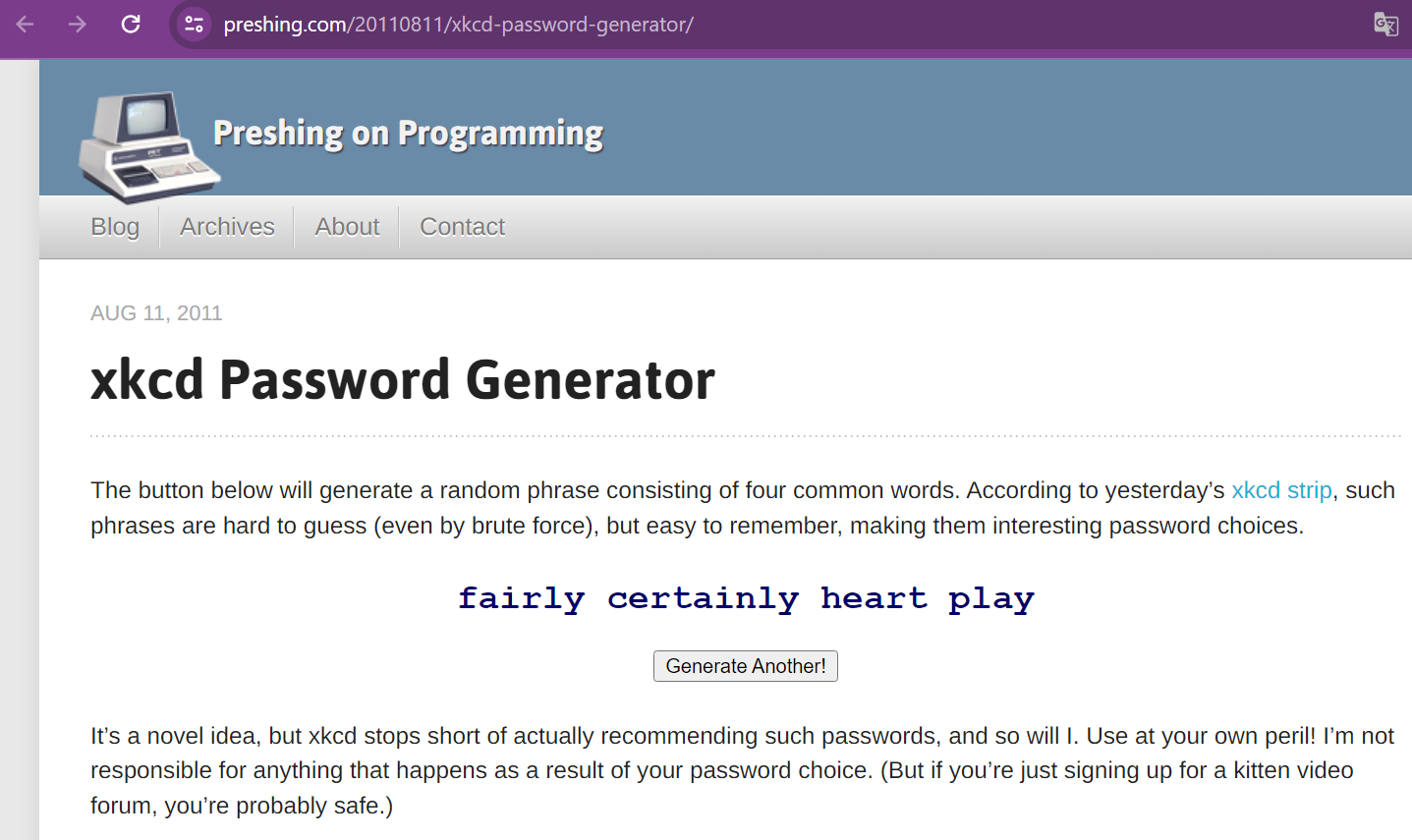
Легка запам'ятовуваність та важкість вгадування для інших осіб дійсно є ключовими характеристиками для створення ефективного пароля. Однак, загальна політика вибору паролів фокусується переважно на технічних аспектах безпеки, таких як складність та унікальність пароля, з метою запобігання злому паролів за допомогою програм або методів "брутфорсу". Політика вибору паролів часто встановлюється з метою забезпечення високого рівня безпеки, а не для зручності користувача.

* 1. Відкриваємо веб-браузер і переходимо на <http://passwordsgenerator.net>. Вибираємо параметри, які відповідають політиці вибору пароля. Генеруємо пароль.

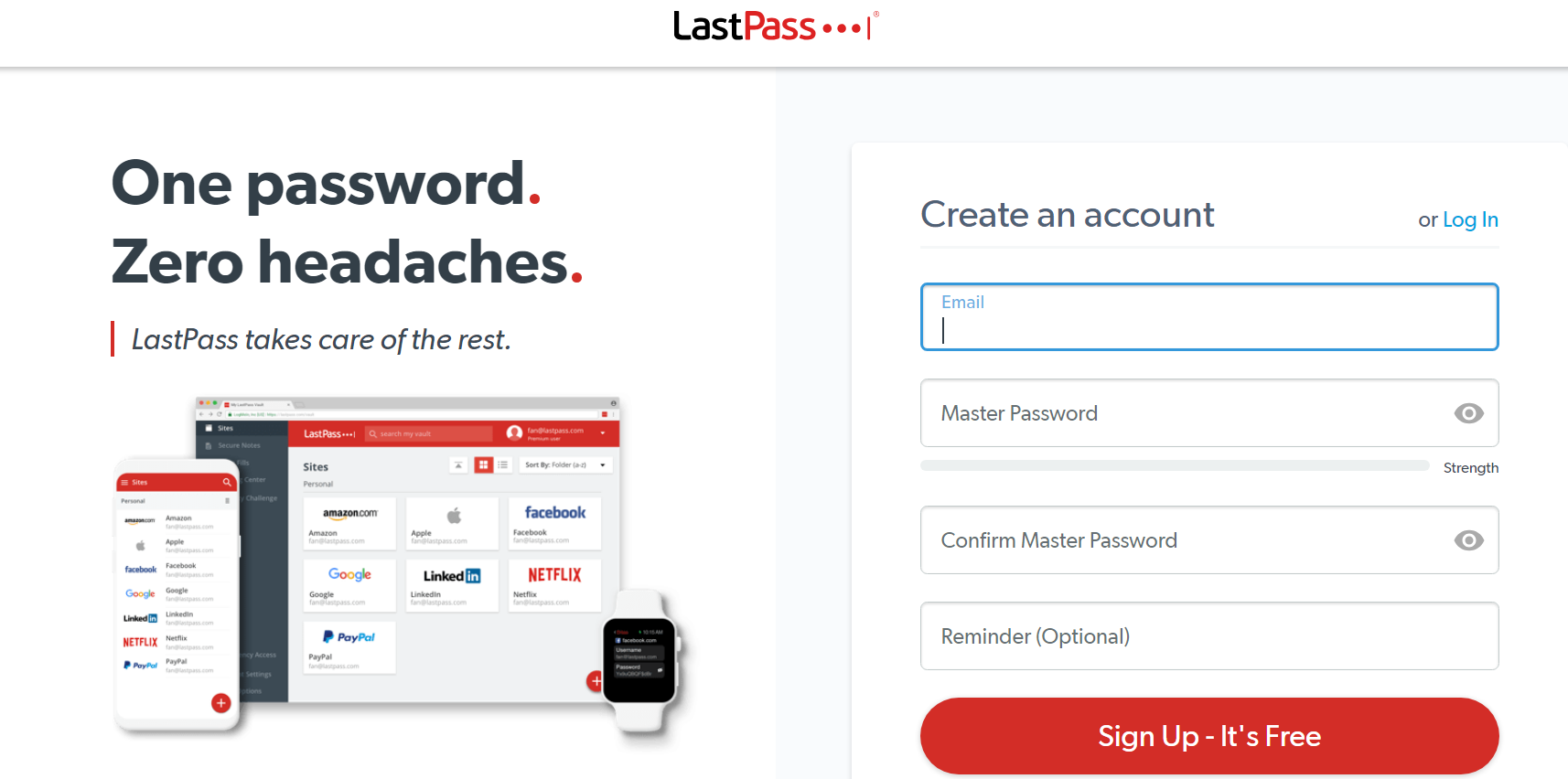


Дійсно, згенерований пароль дуже складний для запам'ятовування.

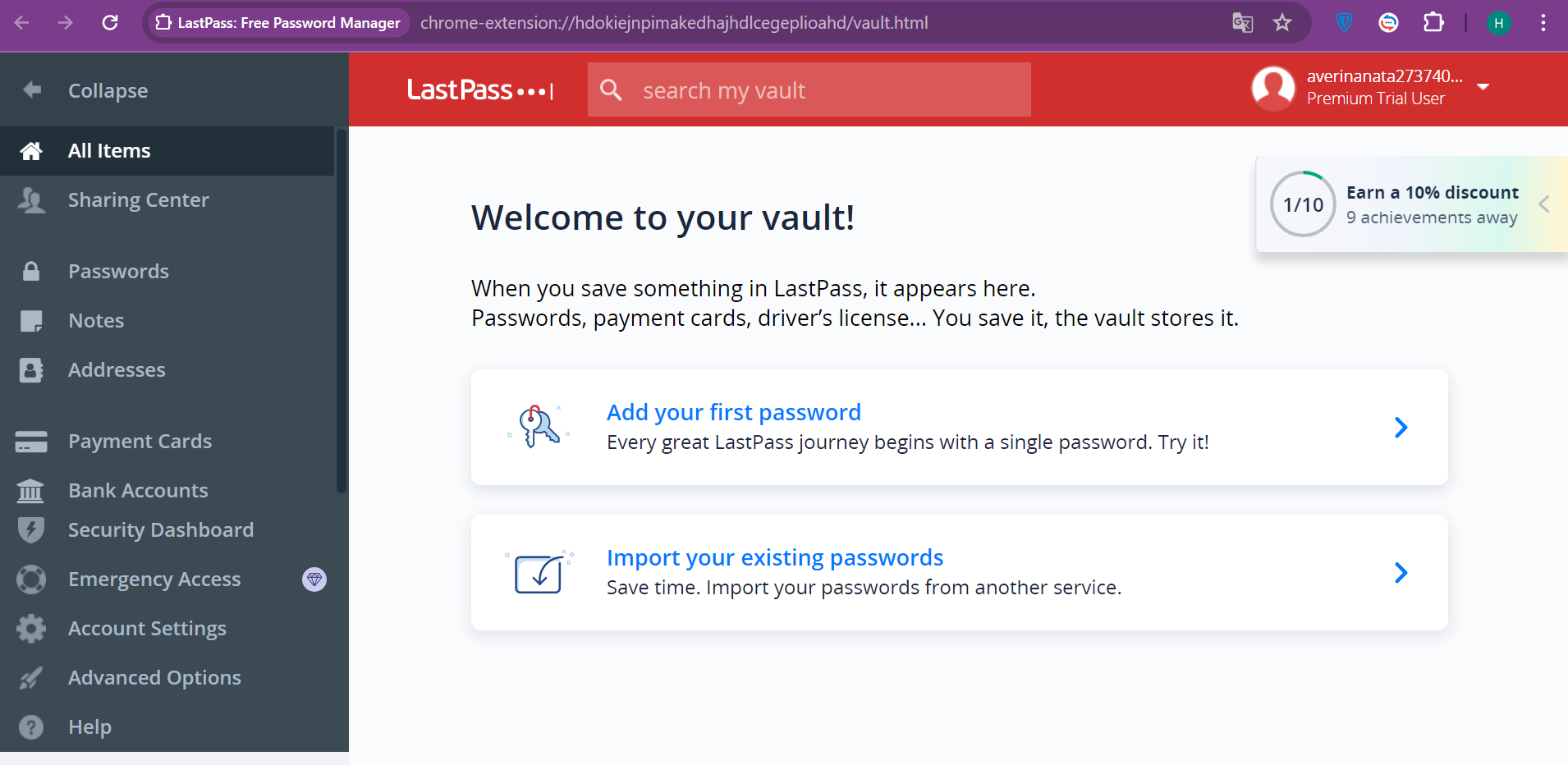
* 1. Відкриваємо веб-браузер і переходимо на <http://preshing.com/20110811/xkcd-password-generator/e>. Генеруємо новий пароль з випадкових слів, натиснувши Generate Another! у верхній частині веб-сторінки. Такий пароль набагато легше запам’ятати.

****

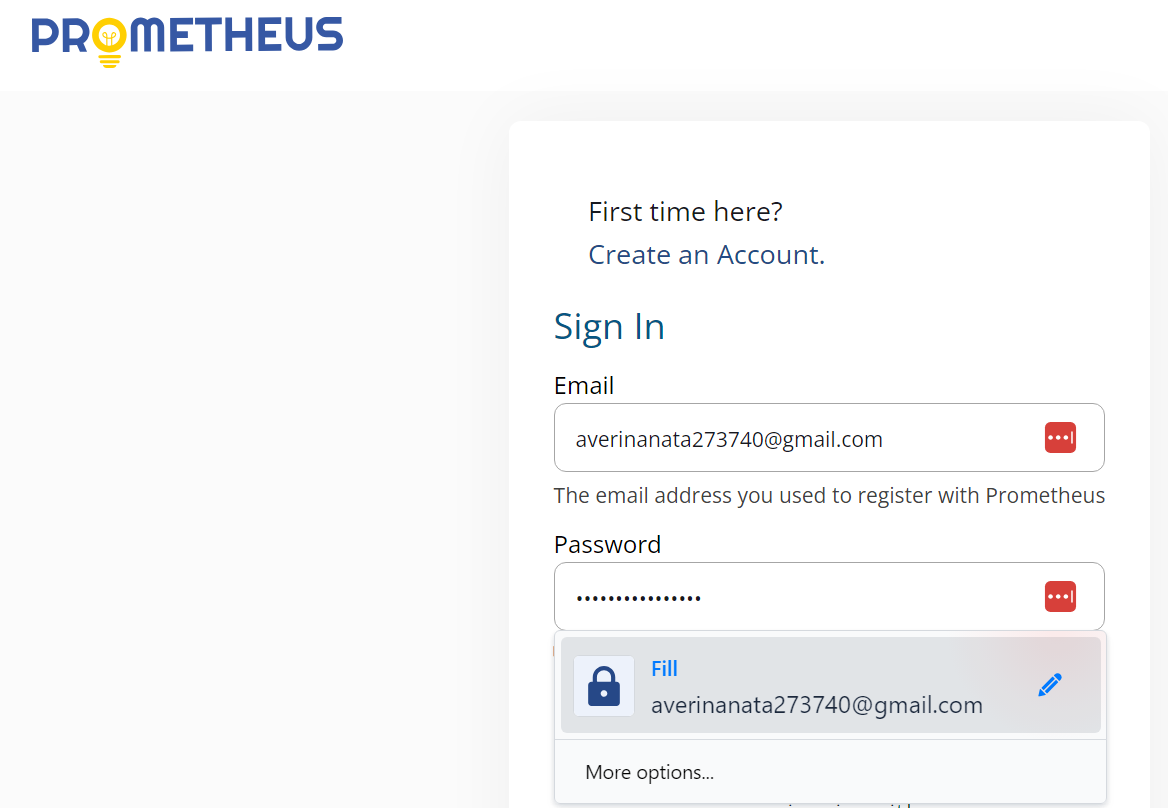
1. Безпечне зберігання паролів
   1. Відкриваємо веб-браузер і переходимо на <https://lastpass.com/b>. Натискаємо Get LastPass Free для створення пробного облікового запису.
   2. Заповнюємо поля, як зазначено в інструкції. Встановлюємо майстер-пароль. Цей пароль дає нам доступ до вашого облікового запису LastPass.



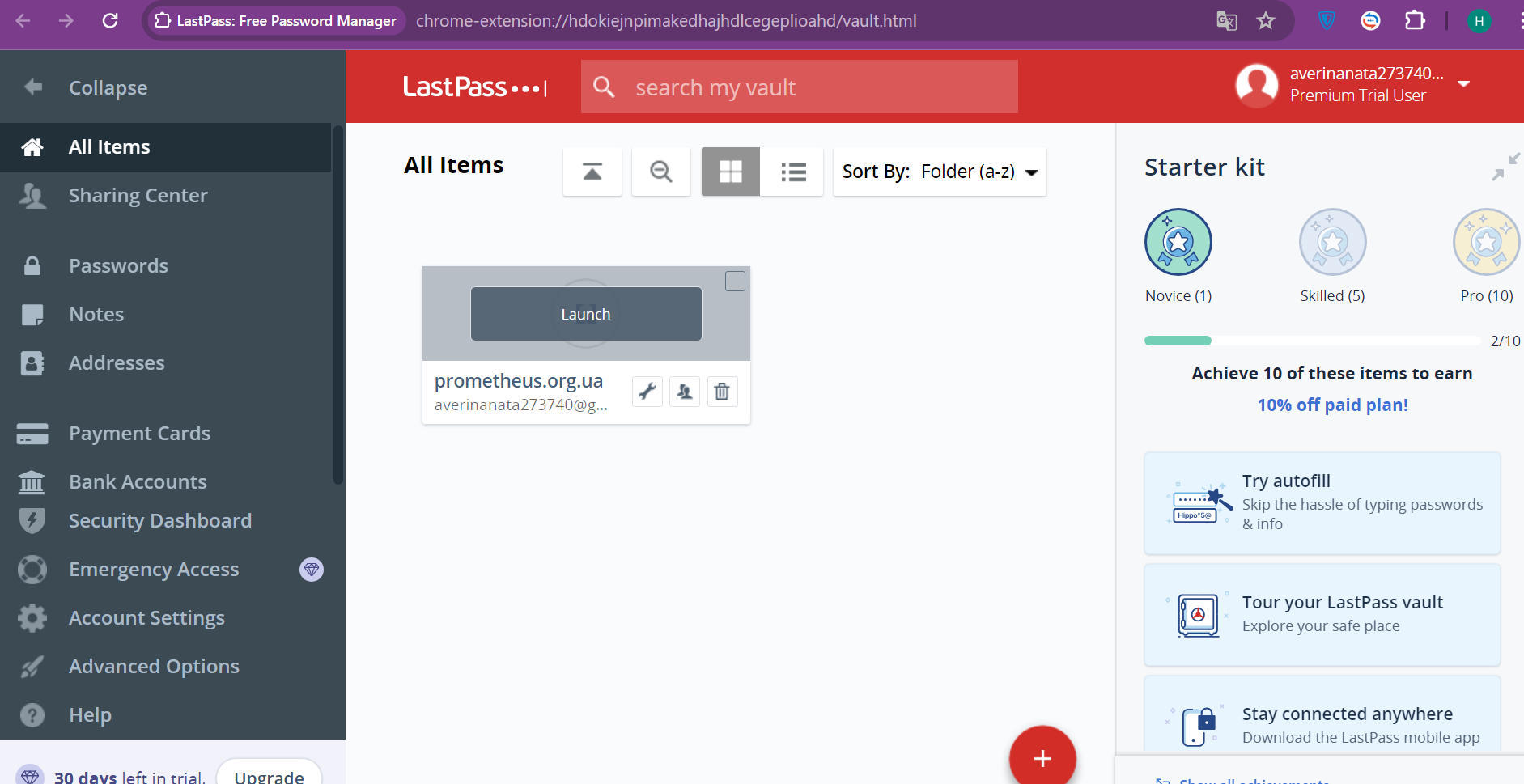
* 1. Завантажуємо та встановлюємо клієнта LastPass.
  2. Відкрийте клієнт і увійдіть до системи за допомогою майстер-пароля LastPass.



* 1. Заходжу в акаунт Prometheus. LastPass автоматично розпізнає пароль та пропонує зберегти його.



* 1. В менеджері пароль зберігається на сторінці «All items» або «Passwords»



* 1. Окрім мене, ще одним суб'єктом, який має доступ до моїх паролів, є розробник менеджера паролів. Це технологічна компанія або постачальник програмного забезпечення, яка створила і підтримує цей сервіс.
  2. Недоліками використання менеджерів паролів:
     1. Хоча більшість менеджерів паролів забезпечують високий рівень шифрування, важливо пам'ятати, що ваши дані зберігаються на серверах компаній. Це означає, що ваші паролі можуть бути компрометовані в разі витоку даних або злому серверів.
     2. Якщо ви забудете майстер-пароль до свого менеджера паролів або втратите доступ до облікового запису, де вони зберігаються, це може призвести до втрати доступу до всіх ваших інших облікових записів.
     3. Як і будь-яке онлайн-програмне забезпечення, менеджери паролів можуть час від часу виявляти проблеми з доступністю або працездатністю, що може перешкоджати вам отримувати доступ до ваших паролів у потрібний момент.

**Висновок**: в ході виконання лабораторної роботи було вивчено політику надійного паролю для типової організації, створено за цією політикою набір паролів за допомогою онлайн інструментів. Виявлено, що надійний пароль не завжди може бути зручним для запам’ятовування. Також було проаналізовано менеджер для зберігання паролів LastPass, який доволі зручно відображає всі збережені акаунти на своїй головній сторінці. Для мене настільки ж зручним є менеджер паролів в браузері Chrome.