Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Козодой Андрія Владиславовича

на здобуття ступеня вищої освіти Бакалавра

Система захисту облікових записів від фішингу на основі менеджеру паролів

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

Шифр КРБКБ.200109.20.01.10 ПЗ

Виконав студент 4 курсу група КБ-20-1 _____ Андрій КОЗОДОЙ

Керівник канд. техн. наук, доцент _____ Віра ТІТОВА

Нормоконтролер старший викладач _____ Сергій МОСТОВИЙ

До захисту допускаю:

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

19 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій
Кафедра Кібербезпеки
Рівень вищої освіти Бакалавр
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
15 лютого 2024 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Козодою Андрію Владиславовичу

1 Тема роботи Система захисту облікових записів від фішингу на основі менеджеру паролів

Керівник роботи Тітова Віра Юріївна
Затверджено наказом ректора університету від 15 лютого 2024 № 8
2 Строк подання студентом кваліфікаційної роботи на кафедру 25.05 2024р
3 Вихідні дані до роботи Створити систему захисту облікових записів від фішингу на основі менеджера паролів

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Дослідження Фішингу. Облікові записи та методи їх захисту. Реалізаія програмного забезпечення. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Схема фішингу. Огляд програм для боротьби з фішингом. Огляд менеджерів паролів. Графічні елементи програми розробленої для дипломного проекту.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент _____ Андрій КОЗОДОЙ

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система захисту облікових записів від фішингу на основі менеджеру паролів».

Автор роботи: Козодой А.В.

Керівник роботи: Тітова В.Ю

Пояснювальна записка: 72с., 32 рис., 1 табл., 40 джерел.

Графічна частина: 3 плакати, 9 презентаційних слайдів.

ЗАХИСТ ВІД ФІШИНГУ, СИСТЕМА ЗАХИСТУ ВІД ФІШИНГУ, МЕНЕДЖЕРИ ПАРОЛІВ, РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Мета дипломної роботи: Метою дипломної роботи є створення системи захисту облікових записів від фішингу на основі менеджеру паролів.

Об'єктом дослідження є менеджери паролів.

Предметом дослідження є оцінка ефективності роботи менеджерів паролів проти різник типів атак в основному фішингових які використовують кіберзлочинці.

Під час написання дипломної робото було проведено дослідження різних менеджерів паролів визначено їхній принцип роботи, виявлено переваги та недоліки і на базі цього дослідження було створено свій менеджер паролів.

20.06.24р

ABSTRACT

The topic of the qualification work: "A system for protecting accounts from phishing based on a password manager."

Author of the work: Kozodoy A.V.

Head of work: Titova V.Yu

Explanatory note: 72 pages, 32 figures, 1 table, 40 sources.

Graphic part: 3 posters, 9 presentation slides.

PROTECTION AGAINST PHISHING, ANTI-PHISHING SYSTEM, PASSWORD MANAGERS, SOFTWARE DEVELOPMENT

The purpose of the thesis: The purpose of the thesis is to create a system for protecting accounts from phishing based on a password manager.

The object of research is password managers.

The subject of the study is the assessment of the effectiveness of password managers against different types of attacks, mainly phishing attacks used by cybercriminals.

During the writing of the thesis, research was conducted on various password managers, their principle of operation was determined, advantages and disadvantages were identified, and a password manager was created on the basis of this research.

20.06.24 р

ЗМІСТ

ВСТУП

Сучасні цифрові технології відкривають широкі можливості для взаємодії та обміну інформацією, однак разом із тим вони несуть і нові загрози для користувачів, серед яких особливе місце посідає фішинг.

Фішинг – це різновид шахрайства, спрямований на крадіжку особистих даних, зокрема облікових записів та паролів користувачів, з подальшим їх протиправним використанням. Ця проблема є надзвичайно актуальною, адже зростаюча кількість користувачів та обсяги інформації, що передається через мережу Інтернет, роблять їх привабливою ціллю для кіберзлочинців.

Захист облікових записів і паролів користувачів є критично важливим не лише для самих користувачів, а й для організацій, установ та підприємств, діяльність яких тісно пов'язана з цифровими технологіями. Недбале ставлення до безпеки облікових даних може призвести до серйозних фінансових та репутаційних втрат, тому необхідно вживати ефективних заходів для протидії фішингу.

1 ДОСЛІДЖЕННЯ ФІШИНГУ

1.1 Фішинг та його різновиди

Погляд в історію фішингових атак показує, що перший фішинговий електронний лист, ймовірно, надійшов приблизно в 1995 році. Багато людей вперше дізналися про фішинг п'ять років потому, коли стався Love Bug. Майже через два десятиліття фішинг залишається основним вектором атак для зламу корпоративних даних і викрадення даних. Можливо, в історії фішингу є якісь зачіпки, історія фішингу почалася в 1990-х роках. На початку та в середині 1990-х єдиним доступом до інтернету був комутований доступ. Для тих, хто не хотів платити за доступ до інтернету, як альтернатива була доступна 30-денна безкоштовна пробна версія доступу до Інтернету через AOL Disk. Замість того, щоб жити без інтернету після закінчення пробного періоду, деякі люди знайшли спосіб змінити своє ім'я користувача, щоб відображатися як адміністратор AOL. Ці псевдоніми використовувалися для «підробки» облікових даних для входу та подальшого отримання безкоштовного доступу до інтернету. З розвитком інтернету шахраї застосували цю тактику, видаючи себе за адміністраторів інтернет-провайдера, надсилаючи електронні листи на облікові записи клієнтів інтернет-провайдера, щоб отримати облікові дані користувача. Спуфінг дозволяв хакеру отримати доступ до інтернету через ваш обліковий запис або розсилати спам через вашу електронну адресу. Love Bug 2000 року через зміну стратегії світ став жертвою любовної помилки 4 травня 2000 року. Починаючи з Філіппін, поштові скриньки по всьому світу були заповнені повідомленнями «Я ТЕБЕ ЛЮБЛЮ». У тексті повідомлення просто говорилося: «Будь ласка, перевірте вкладений любовний лист від мене». Людина, яка не хоче розкривати свою таємницю любовного життя, відкриває файл .txt, який, на її думку, був нешкідливим, лише щоб випустити хробака, який сіяв хаос на його комп'ютері. Хробак перезаписував файли зображень і надсилав свою копію всім контактам користувача в адресній книзі Outlook. «LoveBug» показав, як змусити спам

розсилати себе, і що за допомогою вміло розробленого вірусу, який полює на людську психологію та технічні недоліки, зловмисне програмне забезпечення може отримати величезну кількість жертв. Вважалося, що загалом уражено близько 45 мільйонів ПК з Windows. Історія фішингу показує, що, хоча методи доставки еволюціонували протягом двох десятиліть, щоб уникнути виявлення спам-фільтрами та іншими технологіями, тактика, яку використовують злочинці, залишається досить послідовною. Здавалося б логічним, що люди повинні були навчитися уникати можливості взламати облікові дані для входу, натискання посилань або навіть відкриття вкладень. Проте це все ще ефективна тактика для хакерів. Хоча тактика фішингу, можливо не змінилася, ставки змінилися. Тепер замість того, щоб отримати безкоштовний доступ до Інтернету, фішингові афери можуть завдати шкоди світовій економіці. Навіщо докладати зусиль, щоб зламати брандмауер, коли добре створений фішинговий електронний лист може бути настільки ж ефективним у наданні хакеру доступу до конфіденційної інформації.

Однією з ключових подій став розвиток соціальних мереж. Як згадувалося раніше, лише 10 років тому в Інтернеті було мало інформації про організації та людей, які в них працювали. Сьогодні майже всі в кожній організації мають облікові записи LinkedIn, Facebook або Twitter, деякі мають усі три. Будучи ключовим бізнес-інструментом, ці сайти соціальних мереж пропонують справжню золоту жилу особистої інформації, яку злочинці можуть і використовують для персоналізації електронних листів для певних одержувачів відомими як фішинг. Тільки подумати про кількість інформації, яку злочинець може знайти про компанію лише через LinkedIn. Використовуючи це як відправну точку, хакер може потім глибше пробратися в особисте життя цілей через Facebook і Twitter. Електронний лист, що надходить із (здавалося б) знайомого чи джерела, стосується відповідної теми, заспокоює одержувача. Персоналізовані деталі лише додають автентичності та спокою одержувача, роблячи ймовірність взаємодії з посиланнями чи вкладеннями досить високою. Ці ставки в поєднанні з мінімальними ресурсами, необхідними для здійснення атаки, зробили фішинг

вибором для злочинців, які прагнуть отримати доступ до конфіденційних даних, що зберігаються в мережах великих організацій і корпорацій. Target, Home Depot і Anthem – це лише три останні резонансні зломи, які, як вважають, почалися з того, що співробітник став жертвою фішингу. Хоча здавалося б логічним, що технологічний захист покращиться, нещодавня історія фішингу свідчить про те, що навряд чи технології зможуть повністю запобігти потраплянню фішингових електронних листів до папки «Вхідні» співробітника. Тому цілком зрозуміло, що краудсорсингове виявлення фішингу дозволяє першій лінії захисту повідомляти про атаки, щойно вони потрапляють у мережу. Хорошою аналогією є торговець фруктами, який допоміг запобігти терористичній атаці на Таймс-сквер у 2010 році. Продавець повідомив поліції після того, як помітив, що на вулиці на Таймс-сквер кілька годин стояла машина незвично довго у такому жвавому районі. Автомобіль виявився начиненим вибухівкою. Незважаючи на те, що такі багатолюдні райони, як Таймс-сквер, були оснащені дорогим обладнанням для спостереження та мали значну присутність поліції, знання продавця про вулиці зробили його людиною для виявлення підозрілої діяльності. У мережі користувачі часто є тими першими, хто отримує атаки, тому звіти про підозрілі електронні листи мають важливе значення для запобігання витоку даних.

Фішинг - це коли зловмисники надсилають електронні листи чи інші онлайн-повідомлення, щоб обманом змусити невинних користувачів інтернету віддати гроші чи особисту інформацію.

Окрім фішингу існує багато інших методів, які зазвичай використовують кіберзлочинці, прикладами можуть бути розповсюдження вірусів, шахрайство з інфомацією та взлам комп'ютерів для здійснення DDoS-атак. Популярність Інтернету зростає, і можливості безмежні.

У міру того, як користувачів все більше стає в інтернеті, злочинців також стає все більше, та більше і наміри їхні стають ще жахливішими чим були колись.

Адже злочинці діють скрізь, де є гроші та інформація, інтернет не є виключенням, тому важливо захищати свою особисту інформацію в інтернеті.

Кіберзлочинність є величезною проблемою, тому важливо бути обережним із особистою інформацією під час користування інтернетом.

Так звані темні хакери стають розумнішими з кожним днем і постійно винаходять нові способи викрадення інформації та грошей в інтернеті.

Існують різні методи фішингу, які використовують шахраї, і цей список постійно поповнюється, оскільки кіберзлочинці винаходять нові способи отримати доступ до потрібної їм інформації. З розвитком технологій та інтернет-сервісів хакери шукають нові можливості для використання слабких місць у системах безпеки та отримання доступу до конфіденційної інформації, що може призвести до того, що користувачі потраплять у нові, менш відомі типи фішингових атак.

Нижче наведено деякі з різних типів фішингу:

- оманливий фішинг;
- простий фішинг;
- китобійний фішинг;
- фармінг;
- смс-фішинг;
- програми гугл;
- інвойс.

Оманливий фішинг або фішинг електронною поштою є найпоширенішим видом фішингової атаки, який використовується десятиліттями. Шахрайське, добре розроблене та маніпулятивне повідомлення надсилається особам, які представляють собою якісь організації. Зазвичай адреса електронної пошти з незначною різницею може залишатися непоміченою звичайними користувачами інтернету. Електронний лист містить посилання, яке веде на підроблену веб-сторінку або встановлює шкідливе програмне забезпечення на вашому пристрої. Такі повідомлення не персоналізовані та не націлені на конкретну особу, а також відомі як «масовий» фішинг. Намір полягає в тому, щоб зламати ваші дані та отримати доступ до вашої конфіденційної або таємної особистої інформації.

Простий фішинг – це стратегія, спрямована на людей, які працюють у певному бізнесі чи галузі, у спробі отримати доступ до інформації самого бізнесу. Електронні листи завжди персоналізовані та зазвичай використовують логотипи та підписи електронної пошти, листи зазвичай представлені як якась корпоративна маркетингова кампанія та дають одержувачу дуже мало сумнівів у їх шкідливості.

Китобійний фішинг – це цілеспрямована фішингова атака, спрямована на «крупних риб» в організації: керівників вищої ланки, таких як керівники, директори та ключовий персонал. Злочинці попередньо проводять ретельне дослідження, а щоб уникнути підозри електронні листи являють собою повідомлення, у яких згадуються важливі відомості про організацію.

Кіберзлочинці часто використовують адреси електронної пошти, схожі на адреси податкових інспекцій чи інших державних установ, і запитують конфіденційну інформацію або вміст, який пов’язаний із грошовим переказом.

Незважаючи на те, що загальне враження від електронного листа дуже професійне, показник успіху досить низький, оскільки він націлений на розумних власників бізнесу.

Фармінг – ще одна стратегія фішингу, це коли шахрайські електронні листи надсилаються зі справжніх джерел, таких як банки чи соціальні мережі.

У цих електронних листах можуть просити вжити термінових заходів щодо облікового запису користувача, це включає такі дії, починаючи від зміни паролів до вжиття певних заходів безпеки та маніпулятивних перенаправлень на підроблені веб-сайти.

Фармінг передбачає не лише надсилання шахрайських електронних листів, але й маніпулює кешем DNS, він використовує ту саму веб-адресу, що й джерело, і виглядає так само, як оригінальна сторінка, та запитує інформацію для входу і зламує обліковий запис. Такий спосіб фішингу дуже важко розпізнати простому користувачу інтернету адже все підроблено дуже витончено і схоже до оригіналу.

Смс-фішинг – це різновид фішингової атаки, яка передбачає використання SMS. Отримуються помилкові текстові повідомлення, які маючи певний зміст

запитують у користувача пряму відповідь на питання, або містять посилання на фішинговий веб-сайт, який часто схожий на сайт який виглядає більш знайомим. Користувача можуть зламати через програми Google, багато людей користуються програмами Google, починаючи від Play Store до Gmail.

Більшість із них використовують Google Документи, Таблиці, Диск та інші програми Google для зберігання своїх документів і фотографій, оскільки вони дуже зручні та безпечні, тому злам паролів Google є однією з головних цілей шахраїв, вони створюють електронні листи та надсилають їх користувачам Gmail, які спрямовують їх на сторінку входу в Google. Після введення пароля обліковий запис і всі збережені в ньому файли стають доступними для кіберзлочинця.

Крім того, на початку 2022 року повідомлялося, що функція коментування Google Docs використовувалася для надсилання, простих електронних листів, щоб обманом змусити певних користувачів натискати на шкідливі посилання.

Зловмисник створював документ Google Docs і додавав коментар зі шкідливим посиланням, список жертв комбінувався за допомогою функції «@» і надсилався електронний лист із посиланням на файл Google Docs, в електронному листі відображався повний коментар, включаючи будь-які шкідливі посилання чи інший текст, доданий зловмисником.

Інвойс - це різновид фішингового шахрайства, за якого лист надсилається компанії чи фізичній особі з вимогою оплати товарів чи послуг. Він включав в себе запит на кошти, дату платежу, що минув, або сповіщення про зміну платіжних реквізитів.

Фішинг з деактивацією облікового запису - скориставшись довірою жертви, яка думає, що важливий для неї обліковий запис буде деактивовано, зловмисники можуть обманом змусити деяких людей передавати важливу інформацію, наприклад облікові дані для входу. Тут більшу роль грає психологія та паніка в яку впадає користувач на якого було застосовано такий вид фішингової атаки.

Ось приклад: зловмисник надсилає електронний лист, який, здається, надійшов від важливої установи, як-от банк, і стверджує, що банківський рахунок

жертви буде деактивовано, якщо він не запровадить швидких заходів. Потім зловмисник запитує логін і пароль до банківського рахунку жертви, щоб запобігти деактивації. У хитромудрому варіанті атаки після введення інформації жертва буде спрямована на справжній веб-сайт банку, щоб нічого не виглядало дивним.

Цьому типу атаки можна протистояти, перейшовши безпосередньо на веб-сайт відповідної служби та подивившись, чи законний представник повідомляє користувача про такий терміновий статус облікового запису. Також корисно перевірити рядок URL-адреси та переконатися, що веб-сайт безпечний. Будь-який незахищений веб-сайт, який запитує логін і пароль, слід серйозно перевіряти та майже без винятку не використовувати.

Фішинг з підробкою веб-сайту - цей тип фішингу зазвичай поєднується з іншими кібер-злочинами, такими як фішинг з деактивацією облікового запису. Під час цієї атаки зловмисник створює веб-сайт, який практично ідентичний справжньому веб-сайту компанії, який використовує жертва, наприклад, банку. Коли людина відвідує сторінку будь-яким способом, будь то спроба фішингу електронною поштою, гіперпосилання на форумі чи через пошукову систему, жертва потрапляє на веб-сайт, який, на її думку, є справжнім сайтом, а не копією.

Уся інформація, введена жертвою, збирається для продажу чи іншого зловмисного використання.

На початку розвитку інтернету такий дублікат сайту було досить легко помітити через їх неякісне виконання. Сьогодні такі сайти можуть виглядати як ідеальна копія оригіналу. Перевіривши URL-адресу у веб-переглядачі, зазвичай досить легко виявити щось підозріле. Якщо URL-адреса виглядає інакше, ніж типова, це слід вважати дуже підозрілим. Якщо сторінки, указані як незахищені, і HTTPS не ввімкнено, це тривожний сигнал і фактично гарантує, що сайт або зламано, або піддано фішинговій атаці. Зазвичай такі сайти потрібно обходити стороною, адже це явний факт підробки, але іноді це притаманно і простим веб-сайтам.

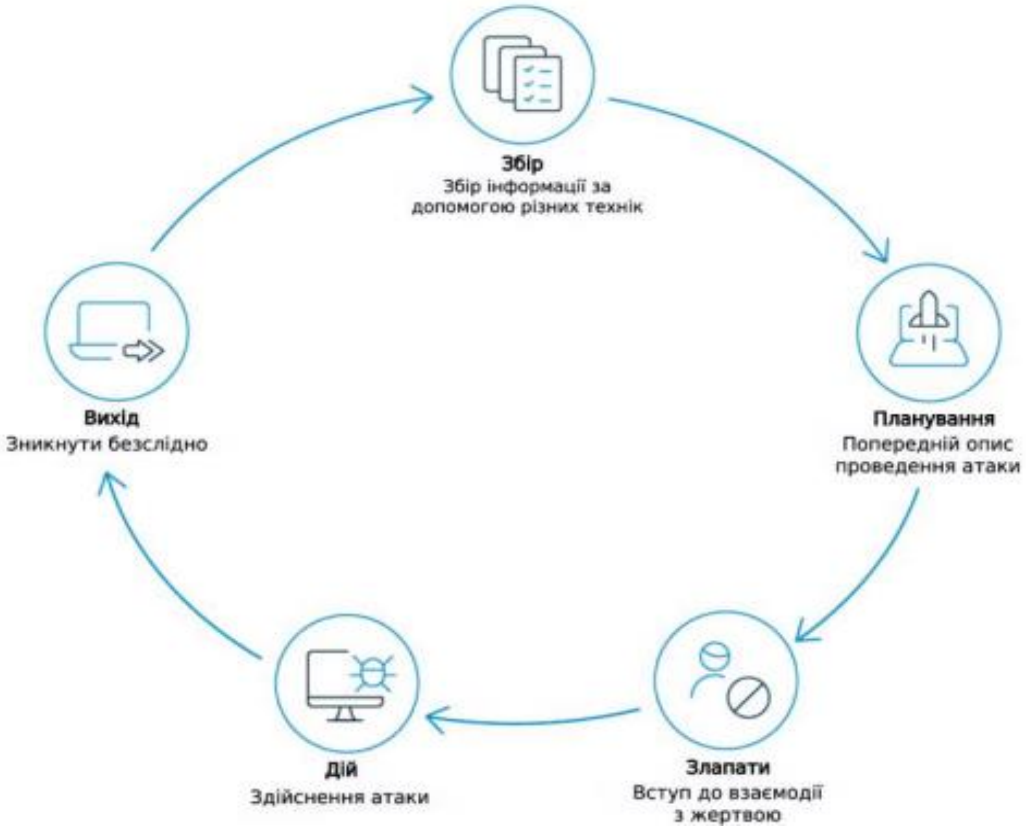


Рисунок 1.1 – Схема фішингу

1.2 Методи захисту від Фішингу

Фішингові атаки викликають усе більше занепокоєння у компаній. Згідно з нещодавнім звітом IBM , фішинг є другою за поширеністю причиною витоку даних, але також і найдорожчою атакою, коштуючи підприємствам у середньому 4,91 мільйона доларів.

Нижче наведено декілька способів захистити себе від фішингу:

- перевірка вмісту;
- перевірка посилання;
- захист своєї особи;
- електронні листи з цифровим підписом.

Більшість фішингових електронних листів мають багато помилок у своєму вмісті, вони адресуються безпосередньо користувачам та використовують їх

особисту інформацію для того щоб обдурити, але вони не містять повної інформації про користувачів. Якщо уважно вивчити тему та зміст таких електронних листів, можна отримати уявлення про їх достовірність або ж ні. Це допоможе уникати таких надходжень та захистити свої данні від зловмисників.

Потрібно бути обачним, надаючи конфіденційну інформацію, таку як облікові дані для входу, дані кредитної картки, номери телефонів або банківські реквізити, слідкувати за поганою граматикою та орфографічними помилками.

Основний трюк злочинів полягає в тому, що вони створюють відчуття важливості та терміновості своїми фішинговими електронними листами. Можна потрапити в пастку, лише якщо пізно вжити заходів. Отже, важливо зберігати спокій, думати, перш ніж клацати, та робити кроки мудро.

Щоб запобігти фішингу, рекомендується двічі перевіряти адреси електронної пошти та посилання на веб-сайти, перш ніж натискати посилання.

Хоча шахрайська електронна адреса майже ідентична оригінальній адресі, вона не така сама й часто має незначні зміни в написанні чи використанні літер.

Якщо посилання запитує інформацію для входу, переходити потрібно безпосередньо на веб-сайт, а не за посиланням в електронному листі.

Захист своєї особи - VPN, або віртуальна приватна мережа, забезпечує зашифрований тунель для всіх дій в інтернеті. Він приховує оригінальну особу і місцезнаходження та дозволяє підключатися до інтернету через захищені віддалені сервери. Це виключає ймовірність шпигунства та сталкінгу, а кіберзлочинці не зможуть отримати доступ до інформації та особистих даних. Надійний VPN також допомагає захистити з'єднання від будь-якого зловмисного програмного забезпечення та робить життя онлайн безпечним. VPN – це безпечний бар'єр на шляху фішингових електронних листів до пристрою.

VPN є одним із інструментом який хакери, кіберзлочині використовують на постійній основі, у користуванні вони навчилися приміняти так званий "Режим бога", е такий режим коли справжню особу яка стоїть то за атакою або за любими противозаконними діями знайти нереально, відслідкувати важко через те що IP-

адреса динамічна та змінюється кожну мілісекунду, в такому випадку відслідкувати ціль стає майже за гранню нереального. Це настільки обширний інструмент для використання, що навіть уявити важко де тільки його можна застосувати. Тому відмовлятися від використання такої програми є поганою ідеєю

П’ять основних принципів боротьби з фішингом

Інформувати співробітників про поточні загрози фішингу - методи фішингу та їх приводи, які використовують кіберзлочинці, щоб зробити свої атаки реалістичними, регулярно змінюються. Співробітники повинні бути навчені поточним тенденціям фішингу, щоб збільшити ймовірність того, що вони зможуть ідентифікувати фішингові атаки та належним чином реагувати на них.

Вчити співробітників повідомляти про підозрілі електронні листи - більшість фішингових атак не націлені на одного співробітника компанії. Крім того, зловмисник може надіслати серію електронних листів і виконати пошук у всьому каталозі електронної пошти організації в алфавітному порядку. Виконання такої великомасштабної атаки збільшує шанси, оскільки вистчатиме лише однієї людини, яка має потрапити на аферу, щоб атака рахувалася успішною. Ось чому важливо навчити своїх співробітників повідомляти про електронні листи, які виглядають як фішингові атаки. Навіть якщо один співробітник не стане жертвою фішингової атаки, інший може стати її жертвою. Якщо IT/служби безпеки дізнаються про атаку, вони можуть вжити заходів для видалення зловмисних електронних листів до їх відкриття, видалення зловмисного програмного забезпечення або скидання паролів уражених атакою користувачів.

Проінформувати співробітників про корпоративну політику електронної пошти - кожна організація повинна мати політику безпеки електронної пошти, включаючи принципи боротьби з фішингом, які визначають правильні міри використання електронної пошти (та інших комунікаційних рішень). Ця політика описує прийнятні та неприйнятні аспекти використання та способи реагування на потенційні атаки, наприклад повідомлення про підозрілі електронні листи та видалення всього відомого фішингового вмісту. Так як більшість фішингових атак

проводяться саме на співробітників різних організацій це є обов’язковим пунктом для виконання, адже саме недосвідчений робітник який незнаю простих правил є ціллю номер один для кіберзлочинців, які можуть вільно напрвити на нього атаку та призвести до втрати не тільки репутації, але й грошей компанії де він працює.

Ознайомитися з найкращими методами захисту пароля - Облікові дані користувача є однією з основних цілей кіберзлочинців. Якщо зловмисник має пароль співробітника, виявити триваючі атаки може бути набагато складніше, оскільки вони можуть маскуватися під простого користувача. Крім того, працівники зазвичай використовують один і той самий пароль для кількох онлайн-акаунтів, а це значить що один зламаний пароль може надати зловмиснику доступ до кількох онлайн-акаунтів співробітника, з цієї причини крадіжка облікових даних є звичайною метою фішингових електронних листів. Важливо розповісти співробітникам про загрозу, яку представляють фішингові електронні листи, і про найкращі методи захисту паролів. До них належать необхідність використовувати унікальні, надійні паролі для всіх своїх облікових записів, ніколи не повідомляти паролі (особливо електронною поштою) і ніколи не вводити пароль на сторінці, на яку переходять за посиланням, надісланим електронною поштою.

Розгорнути автоматизовану систему для захисту від фішингу - незважаючи на всі зусилля компаній, навчання простій кібербезпеці не може повністю запобігти фішинговим атакам.

Атаки стають все більш витонченими і в деяких випадках навіть можуть ввести в оману експертів з кібербезпеки, хоча тренінги з фішингу можуть допомогти зменшити кількість успішних фішингових атак проти компаній, але ж можливо, що деякі електронні листи все одно надійдуть.

Для мінімізації ризику фішингових атак для організації потрібне антифішингове програмне забезпечення на основі штучного інтелекту, здатне ідентифікувати та блокувати фішинговий вміст у всіх комунікаційних службах організацій (електронна пошта, програми для підвищення продуктивності тощо) і платформах (робочі станції співробітників , мобільні пристрої тощо).

Використання такого програмного забезпечення зможе додатково захистити організацію на яку проводитимуться атаки, збереже репутацію, фінанси, а найголовніше збереже конфіденційні данні які є головним активом усіх організацій. Відмовлятися від таких програм не рекомендується цілком та взагалі. 10 найкращих інструментів для боротьби з фішингом

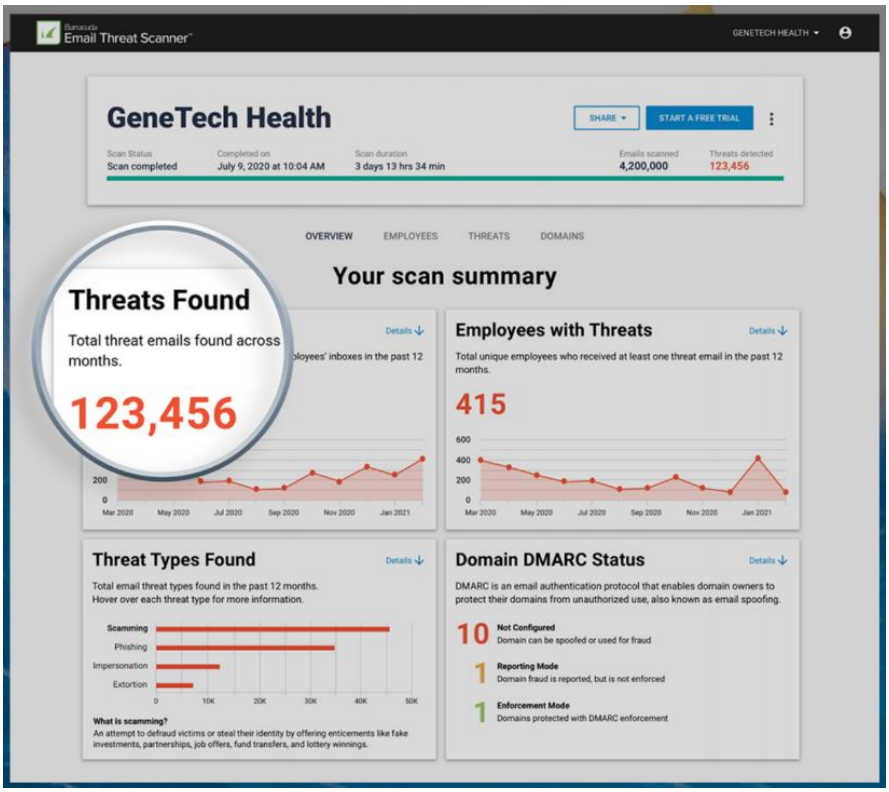


Рисунок 1.2 Barracuda Impersonation Protection

Barracuda Impersonation Protection використовує AI та ML для виявлення та блокування атак на електронну пошту, націлених на бізнес, включаючи компрометацію корпоративної електронної пошти та захоплення облікових записів співробітників.

Найкраще підходить для корпорацій.

Безпека, що забезпечує Barracuda забезпечує захист електронної пошти в режимі реального часу на основі штучного інтелекту, що дуже корисно для збереження наших даних у безпеці. Безпека на основі ШІ забезпечує надійний захист від загроз без налаштування користувача.

Висока ефективність цієї програми для виявлення атак позбавляє від необхідності вказувати, як ваша система має виявляє загрози, або створювати політики виявлення. Завдяки високій ефективності, вона залишається однією з десяти найкращих антифішингових програм. Статистика за рік показала та довела, що використанням цієї програми не є поганим варіантом для організації.

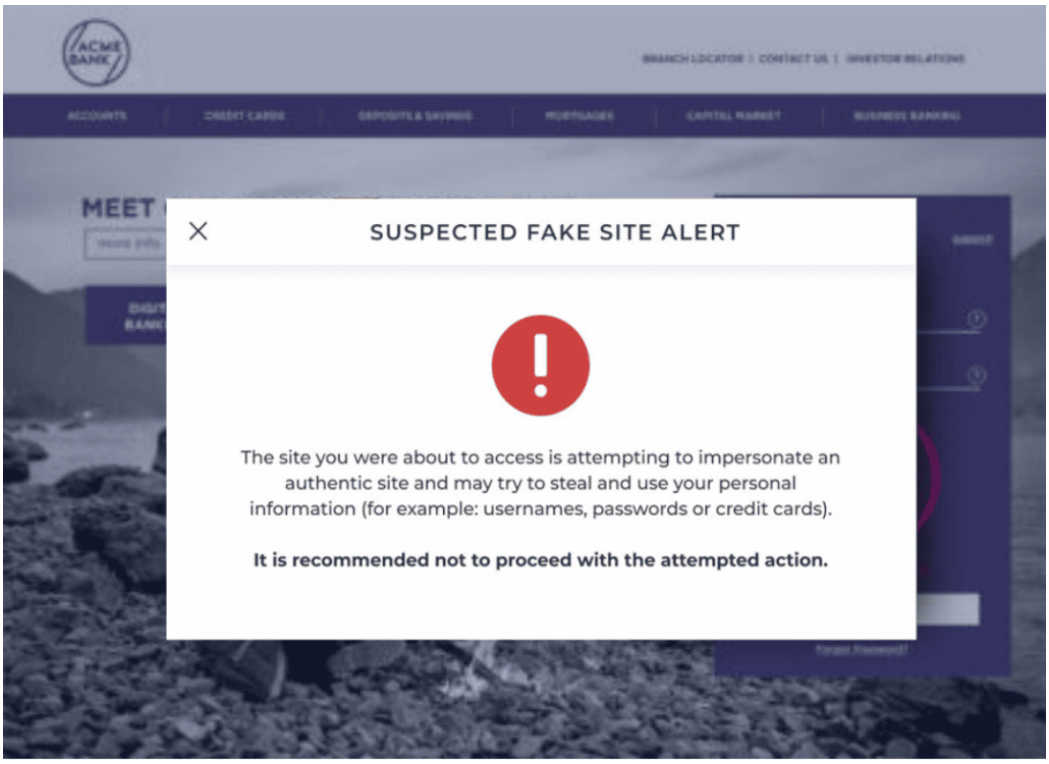


Рисунок 1.3 – Мемцико

Memcyco захищає кінцевих користувачів за межами традиційного периметра корпоративної безпеки, виходячи за рамки того,
що пропонують більшість засобів захисту від фішингу, захищаючи всіх кінцевих користувачів, включаючи клієнтів, від шахрайства.

Найкраще для організацій будь-якого розміру, яким потрібне комплексне рішення для захисту від фішингу, ефективне як у корпоративному середовищі, так і за його межами.

Він працює в режимі реального часу та надає користувачам візуальне підтвердження безпеки через непідробний водяний знак на веб-сайті та електронних листах.

Цифри статистики за останній місяць цього менеджера паролів дивують, завдяки його роботі було пом’якшено нападів аж на вісімдесят дві тисячі користувачів, це дуже велика цифра та мало програм на таке спроможні, захищено повністю від атак одинадцять тисяч користувачів, тобто це означає що захищені не тільки данні а й зекономлена величезна кількість коштів які могли втратитись якби атаки були успішними. Перекрито більше ніж вісімсот чотирнадцять тисяч атак, це величезна цифра для нашого часу, адже кожна атака особлива по своєму.

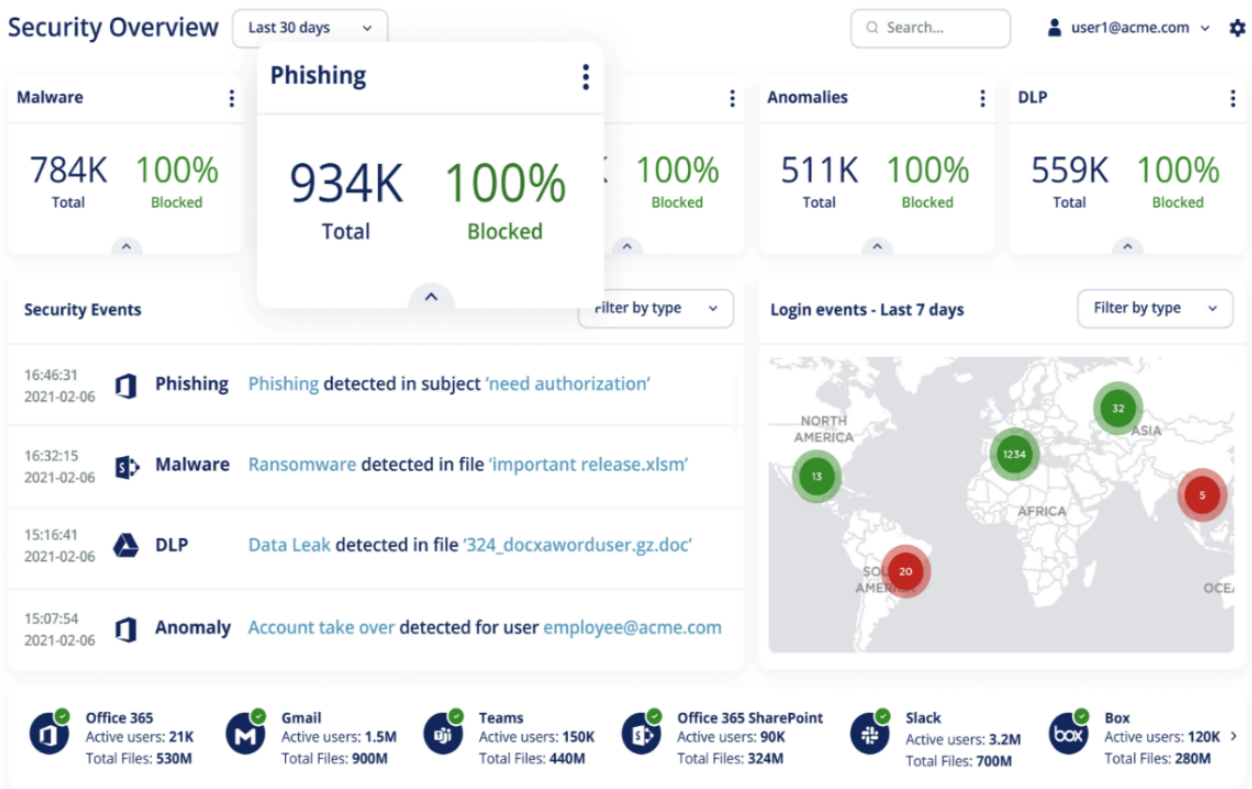


Рисунок 1.4 – Avanan, через CheckPoint

Основні функції: Avanan від CheckPoint використовує штучний інтелект і машинне навчання для забезпечення захисту всього сайту для хмарних рішень. Його API в один клік запобігає зламу корпоративної електронної пошти,

блокуючи фішинг, зловмисне програмне забезпечення, витік даних і спроби захоплення облікових записів співробітників у всій організації.

Найкраще для компаній, які шукають універсальне рішення для своєї хмарної платформи та захисту корпоративної електронної пошти.

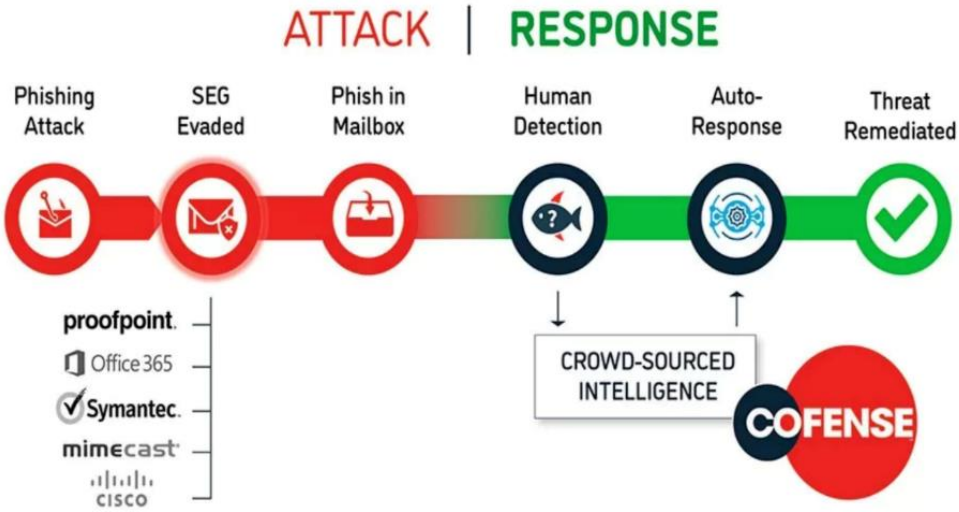


Рисунок 1.5 – Cofense

Була створена комп’ютерною службою захисту безпеки емейлів у США.

Cofense зосереджується на блокуванні фішингових загроз за допомогою AI та ML для автоматичного виявлення та реагування. Він включає доступ до професійної групи аналізу фішингових загроз, яка постійно аналізує нові загрози та надає організаціям зібрані дані.

Найкраще для великих організацій із власними командами безпеки та аналітиками, які шукають рішення, яке працюватиме рука об руку з їхніми поточними засобами для захисту працівників.

IRONS CALES використовує поєднання штучного інтелекту та людської винахідливості для виявлення різноманітних загроз у режимі реального часу, таких як крадіжка корпоративних облікових даних на підроблених сторінках входу, де жертви фішингових електронних листів можуть розкрити особисту інформацію, що призведе до захоплення облікового запису.

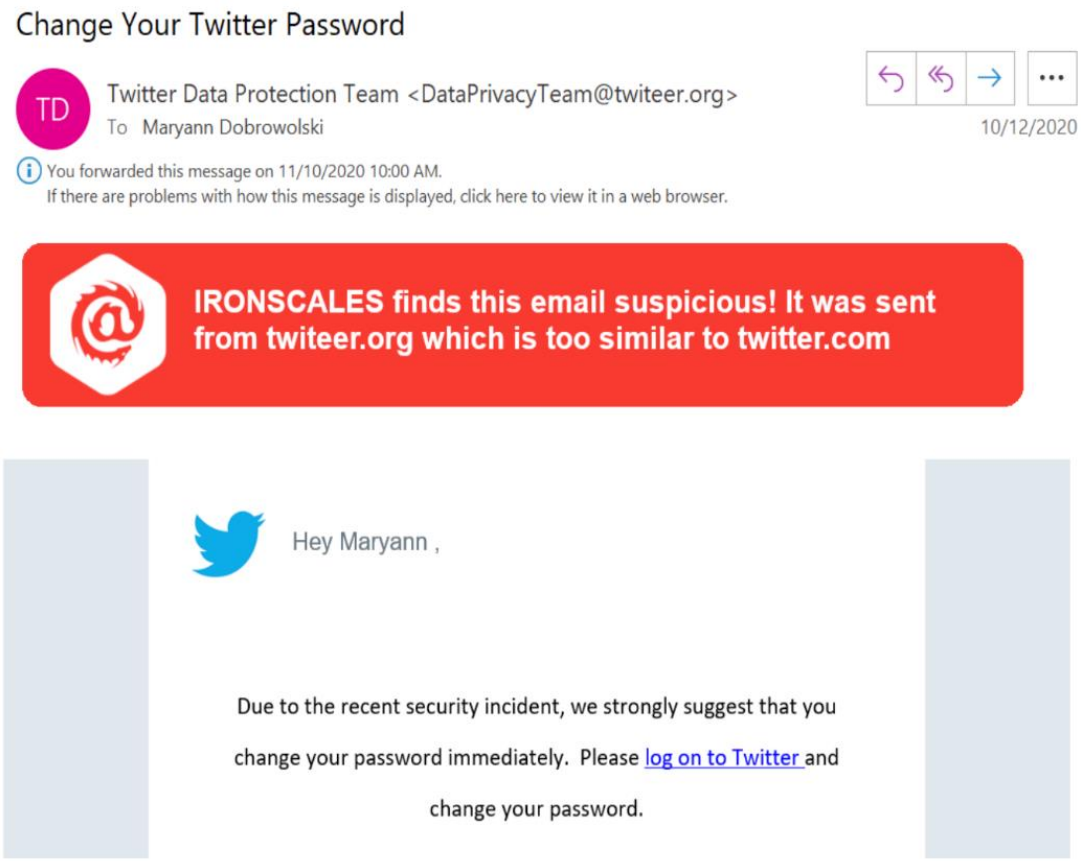


Рисунок 1.6 – IRON CALES

Найкраще для організацій з обмеженими IT-ресурсами, яким потрібне автоматизоване рішення для виявлення загроз для співробітників у режимі реального часу, приваблює функціоналом та дуже проста у використанні для них.

Рисунок 1.7 – KnowBe4

Надає перевагу обізнаності співробітників. Він також включає реагування на інциденти та можливості криміналістичного аналізу. Спеціальні модулі ML підтримують різні етапи фішингової атаки. Наприклад, PhishER обробляє

фішингові та інші підозрілі електронні листи, про які повідомляють користувачі, групуючи та класифікуючи їх на основі правил, тегів і дій. Тим часом PhishRIP поміщає на карантин підозрілі повідомлення, які все ще знаходяться в поштових скриньках у всій організації. PhishFlip перетворює фішингові електронні листи на можливості навчання, перетворюючи їх на симуляцію фішингових кампаній.

Найкраще для організацій, які хочуть запровадити програми інформування співробітників про фішинг.

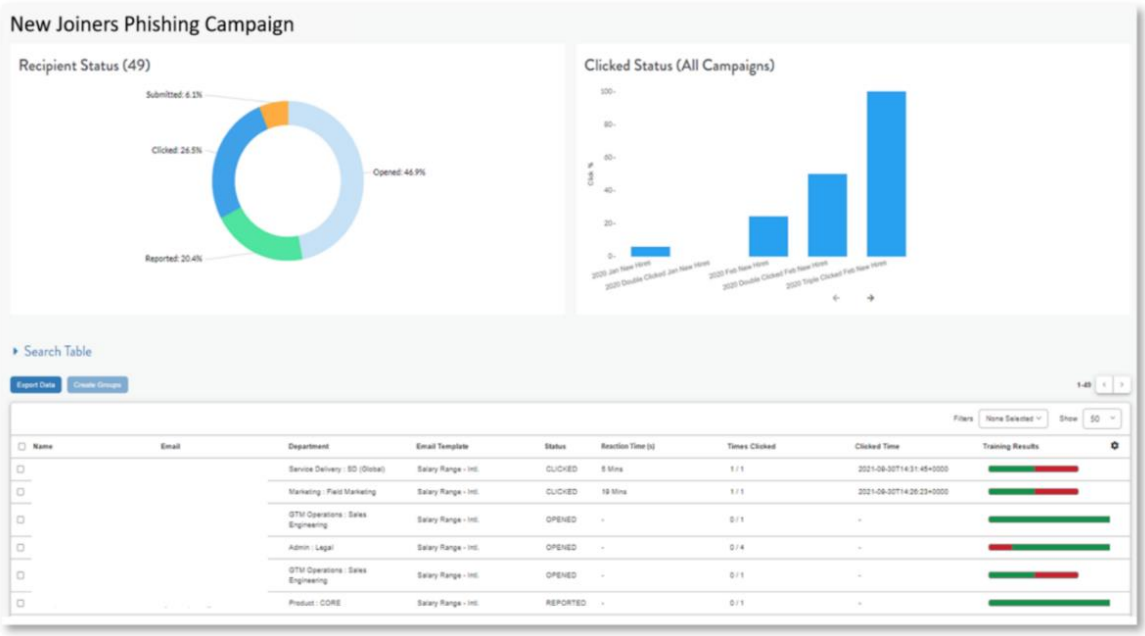


Рисунок 1.8 – Mimecast

Був розроблений американською компанією, спеціалізація якої падає на хмарне управління електронною поштою Microsoft Office 365 та Microsoft Exchange. Туди входить служба безпеки, архівування та постійний захист бізнес пошти.

Mimecast — це хмарне середовище електронної пошти, яке використовує AI та ML для захисту корпоративної електронної пошти від різних загроз, включаючи спам, фішинг, зловмисне програмне забезпечення, URL-адреси та шкідливі вкладення.

Найкраще для організацій, які отримують велику кількість електронних листів, і потребують загального фільтра від фішингу, спаму та інших атак на співробітників.

Рисунок 1.9 – Cybeready

CybeReady пропонує автономну платформу програм безпеки, створених для підприємств.

Найкраще для підприємств у банківській, виробничій та фармацевтичній галузях, які прагнуть запровадити навчання з питань безпеки як регулярну практику. Також банки є одними із перших цілей для зловмисників тому для них це найкращий варіант, щоб захистити свої активи та цінну інформацію клієнтів.

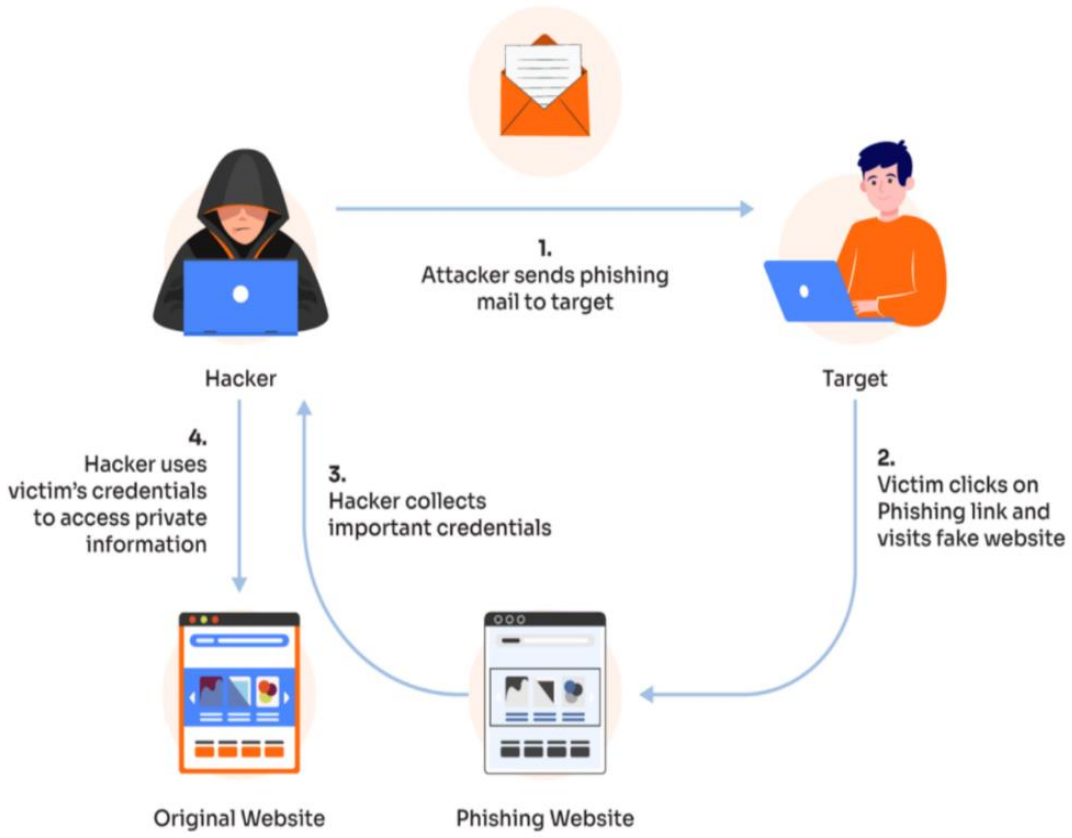


Рисунок 1.10 – Valimail

Valimail надає DMARC-як-сервіс і розміщений DMARC (звітування про автентифікацію повідомлень на основі домену та відповідності). Програма ідентифікує особу відправника, припиняючи атаки і надає захист інформації.

Підходить для невеликих компаній, які хочуть зрозуміти загальний стан безпеки електронної пошти.

Програма була розроблена компанією Valimail яка знаходиться у Каліфорнії, Сан-Франциско. Більше ніж сорок п'ять тисяч компаній використовують програму, для захисту даних, в список таких компаній входять такі відомі Doordash, Glossier, Uber, Yelp.

Вона стовідсотково визначає особу відправника та визначає це атака чи справжній мейл надісланий від людини, партнера, тощо. Змогла зберегти активів більш аніж на чотириста тисяч доларів, що вирізняє її поміж інших програм. Вона

є найкращим автоматизовани рішенням для компаній, яка дає змогу загально захистити електронну пошту та рівень її безпеки.

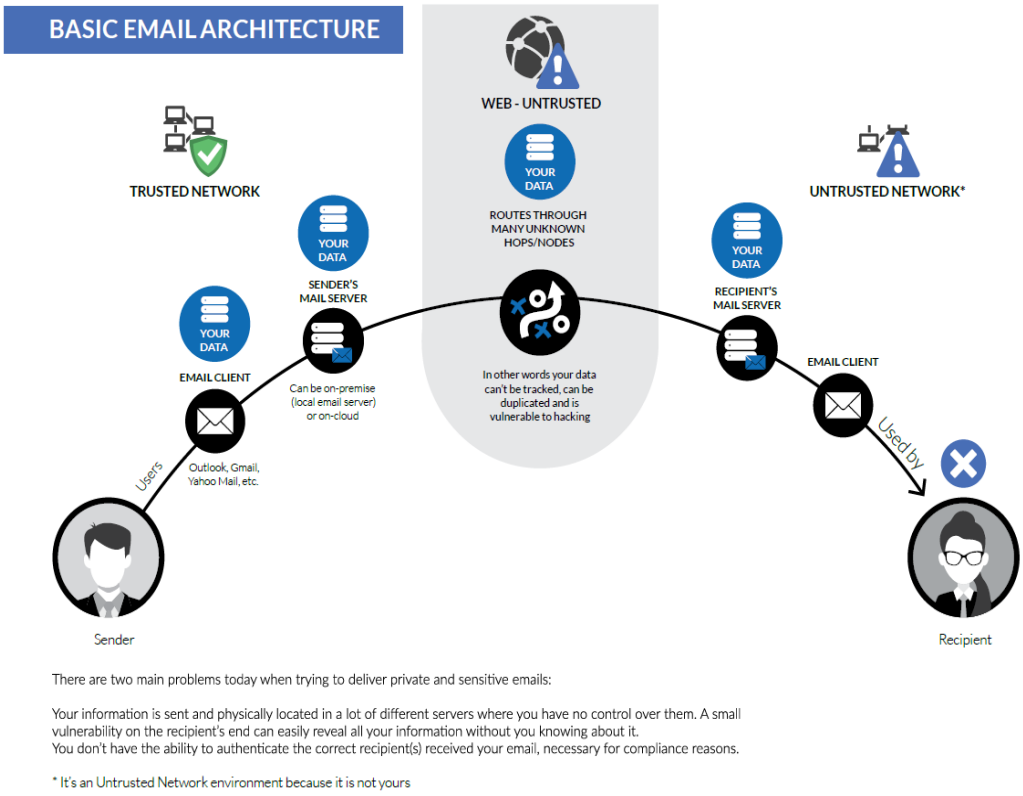


Рисунок 1.11 – Trustify

Trustify пропонує вибір корпоративних рішень безпеки електронної пошти, які організації можуть налаштувати відповідно до своїх потреб безпеки та відповідності. Він забезпечує безпеку вхідних і вихідних електронних листів від одного постачальника, виявлення поведінки на основі штучного інтелекту, виявлення зламаного облікового запису та функції архівування з настроюваним контролем доступу та дозволами.

Найкраще для організацій, які обмінюються конфіденційною інформацією електронною поштою для підтримки щоденних операцій.

1.3 Висновки до розділу

Перший розділ дослідження передбачав детальний аналіз фішингу та його видів. Фішинг, одна з найпоширеніших форм кіберзлочинності, постійно розвивається та створює нові загрози для користувачів і компаній. У цьому розділі підтверджується, що фішинг залишається реальною проблемою через його високу ефективність і постійну адаптацію до нових ситуацій.

Розглянуто різні типи фішингу, зокрема фішинг, китобійний фішинг, фармінг і SMS-фішинг. Кожна з цих технік має свої особливості, але всі спрямовані на викрадення особистої інформації користувачів, такої як логіни та паролі. Також розглянуто основні методи запобігання фішингу, зокрема використовування унікальних та надійних паролів, бути обережним з електронною поштою, перевіряти безпеку веб-сайту та використання антифішингового програмного забезпечення.

Навчання користувачів основам кібербезпеки також є важливим аспектом захисту та може допомогти зменшити кількість успішних фішингових атак. Загалом у цьому розділі наголошується на необхідності комплексного підходу до боротьби з фішингом, включаючи технологічні засоби, освітні програми та дотримання правил безпеки в інтернеті. Це значно знижує ризики та підвищує загальний рівень безпеки інформаційних систем.

2 ОБЛІКОВІ ЗАПИСИ ТА МЕТОДИ ЇХ ЗАХИСТУ

2.1 Аналіз методів захисту

Обліковий запис користувача — це об’єкт, який створюється для того, щоб надати людині доступ до ресурсів. Такий запис може представляти людину, програмну службу або комп’ютер. Облікові записи користувачів дозволяють суб’єктам входити в систему, встановлювати параметри та отримувати доступ до ресурсів на основі дозволів облікових записів. Обліковий запис користувача є одним із найкращих методів автентифікації в системі та отримання необхідного доступу до ресурсів цієї системи.

Облікові записи електронної пошти є одним із найпоширеніших прикладів облікових записів користувачів, деякі комп’ютерні системи є однокористувацькими системами і не вимагають використання облікових записів користувачів, дії пов’язані з користувачем, зберігаються в домашньому каталозі та захищені від доступу несистемних адміністраторів.

Безпека системи значною мірою залежить від того, наскільки добре керуються облікові записи користувачів, облікові записи користувачів забезпечують доступ до мереж, пристроїв, програмного забезпечення та даних.

Фахівцям з кібербезпеки дуже важливо розуміти, що таке облікові записи користувачів і як ними правильно керувати. Облікові записи користувачів є основними цілями для кібератак, оскільки мільярди облікових записів по всьому світу мають доступ до конфіденційних даних і систем, захист цих даних є ключовим для захисту цифрової інформації та активів.

Дотримуючись рекомендованих інструкцій щодо створення, керування, моніторингу та контролю облікових записів користувачів, організації можуть покращити безпеку та зменшити ризики, пов’язані з обліковими записами.

Привілейовані облікові записи, такі як обліковий запис root і облікові записи адміністратора, забезпечують високий рівень привілеїв на комп’ютері, їх зловмисники використовують для викрадення інформації, зміни конфіденційних

даних, зміни конфігурації системи та приховування активності, його також можна використовувати для встановлення та видалення програмного забезпечення та оновлення операційної системи.

Тому моніторинг привілейованих облікових записів має вирішальне значення для запобігання кіберзлочинам серед співробітників і виявлення шкідливих програм.

Privileged Access Management — це технологія контролю та моніторингу доступу до привілейованих облікових записів, щоб зменшити ризик і захистити систему, важливо правильно керувати ролями облікових записів, застосовувати суворі політики безпеки та обмежувати доступ, облікові записи користувачів і служби, які чітко не розділені або належним чином не захищені, можуть становити серйозну загрозу.

Облікові записи користувачів - вони працюють через процес автентифікації та авторизації, аутентифікація підтверджує особу користувача - зазвичай це включає ім’я користувача та пароль, але також може включати багатофакторні методи, такі як ключі безпеки, одноразові паролі та біометричні дані (відбитки пальців, розпізнавання обличчя).

Методи автентифікації перевіряють, чи користувачі є тими, за кого себе видають, перш ніж допустити їх до системи. Після автентифікації авторизація визначає рівень доступу користувача, захист облікових записів користувачів надзвичайно важливий для будь-якої компанії, організації чи сайту.

Дотримання найкращих практик, таких як надійні й унікальні паролі, обмеження привілеїв і моніторинг підозрілої активності, може допомогти запобігти несанкціонованому доступу та захистити конфіденційні системи та дані.

Реалізація багатофакторної автентифікації та єдиного входу, коли це можливо, забезпечує додатковий рівень захисту для облікових записів користувачів, оскільки кіберзагрози стають дедалі складнішими, надійний захист облікових записів користувачів стає більш важливим ніж будь-коли, добре розроблена політика та засоби контролю автентифікації, авторизації та керування

обліковим записом мають важливе значення для того, щоб лише авторизовані особи мали доступ до систем та інформації, постійний моніторинг і адаптація до мінливих ризиків допомагає забезпечити безпеку облікових записів користувачів і активів, які вони захищають.

Локальні облікові записи зберігаються в локальній системі та дозволяють доступ лише до цієї системи, мережеві облікові записи зберігаються на контролерах мережевого домену та забезпечують доступ до ресурсів у мережі, віддалені облікові записи дозволяють користувачам входити в систему з віддалених місць через мережу, безпека віддаленого доступу до систем і даних вимагає застосування додаткових заходів безпеки, правильна конфігурація та керування обліковим записом мають вирішальне значення для безпеки системи та мережі. Обмеження доступу та привілеїв адміністратора може зменшити ризик їх використання зловмисниками.

Використання унікального паролю для кожного облікового запису є одним із найважливіших кроків для захисту облікових записів онлайн від несанкціонованого доступу, хоча для зручності може виникнути спокуса використовувати один і той самий пароль для кількох облікових записів, це може бути серйозним ризиком, оскільки якщо один обліковий запис зламано, хакер може легко отримати доступ до всіх інших облікових записів.

Створений довгий і складний пароль - довжина і складність важливі при створенні пароля, чим довший і складніший пароль, тим важче буде зламати його хакеру. Уникання використання типового паролю, такого як «password» або «123456», оскільки їх легко вгадати дасть можливість краще захистити обліковий запис користувача. Натомість використати комбінацію великих і малих літер, цифр і спеціальних символів. Наприклад, користувач може використовувати такий пароль, як "P@$$w0rd!" він набагато безпечніше, ніж "password123". Чим унікальнішим і складнішим є пароль, тим безпечнішим буде обліковий запис.

Розглянути можливість використання менеджера паролів – керування кількома унікальними та складними паролями може бути складним завданням. Тут стане в нагоді менеджер паролів.

Менеджер паролів надійно зберігає всі паролі в зашифрованому сховищі, тому ви можете створювати та використовувати надійні паролі, не запам'ятовуючи їх усіх, такі популярні менеджери паролів, як LastPass і Dashlane, також пропонують такі функції, як автоматична зміна пароля та двофакторна автентифікація для додаткового захисту вашого облікового запису.

Увімкнення двофакторної автентифікації (2FA) – двофакторна автентифікація додає додатковий рівень безпеки до облікового запису, вимагаючи додаткової другої форми перевірки, зазвичай отримується унікальний код, який надсилається на мобільний пристрій. Багато онлайн-платформ, включаючи веб-сайти банків, пропонують варіант 2FA.

Регулярне оновлення свого паролю – щоб зменшити ризик несанкціонованого доступу, важливо регулярно оновлювати пароль. Обов'язкове оновлення свого паролю рекомендують принаймні кожні 3–6 місяців, якщо виникла підозра про через звичайну активність у обліковому записі, негайно потрібно оновити свій пароль, який є першою лінією захисту від несанкціонованого доступу. Тому дуже важливо зробити його сильним та унікальним.

Концепція захисту облікових записів еволюціонувала в міру того, як частішали порушення безпеки.

Наприклад, багато смартфонів тепер використовують відбитки пальців або розпізнавання обличчя як безпечний метод для розблокування пристрою та доступу до облікових записів.

Машинне навчання та штучний інтелект: Машинне навчання та штучний інтелект зробили революцію в захисті облікових записів, дозволивши системам навчатися та адаптуватися до нових загроз.

Вразливості облікового запису: облікові записи можуть бути скомпрометовані різними способами, включаючи фішингові атаки, слабкі паролі, зараження зловмисним програмним забезпеченням і методи соціальної інженерії.

Розуміння таких вразливостей є важливим для розробки ефективних стратегій зменшення ризиків.

Фінансові наслідки – злам облікових записів може призвести до значних фінансових втрат як для фізичних осіб, так і для компаній, наприклад несанкціонований доступ до банківських рахунків може призвести до втрати коштів і шахрайських операцій, для вирішення яких може знадобитися значний час і зусилля.

Крадіжка особистих даних – захист облікового запису відіграє важливу роль у запобіганні крадіжці особистих даних, кіберзлочинці часто націлюються на особисту інформацію, що зберігається в облікових записах, щоб видати себе за когось із незаконною метою, як-от відкриття кредитного рахунку чи здійснення шахрайських покупок.

Відповідність законодавству та нормам – багато компаній мають особливі законодавчі та нормативні вимоги щодо захисту облікових записів, недотримання цих стандартів може призвести до значних штрафів, юридичної відповідальності та шкоди репутації компанії.

2.2 Існуючі засоби захисту паролів

Захист паролем є важливим аспектом кібербезпеки, який часто не помічають або недооцінюють, базові заходи безпеки запобігають несанкціонованому доступу до конфіденційних даних і систем, і варіанти їх використання стосуються всіх типів підприємств, організацій та установ.

Захист паролем означає поєднання політик, процесів і технологій, які роблять паролі та методи автентифікації більш безпечними, це набір важливих

стратегій захисту, спрямованих на запобігання несанкціонованому доступу до конфіденційної інформації та забезпечення того, щоб співробітники використовували надійні паролі для захисту своїх облікових записів і даних.

Захист паролем є першою лінією захисту від кібератак і обмежує несанкціонований доступ до особистої та конфіденційної інформації, що зберігається в облікових записах користувачів, однак для повного охоплення захисту паролі слід використовувати в поєднанні з іншими засобами захисту, такими як брандмауери та антивірусне програмне забезпечення.

Засоби захисту паролів – захист паролю призначений для створення надійного бар'єру між конфіденційними даними та потенційними кіберзагрозами.

Політики безпеки паролів – це правила, призначені для покращення безпеки паролів шляхом заохочення користувачів створювати надійні та надійні паролі, а також зберігати та використовувати їх відповідно.

Біометрія – інтеграція біометричних методів автентифікації, таких як розпізнавання відбитків пальців, розпізнавання обличчя та сканування райдужної оболонки ока, започаткувала нову еру захисту облікових записів. Такі методи не тільки безпечні, але й зручні для користувачів. Вона є чудовим варіантом, адже доступ тоді матимуть тільки ті користувачі біометричні данні яких є у реєстрі.

Паролі мають містити принаймні 12 символів, містити великі та малі літери, знаки пунктуації та уникати клавіатури, яку легко запам'ятати, або шляхів клавіатури, шифрування додатково захищає паролі, навіть якщо їх вкраде кіберзлочинець, найкраще розглянути незворотне наскрізне шифрування, це дозволяє захистити паролі під час їх переміщення у мережі, також корисно реалізувати двофакторну автентифікацію.

Менеджер паролів допомагає запобігати та уникати загроз мережевій безпеці, безпечно зберігаючи та керуючи даними облікового запису онлайн та офлайн, менеджери паролів використовують комп'ютерне шифрування урядового рівня США для зберігання паролів, менеджери паролів також шифрують паролі користувачів, забезпечуючи безпечний доступ. Захист паролем при правильному

використанні може ефективно перешкодити хакерам і запобігти різним формам витоку даних, найкращим захистом від цих загроз є обізнаність і навчання безпечним онлайн-практикам, створення надійних паролів і розуміння того, як працюють ці методи злому.

Захист паролю починається зі створення надійних паролів, це важливо для захисту облікових записів від хакерів і кіберзлочинців:

- робити паролі унікальними та не використовувати їх повторно, повторне використання ненадійних паролів підвищує ризик витоку даних, викрадення облікових записів, викрадення особистих даних та інших загроз;
- використовувати різні великі та малі літери, цифри та символи без шаблонів;
- розглянути пароль-фразу замість одного слова, пароль-фраза – це фраза або комбінація слів, яку легко запам’ятати, але іншим важко вгадати, приклад: I love eat pizza and burger!;
- уникати використання звичайних слів, фраз і шаблонів, які легко вгадати. Уникати таких загальних слів, як «password», ім’я користувача чи назва організації;
- створення та зберігання складних паролів за допомогою інструментів менеджера паролів, ці інструменти генерують випадкові складні паролі для кожного облікового запису та надійно зберігають їх;
- не використовувати особисту інформацію у паролі, таку як: ім'я, дата народження, адреса;
- переконатися, що пароль має щонайменше 12 символів, 14 або вище зазвичай краще, якщо немає чіткої моделі паролю;
- якщо пароль розкрито, використовувати двофакторну або багатофакторну автентифікацію як додатковий рівень безпеки.

Надійні паролі є одним із найкращих способів захистити облікові записи від кіберзагроз, для компаній важливо впроваджувати політики, які вимагають від співробітників дотримання цих методів захисту паролем, щоб мінімізувати ризики хакерів і потенційні порушення безпеки. Надійний пароль запорука вашої безпеки.

Коли ви зберігаєте новий пароль, хеш-функція створює хеш-версію та зберігає її на сервері.

Кожного разу, коли ви входите в систему, використовуючи свій пароль, хеш-функція повторно створює хеш, щоб перевірити, чи відповідає він тому, що зберігається. Якщо хеші збігаються, алгоритм проходить автентифікацію та виконує вхід.

Наприклад:

Оригінальний пароль: Pa$$w0rd123

Хешований пароль: 6AF1CE202340FE71BDB914AD5357E33A6982A63B

Хоча це може здатися безпечним, прості хешовані паролі не захищені від злому. Хеш-функція створює унікальний хеш лише для кожного пароля, а не для кожного користувача. Отже, якщо декілька користувачів мають пароль Pa@@w0rd321, хеш буде абсолютно однаковим.

Щоб подолати цю вразливість шифрування, інженери створюють паролі, щоб кожен хеш був унікальним, навіть якщо паролі ідентичні.

Наприклад:

Два однакових пароля: Pa@@w0rd321

Пароль один перед хешем: Pa@@w0rd322E1A421

Пароль два перед хешем: Pa$$w0rd368795EERT11YYY

Перше хешоване значення пароля (SHA256): 52EA3894B2049 C40322D49F9A72E4F1436C90F048F59027HD9C8C8900A5C3K8

Друге хешоване значення пароля (SHA256): B4B6603ABC670 967E99C7E7F1389E40CD16E78AD38EB1468EC2AA1E62B8BED3A

Стандарт шифрування даних (DES) - хоча програми більше не використовують стандарт шифрування даних (DES), важливо згадати цей метод шифрування пароля через його історію та вплив на безпечніші сучасні стандарти.

IBM розробила DES як технологію 56-бітного шифрування на початку 1970-х років. АНБ прийняло та вдосконалило DES до того, як він був схвалений у всьому світі як стандарт шифрування.

Однак з кінця 70-х років хакерам вдалося зламати паролі, зашифровані DES. У 1999 році етичним хакерам вдалося зламати ключ DES менш ніж за 24 години.

Щоб зробити DES більш безпечним, інженери створили Triple DES, а пізніше Advanced Encryption Standard (AES), який ми використовуємо й сьогодні.

Потрійний DES - Triple DES використовує три 56-бітні ключі (блоки) для створення 168-бітного шифрування (деякі експерти з безпеки стверджують, що Triple DES є лише 112-бітним). Хоча Triple-DES поступово припиняється, багато фінансових установ все ще використовують його для шифрування PIN-кодів банкоматів.

Розширений стандарт шифрування (AES) - AES — це новий стандарт шифрування, якому довіряють уряд Сполучених Штатів і багато інших відомих організацій у всьому світі. При 128 бітах AES достатньо безпечний, але більшість організацій віддають перевагу потужному 256-бітному шифруванню.

У TeamPassword використовується 256-бітне шифрування для зберігання паролів, забезпечуючи найвищий рівень безпеки для клієнтів. Він також є безпечним хостинг-провайдером, який має численні акредитації безпеки.

Хакери можуть зламати пароль, зашифрований AES, лише за допомогою атаки грубої сили, намагаючись знайти потрібну комбінацію паролів.

Щоб протистояти атакам грубої сили, програми блокуватимуть обліковий запис після певної кількості спроб або використовують такі інструменти, як reCAPTURE від Google.

2.3 Огляд менеджерів паролів

Менеджер паролів надійно зберігає всі паролі, це єдиний спосіб створити, запам’ятати та ввести унікальні паролі для всіх облікових записів онлайн.

Кожен в мережі має певну систему паролів; будь то написання їх на звичайному старому аркуші паперу, використання варіацій тієї самої фрази чи

збереження їх у браузері. Але правда в тому, що є вагомі причини, чому такі менеджери паролів, як Dashlane, стають все популярнішими, Dashlane нещодавно рекомендували Time, People Magazine, CNBC, USA Today тощо.

Люди в усьому світі почали використовувати менеджери паролів, багато дослідників і експертів з безпеки наполегливо рекомендують усім використовувати менеджер паролів, оскільки він забезпечує зручність та безпеку.

Більшість людей використовують паролі неодноразово або включають у свої паролі таку інформацію, як ім’я чи дата народження, менеджер паролів генерує довгі випадкові паролі для різних облікових записів в Інтернеті та зберігає ці паролі.

Менеджери паролів більш безпечні, ніж альтернативи: якщо не використовувати менеджер паролів для зберігання своїх паролів, то ймовірно, що користувач не зможе запам'ятати всі унікальні та надійні паролі, які йому потрібні, більшість людей повторно використовують паролі на кількох веб-сайтах, це найнебезпечніше, оскільки якщо таку базу даних паролів зламано на одному веб-сайті, то обліковий запис на іншому веб-сайті буде повністю розкрито, все що злочинцю потрібно буде зробити, це спробувати ввійти за допомогою тієї ж комбінації адреси електронної пошти та пароля.

Оцінка найкращих менеджерів паролів у 2024 році:

Безпека – проаналізувавши налаштування шифрування, які захищають кожен менеджер паролів — 256-бітне шифрування AES є стандартним для цього списку. Також знайдено такі унікальні функції, як двофакторна автентифікація (2FA) і протоколи з нульовим знанням — таким чином навіть компанія, яка стоїть за таким менеджером паролів, не зможе отримати доступ до інформації.

Особливості – менеджери паролів включають масу різних функцій, зокрема зберігання файлів, заповнення веб-форм, безпечний обмін паролями, VPN і навіть темний веб-моніторинг та багато різних корисних функій для різного типу людей.

Юзабіліті – усі функції марні, якщо користувальницький інтерфейс схожий на безлад. Глибоко покопавшись в менеджерах паролів, можна побачити, які з них

кращі для досвідчених користувачів, а які ідеальні для людей, які не розуміються на техніці.

Десять найкращих менеджерів паролів у 2024 році

1 Бітварден

Bitwarden не потребує реєстрації в службі Bitwarden. Легко можна додавати двофакторні облікові записи за допомогою сканера QR-коду. Це дуже полегшує роботу з цим менеджером паролів, та є зручною функцією.

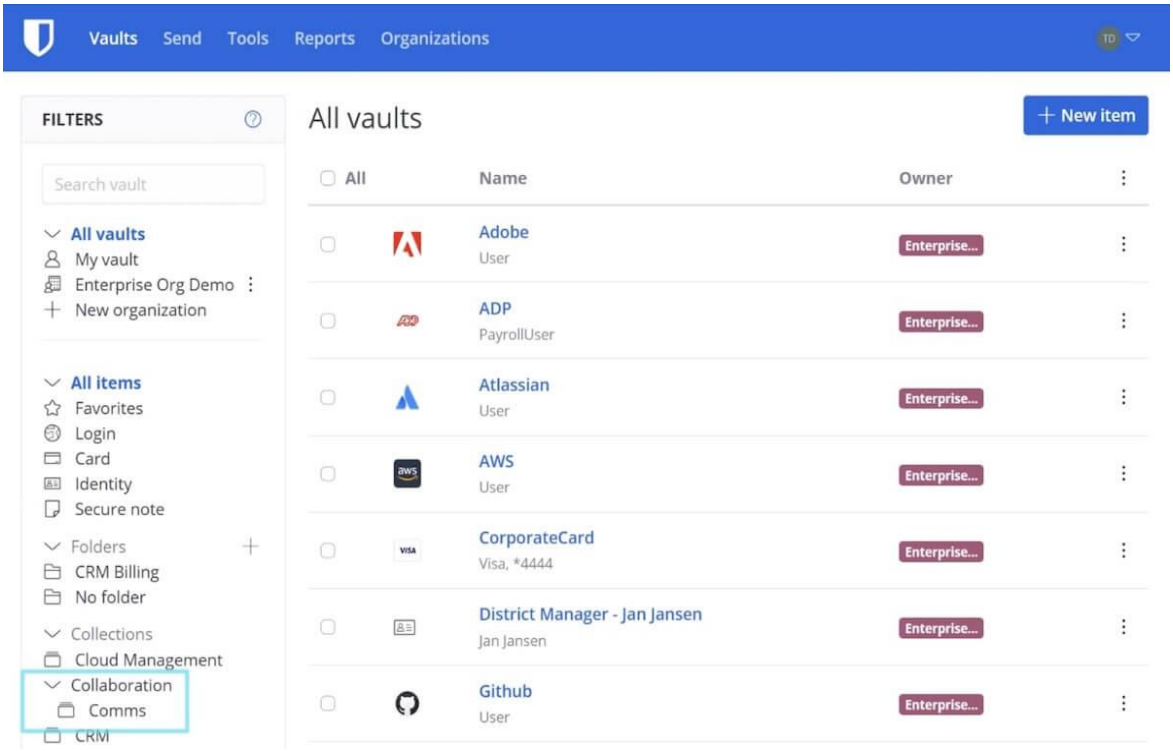


Рисунок 2.1 – Менеджер паролів Бітварден

Bitwarden — це міжплатформний менеджер паролів, який надійно зберігає конфіденційні дані та керує логінами. Це також дозволяє генерувати необмежену кількість паролів і ключів доступу на будь-якій кількості пристроїв. Функції безпеки включають нульовий рівень знань, наскрізне шифрування, комплексну відповідність і сторонні аудити безпеки програмного забезпечення з відкритим кодом, у той час як безкоштовна версія надає безпечне сховище паролів, недорогий план Premium включає екстрений доступ, звіти про стан сховища та програму

автентифікації Bitwarden. Це дозволяє підтвердити особу під час двофакторної автентифікації на веб-сайтах або в програмах.

2 KeePass

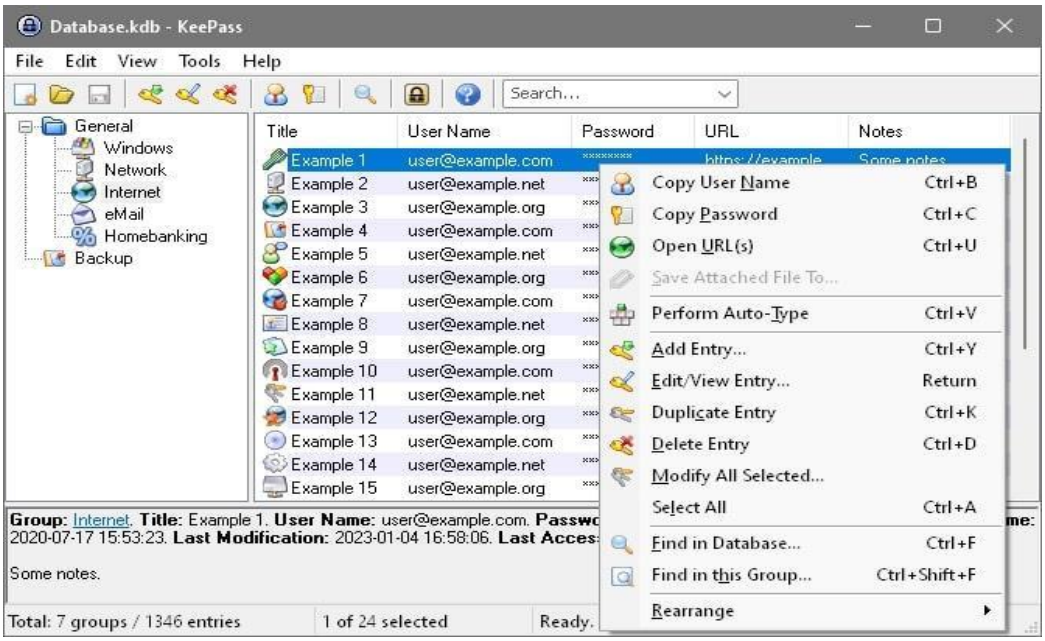


Рисунок 2.2 – Менеджер KeePass

KeePass — це безкоштовний менеджер паролів, який використовує відкритий код для зберігання всіх паролів, тому потрібно буде запам’ятати лише один пароль, щоб отримати доступ до решти. Можна встановити нагадування про регулярне оновлення паролів, а також система зберігає історію паролів, щоб уникнути їх повторного використання.

3 Дашлейн

Цей менеджер паролів був заснований у 2009 році, та випущений для ПК, Mobile.

Менеджер паролів Dashlane дозволяє зберігати паролі, ключі доступу та платіжну інформацію, а потім отримувати ці дані. Функція автозаповнення зручно надає особисті дані та облікові дані для входу, цей менеджер паролів також включає VPN і темний веб-моніторинг, який автоматично сканує ознаки того, що будь-який із ваших облікових записів міг бути зламаний.

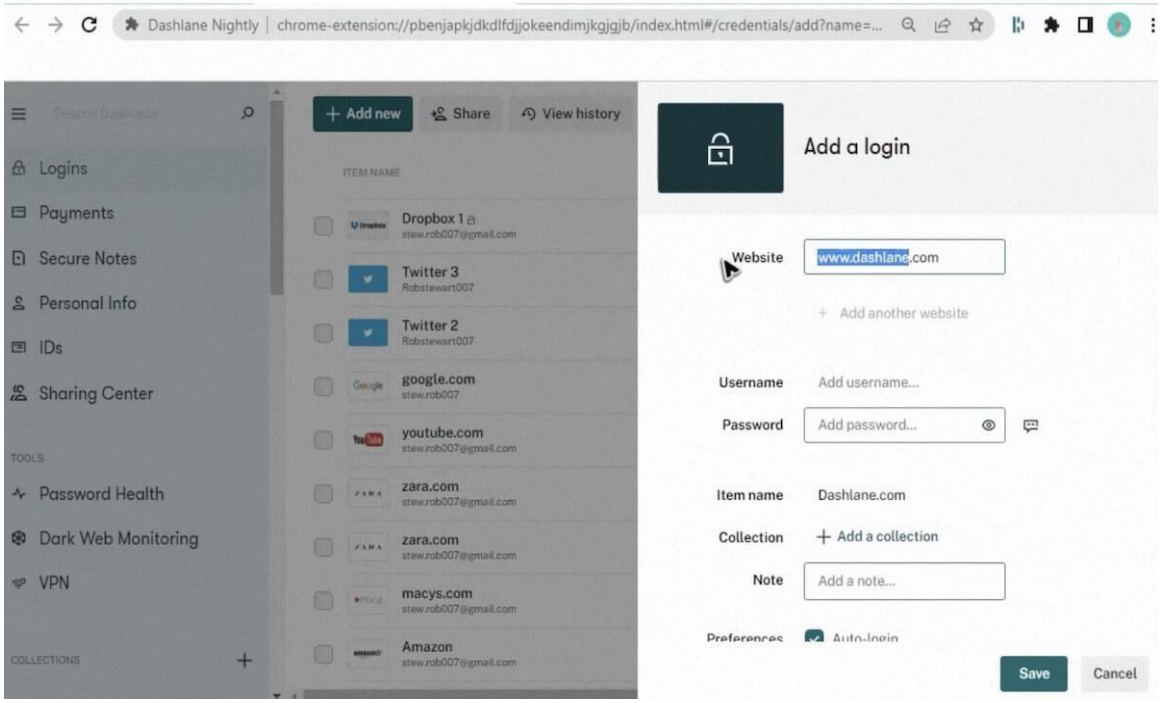


Рисунок 2.3 – Менеджер Дашлейн

Найкращі функції Dashlane:

- легко переносить інформацію з інших менеджерів паролів;
- отримання доступу до цього менеджера паролів з будь-якого пристрою чи платформи;
- використовує доповнення для більшості основних браузерів;
- безпечно ділиться паролями та легко скасовує доступ з будь-якого місця, якщо це потрібно.

Обмеження Dashlane:

- немає додатка.

4 LogMeOnce

Платформа LogMeOnce пропонує керування паролями без пароля. Можна використовувати 41ей сайді, PIN-код, відбиток пальця або біометричний ідентифікатор обличчя для входу замість пароля, хоча також можна використовувати пароль, якщо користувач бажає, безкоштовна версія дозволяє зберігати необмежену кількість унікальних паролів на будь-якій кількості пристроїв.

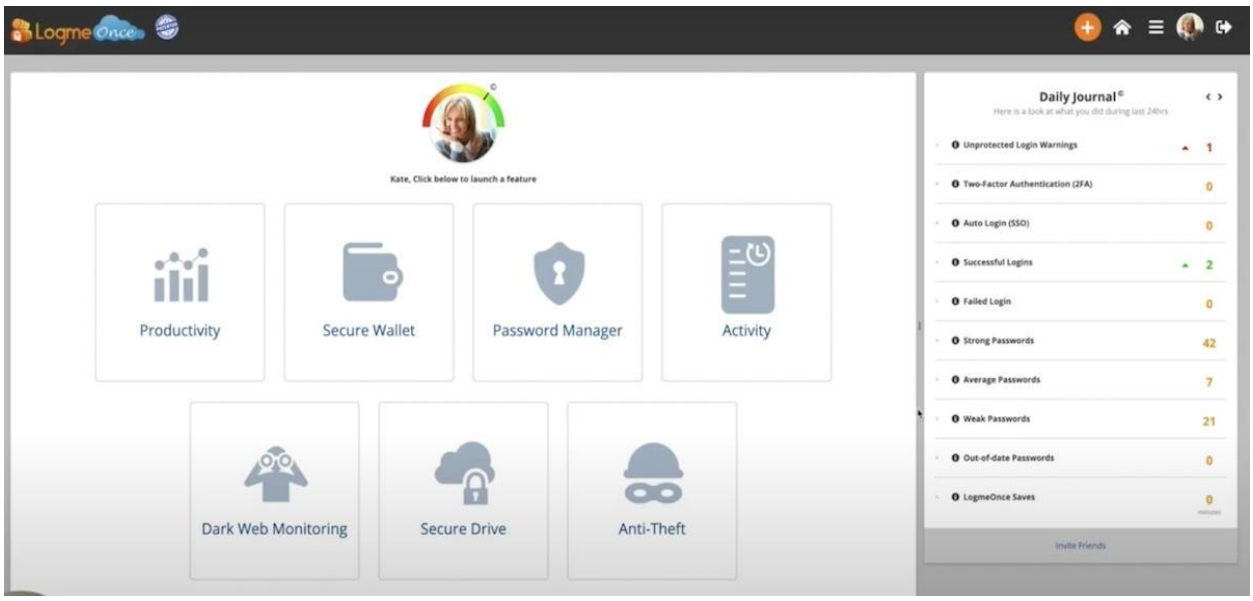


Рисунок 2.4 – Менеджер LogMeOnce

Найкращі функції LogMeOnce:

– захист своєї конфіденційну інформації за допомогою багатофакторної автентифікації;

– заощаджує час і клопоти за допомогою функції автоматичного заповнення;

– синхронізує свої дані в MacOS, Windows, Linux, Android та iOS.

Обмеження LogMeOnce:

– безкоштовна преміум-версія не пропонує екстрений доступ або багатофакторну автентифікацію.

5 1Password

1Password, розроблений для окремих осіб, сімей і співробітників у всьому світі, використовує повне шифрування для захисту ключів доступу, паролів та інших особистих даних. Функція безпечного автозаповнення економить час автозаповненням форми, а також допомагає входити в інші облікові записи, як-от Google або Apple, секретний ключ пропонує додатковий рівень безпеки, а сторонні перевірки гарантують раннє виявлення та швидке усунення будь-яких потенційних загроз.

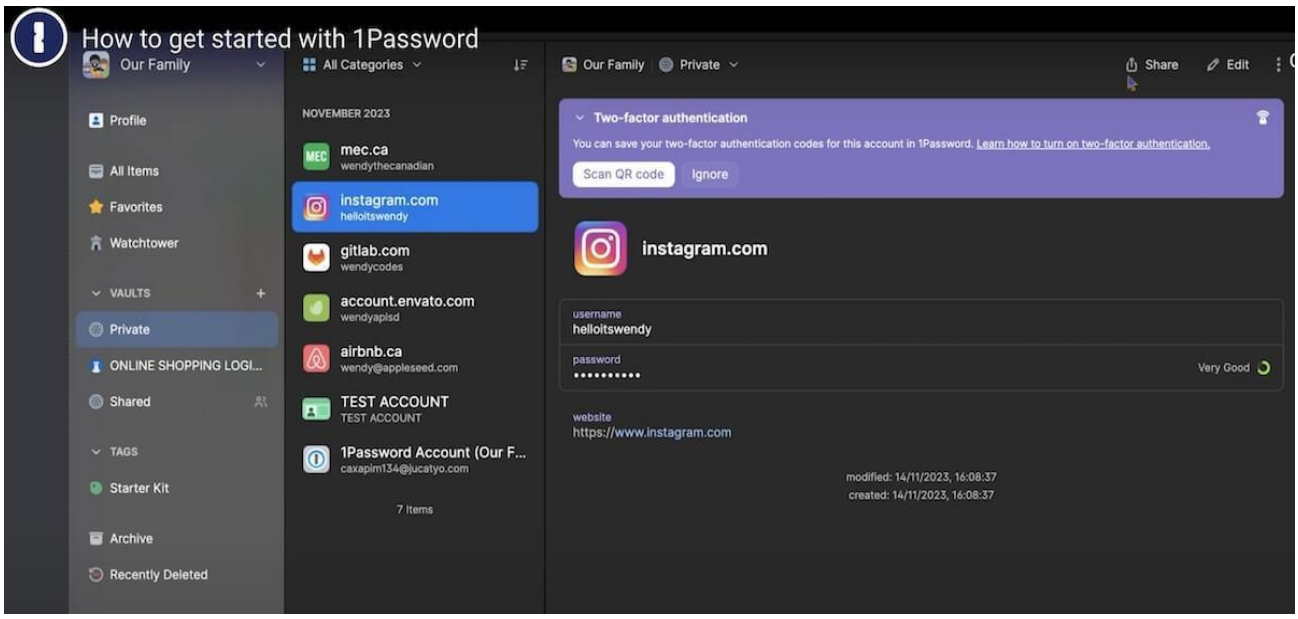


Рисунок 2.5 – Менеджер 1Password

Найкращі функції 1Password:

− просить генератор паролів створити складні паролі;

− використовує 1Password офлайн або онлайн;

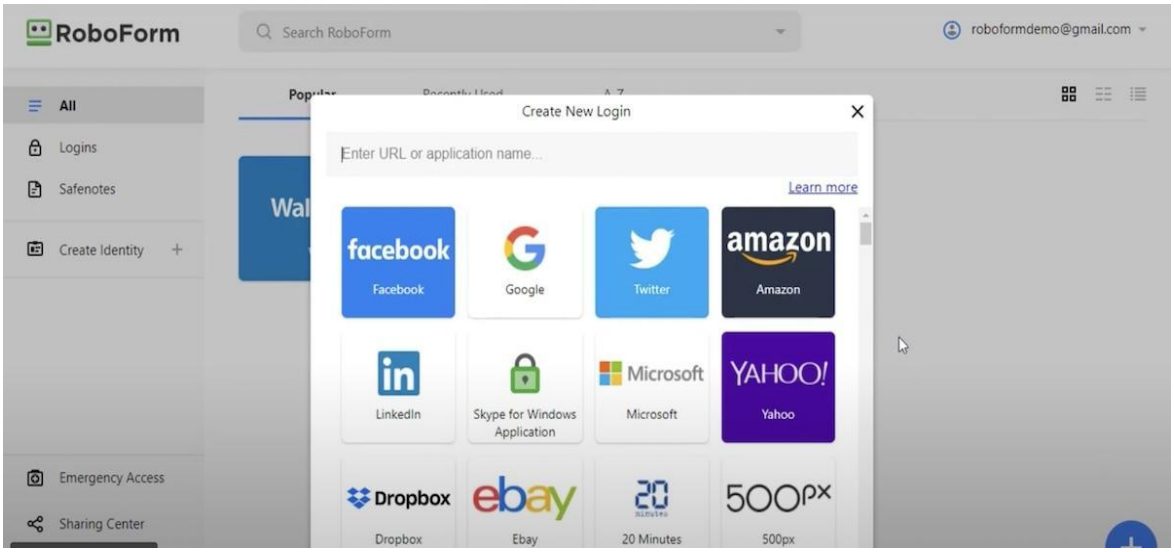
− інтеграція з іншими інструментами, такими як Microsoft, Google Workspace і GitHub.

6 RoboForm

RoboForm заснований та випущений у 1999 році компанією Siber Systems, яка є приватною та знаходиться у штаб-квартирі на території Ферфаксу, штат Вірджинія.

Він використовує шифрування AES-256 і алгоритм PBKDF2 для захисту паролів та інших приватних та конфіденційних даних.

RoboForm представляє себе як менеджер паролів нового покоління. Він генерує надійні й унікальні паролі, потім зберігає їх і швидко вводить під час наступного відвідування цього сайту, цей менеджер паролів сканує інтернет і попереджає, якщо якісь із паролів було зламано.



Рсиунок 2.6 – Менеджер RoboForm

Найкращі функції RoboForm:

– швидко заповнює форми, використовуючи збережені дані;

– використовує автентифікатор RoboForm для аутентифікації 2FA на інших сайтах;

– дає змогу надійно ділитися паролями, зберігаючи дані від сторонніх чинників;

– можливість використання RoboForm на пристроях iPhone і Android, а також у веб-браузерах.

Обмеження RoboForm:

– безкоштовний план дає доступ лише на одному пристрої.

7 NordPass

NordPass це менеджер паролів який був створений у 2019 році та досі є одним із найкращих менеджерів паролів що говорить про його юзабіліті та вирішення проблем на високому рівні користування, зберігаючи все на рівні шифру.

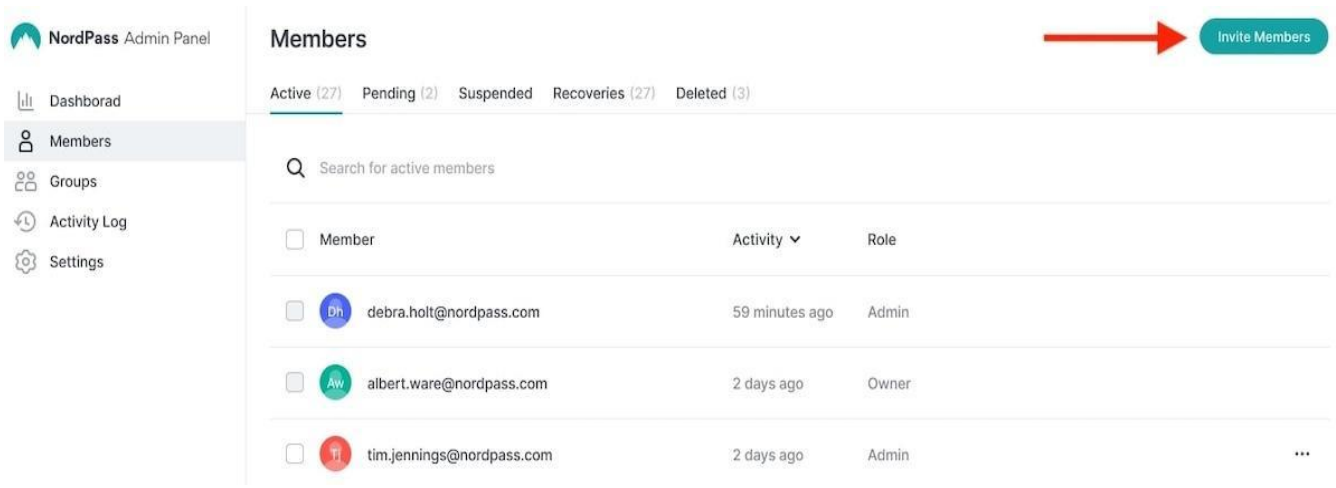


Рисунок 2.7 – Менеджер Nord Pass

NordPass — це простий у користуванні «цифровий менеджер життя», який генерує та зберігає паролі та дозволяє безпечно ними ділитися. Він також зберігає дані кредитних карток та автоматично заповнює форми, цей менеджер паролів підтримує кілька типів багатофакторної автентифікації та пропонує доступ до облікового запису довіреному другу або члену сім'ї в разі надзвичайної ситуації.

Найкращі функції NordPass:

– дізнається, чи ваші дані були скомпрометовані за допомогою Data Breach Scanner;

– надійно зберігає іншу інформацію, наприклад паролі Wi-Fi або номер соціального страхування.

Обмеження NordPass:

– безкоштовний варіант досить обмежений.

3 Enpass

Він був створений як для мобільних платформ так і для комп'ютерів, безкоштовна версія цього додатку давала можливість зберігати лише 25 паролів, в 2017 році компанія чомусь перестала випускати оновлення для блекберрі мобільних платформ а пізніше в 2018 і для Windows 10.

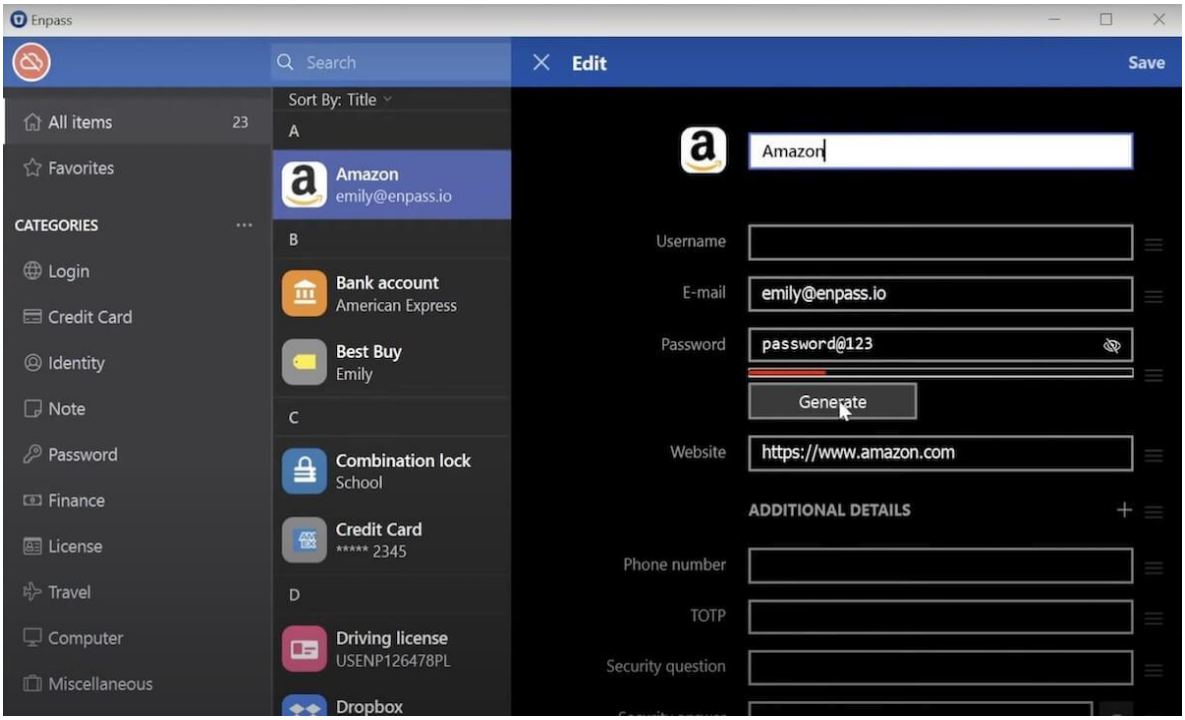


Рисунок 2.8 – Менеджер EnnPass

Enpass дозволяє зберігати паролі будь-де, де користувачу подобається, чи то OneDrive, Dropbox, Google Drive, iCloud або офлайн на вашому власному пристрої. Можливість створити окремі сховища для особистих даних, робочих даних і інформації про сім'ю. Та зберігає всі данні користувачів у зашифрованому вигляді.

Enpass найкращі функції:

– регулярно перевіряє старі та прострочені паролі за допомогою функції перевірки паролів;

– використовує один із шаблонів для зберігання різних типів інформації, наприклад даних кредитної картки, документів про страхування чи паспорта.

3 Keeper

Програма яка була створена глобальною компанією з кібербезпеки Cyber Security Inc, але спочатку був створений сам менеджер паролів Keeper у 2009 році, після чого в 2011 була заснована сама компанія. CEO компанії є Крейг Люррі та Даррен Гучіоне, програма була випущена як мультиплатформений додаток, як для телефонів так і для настільних комп'ютерів.

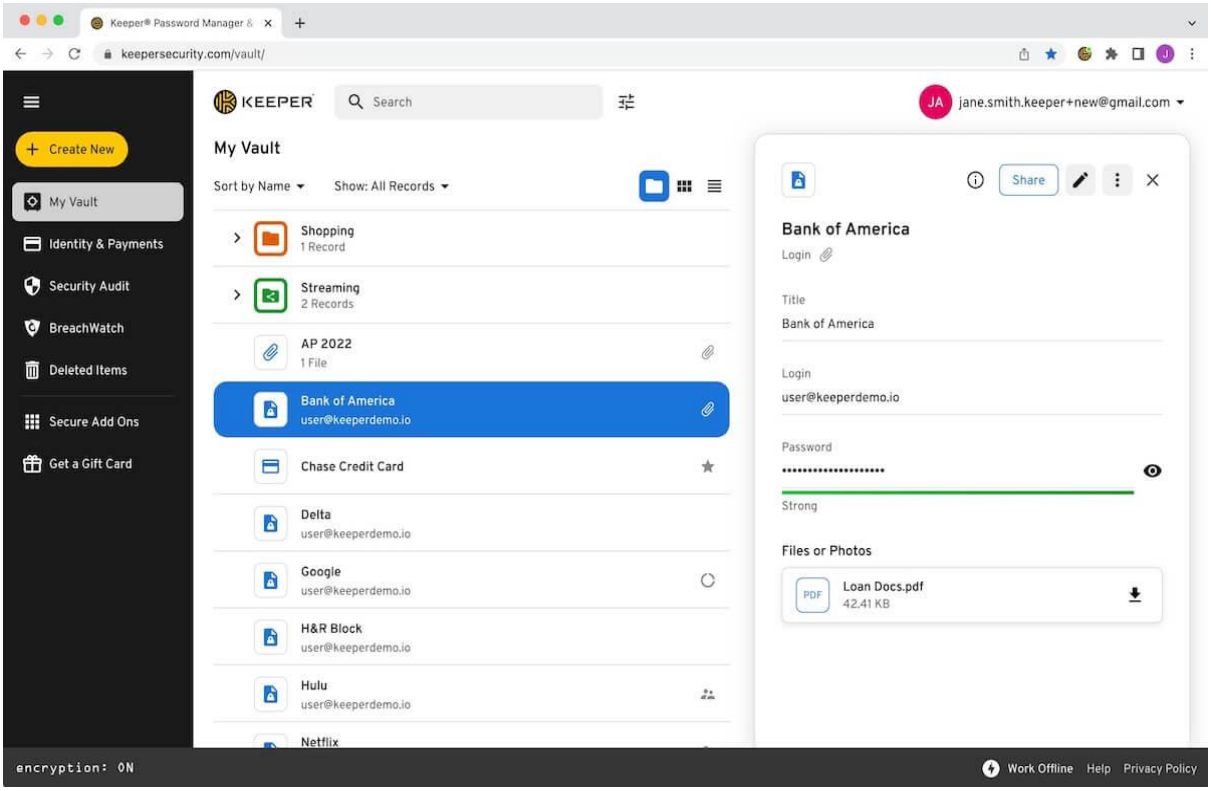


Рисунок 2.9 – Менеджер Keeper

Keeper — це менеджер паролів, який також зберігає іншу інформацію, як-от конфіденційні файли або критичну інформацію компаній, установ тощо. Він добре підходить для особистого користування, сімей або підприємств.

Найкращі функції Keeper:

– автоматизація ротації паролів, щоб ще більше знизити ризик;

– виконує сканування темної мережі, щоб дізнатися, чи ваш пароль було зламано.

Обмеження Keeper:

– функція автозаповнення не завжди працює ідеально.

10 LastPass

Програма яка була заснована чотирьма програмістами у 2008 році, пізніше була викуплена іншою компанією за 115 мільйонів доларів та пізніше її відокремили в окремий бізнес десь у 2015 році. Заснована була у Бостоні штат Массачусетс, у Сролучених Штатах Америки.

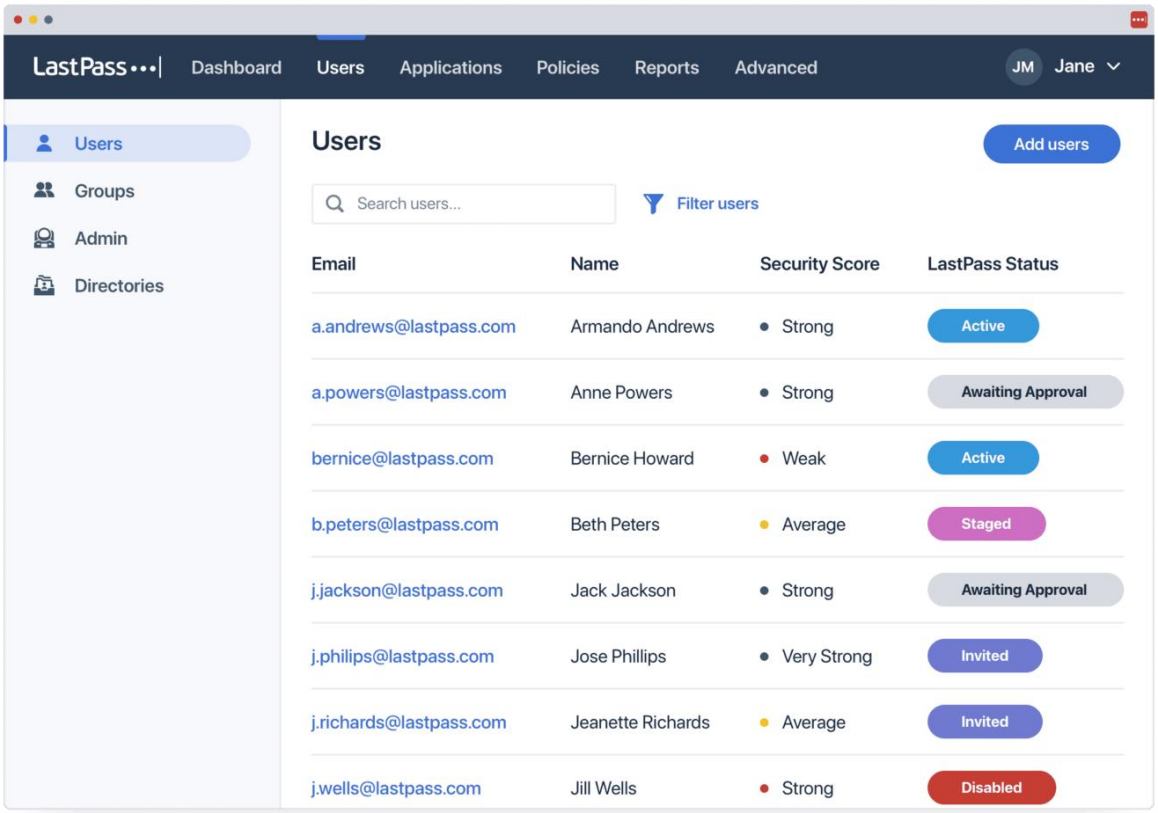


Рисунок 2.10 – Менеджер LastPass

Цей менеджер паролів зберігає необмежену кількість паролів і може генерувати паролі. Він також автоматично заповнює форми та дозволяє безпечно ділитися своїми паролями з іншими, проста у користуванні інформаційна панель адміністратора допоможе бути в курсі безпеки паролів родини чи компанії.

Найкращі функції LastPass:

– легкий доступ до паролів незалежно від того, перебуває користувач в мережі чи офлайн;

– зберігає всілякі цифрові записи, як-от ліцензії на програмне забезпечення та інформацію про Wi-Fi;

– захист даних за допомогою багатофакторної автентифікації в пакетах Premium і Business.

2.4 Переваги та недоліки менеджерів паролів

Сьогодні багато хто має кілька акаунтів у соціальних мережах або на веб-сайтах онлайн-банкінгу. Кожен обліковий запис потребує унікального імені користувача та пароля, і кожному користувачу важко запам’ятати ці десятки облікових даних для входу і тут з’являється менеджер паролів. Цей спрограмований інструмент дозволяє безпечно зберігати паролі в зашифрованому сховищі на комп’ютері локально або в хмарі, що забезпечує зручність і спокій.

Однак, як і інші технологічні рішення, використання менеджера паролів має свої переваги та недоліки.

Переваги менеджера паролів:

− згенерують складний пароль – менеджери паролів можуть автоматично генерувати складні паролі для кожного облікового запису. Таким чином, не потрібно запам’ятовувати паролі, крім головного. Можна використовувати функцію створення пароля, щоб створювати неймовірно надійні та унікальні паролі. Крім того, також можна налаштувати створення пароля, встановивши певну довжину символів і рівень читабельності;

− легкий доступ до облікових записів – менеджери паролів надзвичайно спрощують доступ до всіх облікових записів. Оскільки тепер не потрібно запам’ятовувати всі паролі від своїх облікових записів. Крім того, він також може автоматично заповнювати інформацію для входу в обліковий запис будь-яких веб-сайтів і програм, до яких користувач хоче мати доступ. Таким чином він може швидко та зручно отримати доступ до будь-якого свого облікового запису в менеджері паролів;

− працює на кількох пристроях – менеджери паролів працюють на кількох пристроях, таких як комп’ютери, ноутбуки, смартфони чи планшети, тому можна легко отримати доступ до всіх своїх облікових записів на цих пристроях. Таким чином, користувачу більше не доведеться турбуватися про доступ до паролів адже вони завжди під рукою, навіть коли він десь в дорозі.

− розширені функції безпеки – деякі менеджери паролів мають додаткові функції захисту для користувачів, наприклад двофакторну автентифікацію (2FA) і функцію безпечного обміну паролями для спільних облікових записів. Крім того, надійні менеджери паролів (наприклад, Chrome Password Manager) пропонують розширені протоколи шифрування, щоб захистити від хакерів, таким чином, користувачі менеджера паролів мають набагато більший захист свого паролю, ніж люди без менеджера паролів.

− необхідно запам’ятати тільки один пароль – основна перевага використання менеджерів паролів полягає в тому, що потрібно запам’ятати лише один головний пароль.

Оскільки всі мають десятки облікових записів в інтернеті, неможливо запам’ятати кілька паролів, якщо вони не однакові.

Менеджери паролів мають потенційні недоліки, залежно від програмного забезпечення.

Ось деякі недоліки:

− єдина точка відмови – найбільшим недоліком менеджерів паролів є те, що всі паролі захищені одним надійним паролем, що може призвести до одноточкової помилки. Наприклад, якщо зловмисник зламав наш головний пароль, він може отримати доступ до нашого сховища паролів і переглянути всі наші облікові записи та отримати доступ до них. Однак це буде неможливо, якщо уввімкнено двофакторну автентифікацію (2FA);

− захист паролем – менеджери паролів чудово захищають паролі, але вони не запобігають іншим атакам, таким як фішингові електронні листи, зловмисне програмне забезпечення, кейлоггери тощо, таким чином, під час перегляду веб-сторінок важливо користуватися інтернетом безпечно. Не натискати, не відкривати та не завантажувати жодних підозрілих посилань чи файлів;

− 2FA не завжди потрібно, деякі менеджери паролів не реалізують 2FA, що додає додатковий рівень безпеки. Це може призвести до багатьох ризиків для

людей, які використовують менеджери паролів, але не знають, що автентифікація 2FA забезпечує більшу безпеку та захист облікового запису;

− процес налаштування – під час першого використання менеджера паролів потрібен процес налаштування. У результаті потрібно буде імпортувати всі паролі, які користувач хоче зберегти, і встановити менеджер паролів на кожному пристрої, який людина хоче використовувати;

− все ще вимагає ручного введення – хоча менеджер паролів керує нашими паролями, він все одно потребує ручного введення від користувача. Зрештою, для доступу до менеджера паролів потрібно запам’ятати головний пароль. Також не забувати використовувати менеджер паролів для всіх облікових записів. Якщо цього не зробити, менеджер паролів не зможе допомогти.

Менеджер паролів пропонує кілька надійних заходів безпеки, але важливо розуміти, що жодна система чи програма не може гарантувати 100% безпеки. Як і будь-яка інша технологія, менеджери паролів схильні до потенційних вразливостей та ризиків, коли справа доходить до безпеки, сховище для паролів має бути головним пріоритетом для того щоб не заощаджувати кілька доларів на місяць, а витратити їх на свою безпеку. Це особливо стосується безкоштовних менеджерів паролів, яким часто не вистачає необхідних функцій безпеки для ефективного захисту облікових даних у будь-який час. Та важливо запам’ятати що ніколи не потрібно економити на своїй безпеці, адже зекономивши можна призвести потім до того що втратиться ще більше ніж можна було заплатити за це.

2.5 Висновок до розділу

Друга половина роботи стосувалася облікових записів та їх захисту. Облікові записи користувачів є ключовим елементом контролю доступу до системних ресурсів, оскільки вони дозволяють ідентифікувати користувачів і надавати відповідні права доступу. Проаналізовано існуючі заходи захисту паролями, включаючи використання надійних унікальних паролів і використання багатофакторної автентифікації, як-от ключі безпеки, одноразові паролі та біометрія. Особливу увагу приділено менеджерам паролів, які дозволяють користувачам безпечно зберігати та керувати паролями. Розглянули плюси та мінуси використання менеджера паролів. Перевагою яких є зручність, можливість генерувати складні паролі та автоматично заповнювати реєстраційні форми значно підвищує безпеку користувачів. Недоліком є те, що ви повинні довіряти своєму менеджеру паролів, і безпека може бути скомпрометована, якщо сам менеджер буде зламано. Також розглядаються методи автентифікації та авторизації для підтвердження особистості користувача та визначення рівня доступу до системи. Важливість захисту вашого облікового запису підкреслюється необхідністю дотримання найкращих практик, таких як використання надійних паролів, обмеження привілеїв і моніторинг підозрілої активності. Висновок цього розділу полягає в тому, що забезпечення кібербезпеки організацій і користувачів в умовах зростання кіберзагроз вимагає комплексного підходу до управління обліковими записами та використання сучасних технологій захисту.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗБЕЧЕННЯ

3.1 Потреба у розробці

У теперішньому світі інформаційних технологій безпека облікових записів і особистих даних є головним пріоритетом для користувачів і організацій.

Однією з найпоширеніших загроз є фішинг, спрямований на викрадення особистих даних, таких як паролі та іншої конфіденційної інформації.

Потреба у розробці мого програмного забезпечення зародилася на етапі огляду менеджерів паролів інших компаній та розробників. Якщо приглянутися до них усіх, то кожен має якісь переваги та недоліки, якимось притаманні кращі та доступніші функції, десь потрібно заплатити аби підвищити свій рівень безпеки. Зібравши до купи всю інформацію, було вирішено створити свій менеджер паролів для користувачів, який мав би як і прості функції, притаманні іншим менеджерам паролів, так і покращені функції, які давали б змогу користувачам без доплат підвищувати свій рівень безпеки та можливість захистити себе від фішингових атак кіберзлочинців.

Традиційні прості паролі не можуть забезпечити достатній рівень безпеки, а більш складніші паролі звичайні користувачі навіть не намагаються створити, чим наражають себе на небезпеку крадіжки та використання інформації в різних незаконних цілях. На виручку приходить менеджер паролів, який буде зберігати всі паролі в зашифрованому вигляді, що неабияк сприяє покращенню рівня захисту користувачів.

Для показу ефективності мого менеджера паролів над звичайними проведемо порівняння структурних схем та проведемо оцінку ефективності зі звичайними менеджерами. Це ми будемо робити для того щоб краще розуміти різницю між звичайними менеджерами паролів, та менеджером що було створено на основі експерименту з іншими програмами. Це дасть нам побачити усі переваги та недоліки як мого програмного забезпечення так і менеджерами інших компаній.

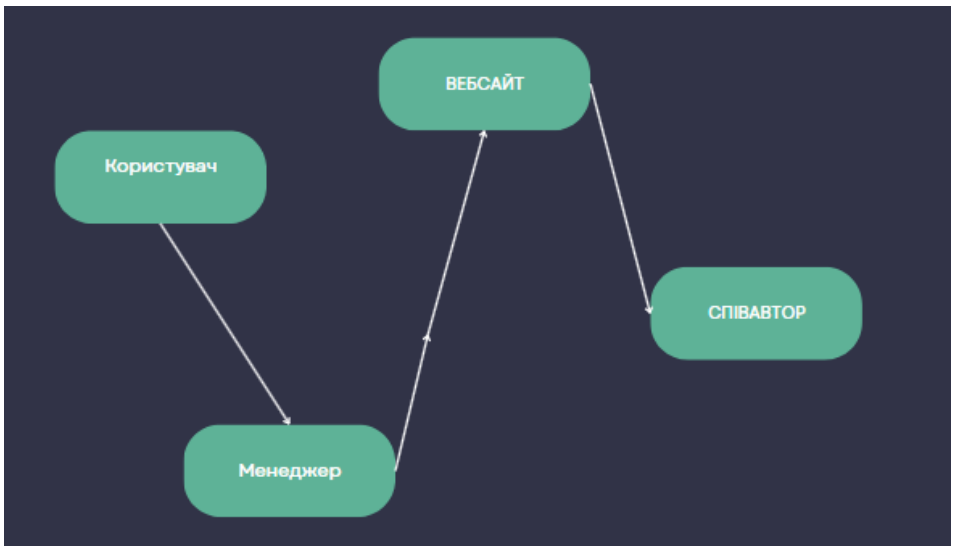


Рисунок 3.1 – Структурна схема використання менеджера паролів

Тут ми можемо бачити, як на прикладі працює звичайний менеджер паролів, деякі з них мають функцію, яка дає можливість ділитись паролями разом зі співавтором. Юзер просить згоду менеджера паролів для спільного використання даних разом із співавтором, після чого програма пересилає облікові данні коли йому це потрібно. Розглянемо структурну схему роботи мого менеджера паролів

Рисунок 3.2 – Структурна схема MYPmanager

На структурній схемі менеджера зображено його функції та операції, які повинні реалізовуватись, розглянемо їх детальніше.

Операції:

– операція додавання, тут користувач може додати пароль, який він хоче зберегти, та прив'язати його до певного веб – сервісу, це дає можливість не робити безлад серед паролів, які він хоче зберігати, адже мій менеджер може зберігати величезну кількість паролів чим відрізняється від інших;

– функція пошуку, дає можливість швидко знайти пароль, який на даний момент потрібний користувачу, і щоб не гортати величезний перелік збережених паролів він може просто ввести назву сервісу, від якого йому потрібен пароль, і якщо у користувача збережено багато паролів від одного сервісу, то є можливість пошуку по ключовим словам;

– редагування, дає змогу змінювати пароль при виявлені якихось аномалій з ним, або ж просто змінити пароль, придати йому вищий рівень безпеки, який зменшить можливість його зламу.

Легкість користування – легкість користування моїм менеджером паролів полягає в тому що, у ньому зрозумілий інтерфейс, все легко, просто та доступно. Навіть недосвідчений користувач, який не дуже знайомий з комп'ютером, з легкістю зможе розібратися в ньому та вільно користуватися програмним забезпеченням, адже інші менеджери паролів, які були наведені до прикладу у пункті 2.3, мають дуже за мудрений інтерфейс, який ускладнює роботу з програмою та відштовхує користувачів від користування, наражаючи їх на небезпеку, а саме – на фішингові атаки, які можуть призвести до дуже великих як фінансових, так і особистих втрат. Простий інтерфейс завжди був і буде найкращим для таких програм навіть з дизайнерської точки зору, також у ньому виражається з усіх переваг портативність, це завжди було великим плюсом для таких програм, адже захист паролів потрібен нам не тільки на ноутбуках чи комп'ютерах, телефони – це така річ, де люди також зберігають велику кількість

особистої інформації, яка несе цінність для них та є ціллю для кіберзлочинців, тому є можливість користуватися ним як на Android, так і на IOS.

Захист – це додаток, що сам по собі має велику надійність в порівнянні з іншими менеджерами паролів, що зумовлено тим, що всі паролі зберігаються не на сервері, а на персональному комп'ютері, а співавтор немає ніякого доступу до них і користувач може не хвилюватися, що його данні з годом викрадуть і вони попадуть в недобрі руки. Також в сам менеджер паролів встановлена система двох етапного шифрування, яка шифрує паролі за одним алгоритмом перший раз і другий раз вже використовує зовсім інший алгоритм, що надає неабияку перевагу серед звичайних менеджерів паролів. Сам менеджер паролів немає ніякого виходу в інтернет, що надає високу конфіденційність і прибирає загрозу витоку інформації в глобальну мережу. Хоч самі паролі зберігаються на персональному комп'ютері користувача вони надійно захищені, так як зберігаються в зашифрованому вигляді і розшифрувати їх сплине дуже багато часу. Але навіть якщо їх розшифрують, то в цілях захисту інформації та боротьби з кіберзлочинністю вони будуть негайно видалені з персонального комп'ютера користувача. Так звичайно користувач втратить свої паролі, але зловмисники їх не зможуть отримати в ніякому разі, що підтверджує неможливість викрадення інформації. Проте, навіть як що таке і станеться, всі втрачені данні є можливість повернути в самому менеджері паролів. Щоб це зробити потрібно підтвердити свою особу за допомогою двох факторної автентифікації, яка наддасть доступ до процесу відновлення всіх паролів навіть після їх видалення, щоправда це займе певний час, що тільки підтверджує надійність мого менеджера паролів.

3.2 Демонстрація роботи менеджера паролів

При запуску програмного забезпечення нас зустрічає головне меню нашого менеджера паролів, де нам потрібно ввести головний пароль, який дасть нам доступ до всіх інших збережених нами паролів, та функцій програми, якщо у

користувача стоїть 2FA, його після вводу паролю перекине в меню, де він повинен буде ввести шестизначний код, який прийде йому на пошту або номер телефону, пароль зазначений для входу повинен мати щонайменше 8 символів.

Рисунок 3.3 – Головне меню

Після входу нас зустрічає меню, де користувач може працювати зі своїми паролями та обліковими даними. Тут він може вибрати опцію, яка саме йому потрібна, а саме додати видалити редагувати пароль. Як ми бачимо тут продемонстрована функція додавання паролю, юзер вводить ім’я веб сервісу, до якого він хоче прив’язати пароль, далі він має ввести ім’я та пароль для збереження, після чого, натискаючи на кнопку знизу, програма повідомляє нас про успішне виконання операції.

Воно було розроблене простим без лишніх деталей, аби навіть недосвідчений користувач зміг розібратися у його функціоналі.

Адже деякі менеджери мають дуже заповнене меню, в якому є купа різних функцій, лишніх деталей які можуть злякати користувача та відвернути його увагу від використання менеджеру паролів.

Я врахував цей нюанс, та ми можемо побачити результат де видно що все просто, легко та зручно, що є одним із головних факторів гарно розробленої програми. Також при необхідності користувач може змінити тему на чорний колір.

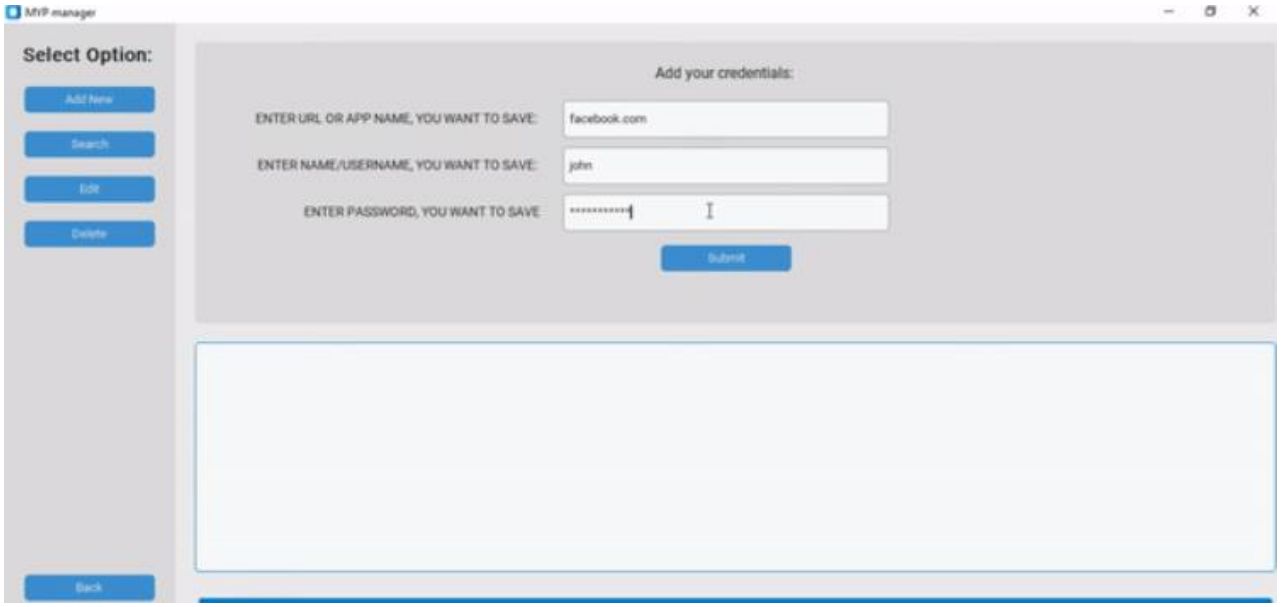


Рисунок 3.4 – Меню роботи з паролями

Функція пошуку працює за принципом, користувач вводить URL адресу або назву веб сервісу, від якого йому потрібно переглянути паролі, та знизу у списку виникає список, де зазначений потрібний веб сервіс, юзернейм та пароль.

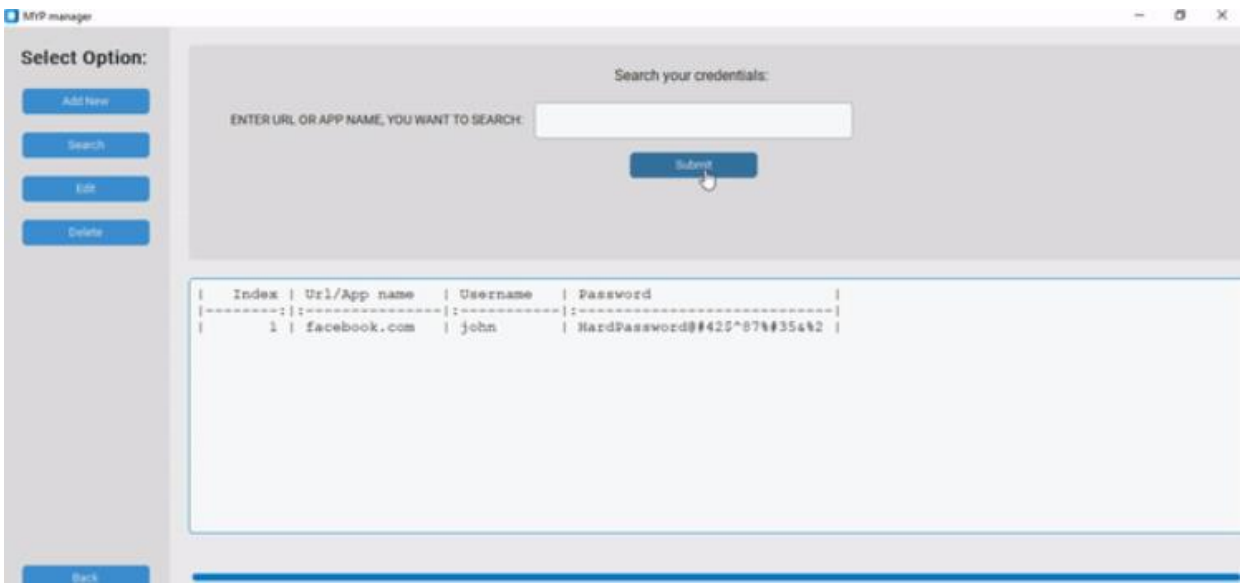


Рисунок 3.5 – Реалізація функції пошуку

Функція редагування призначена для того, щоб користувач міг в любий момент записати новий пароль, якщо він змінив його попередньо до якогось веб сервісу, аби не виникало проблеми коли менеджер паролю видає старий пароль від сервісу, коли користувач має новий. Розглянемо на прикладі програми steam, після того як користувач змінив пароль від свого аккаунту та хоче записати новий, щоб зберегти він вводить ім'я програми, йому видає дані від цього веб сервісу та далі він може записати як новий логін, так і пароль, якщо їх було змінено.

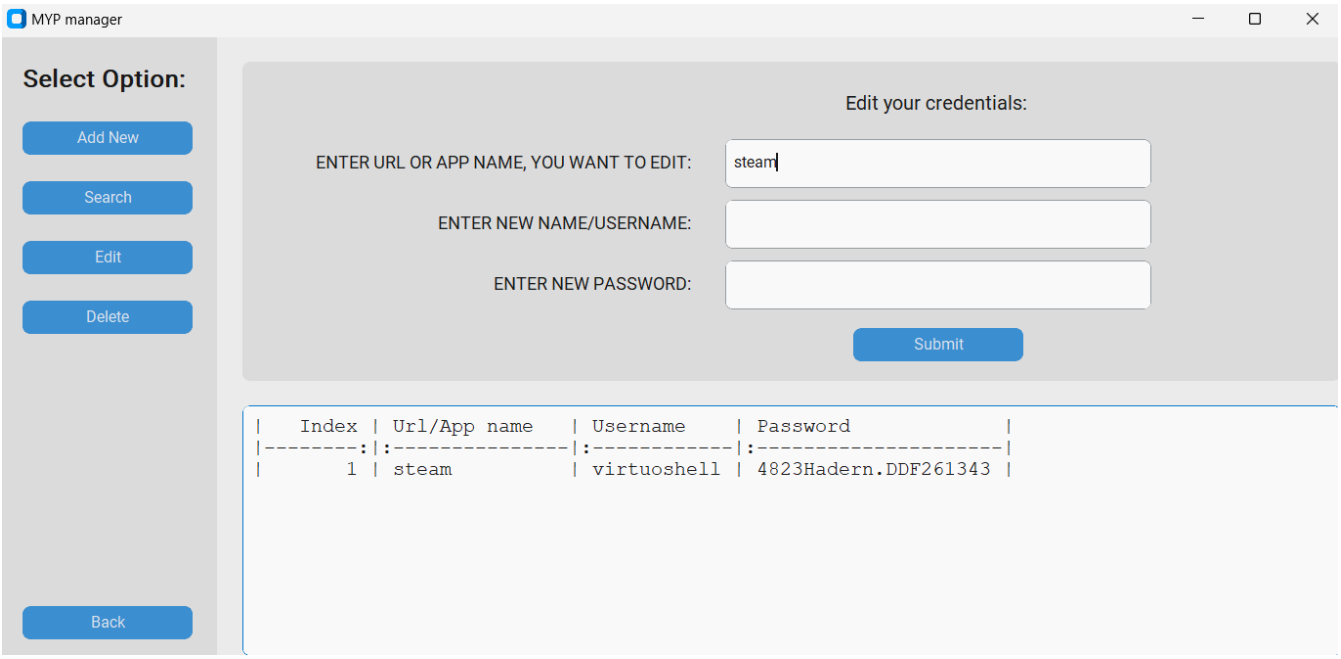


Рисунок 3.6 – Функція редагування

Після того як користувач все змінив, він може перейти в меню пошуку ввести нові дані та менеджер паролів покаже йому вже відредаговані. Як ми можемо побачити тепер нам показує вже нові змінені дані.

Тепер розглянемо на прикладі як працює функція видалення. Вона реалізовувалася для того, щоб користувач в любий момент зміг видалити вже неактуальні для нього дані, щоб не виникало безладу серед всієї купи інформації, яку менеджер паролів може зберігати. Адже порядок та організованість серед паролів та інформації – один із ключових аспектів обізнаності роботи з

інформацією. Як ми бачимо користувачу потрібно ввести ім’я сервісу, від якого йому потрібно видалити неактуальні для нього дані.

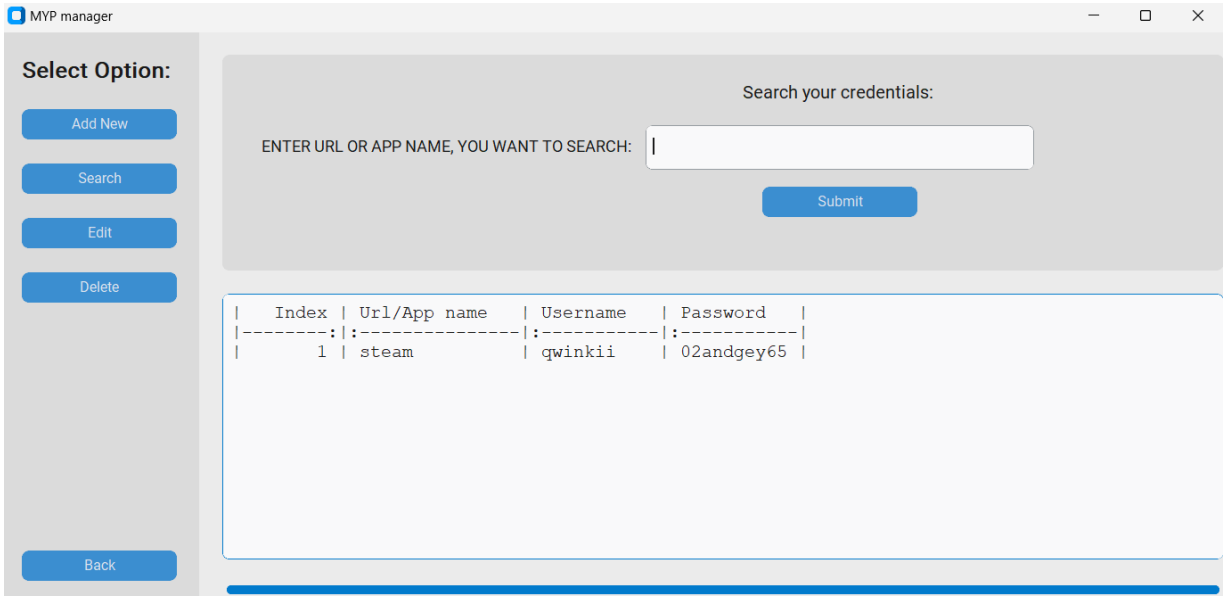


Рисунок 3.7 – Результат роботи функції редагування

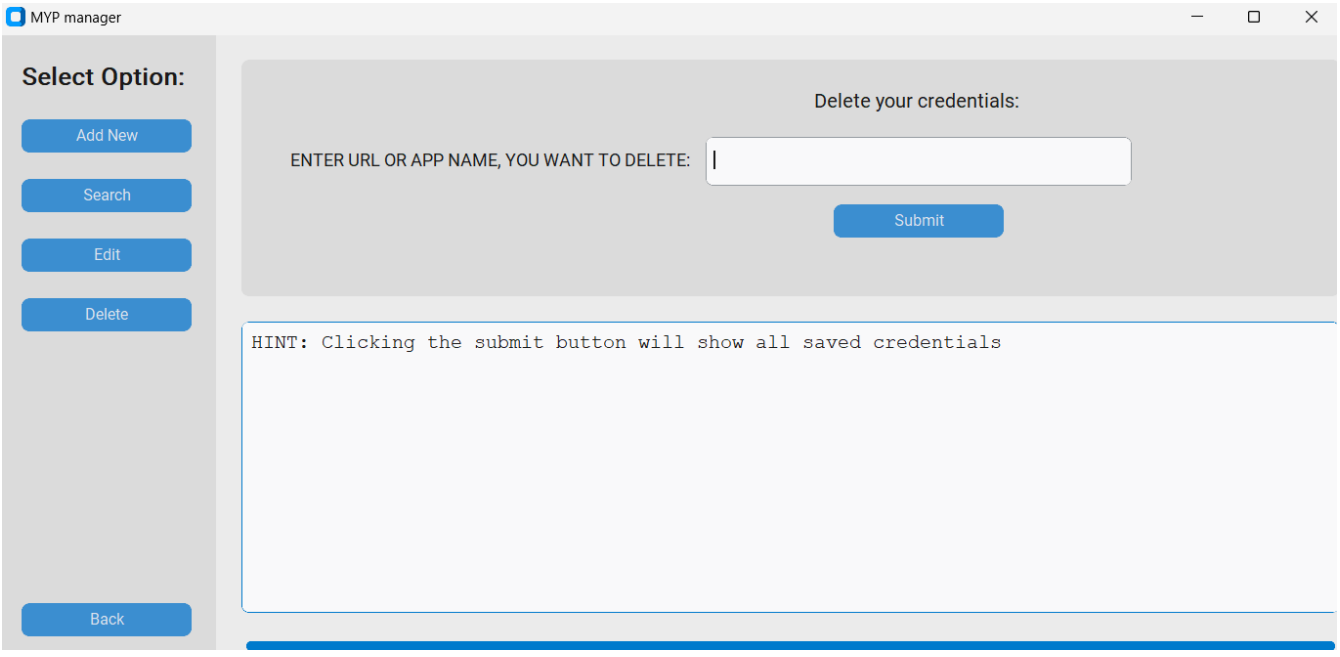


Рисунок 3.8 – Функція видалення

Тут все просто та без лишніх нюансів, користувач просто вводить ім’я сервісу та натискає на кнопку чим вказує програмі приступити до виконання функції видалення, після потрібно підтвердити операцію в іншому вікні додатку.

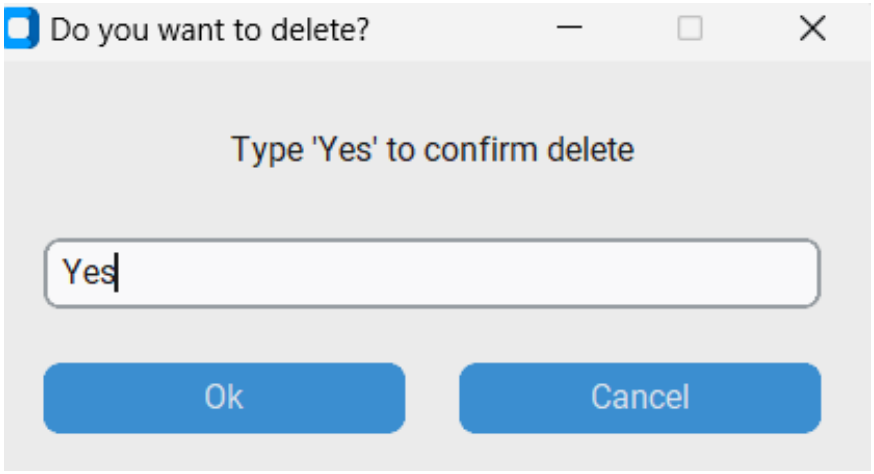


Рисунок 3.9 – Вікно підтвердження

Після того, як користувач вводить сервіс з’являється вікно, де у нього просить ввести слово “Yes” для того, щоб підтвердити видалення.

Тепер програма повідомляє нас про успішне виконання операції, всі ці функції було організовано для того, щоб зробити менеджер паролів не тільки простим у використанні, але і зручним. Кожна з цих функцій відіграє важливу роль, та є корисною по своєму, вони і роблять цей менеджер паролів особливим, чимось вирізняє його серед інших менеджерів паролів представлених вище.

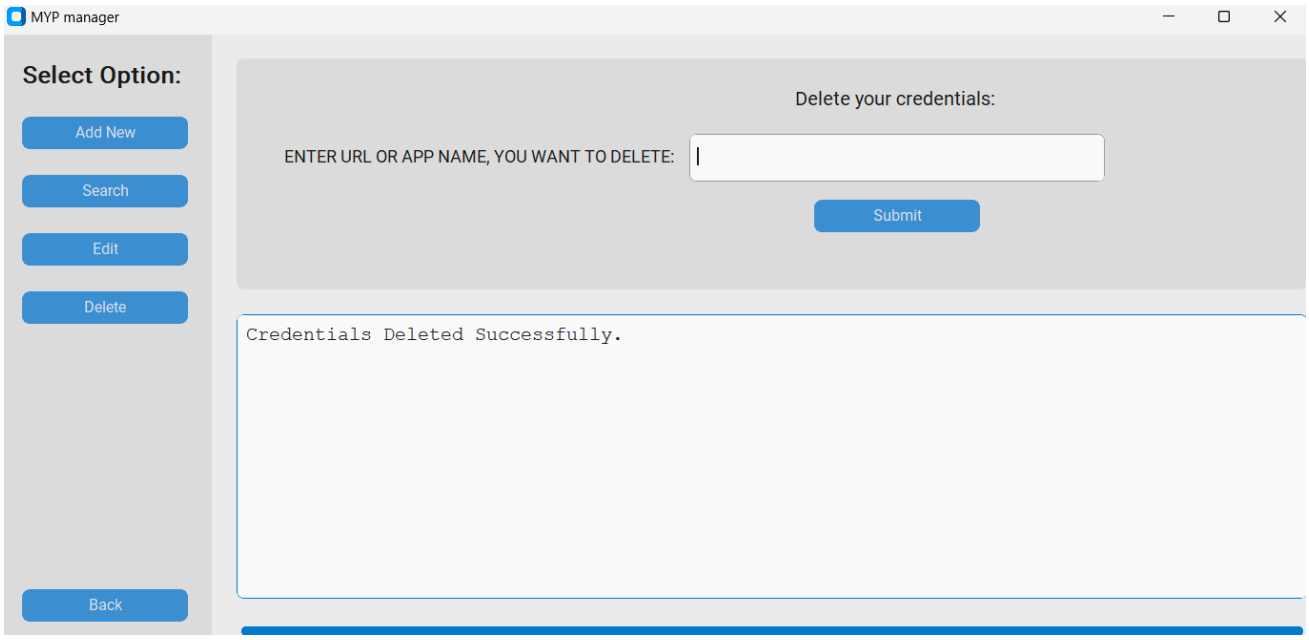


Рисунок 3.10 Успішне виконання операції видалення

Як ми можемо побачити функція видалення працює добре та після того як користувач вводить назву сервісу менеджер паролів не показує ніяких даних, пов’язаних саме з цим сервісом, для цього ми перейшли знову в меню пошуку та спробували знайти данні пов’язані з нашим веб сервісом steam, та як зазначалося і видно на наступному рисунку менеджер паролів нічого не знайшов.

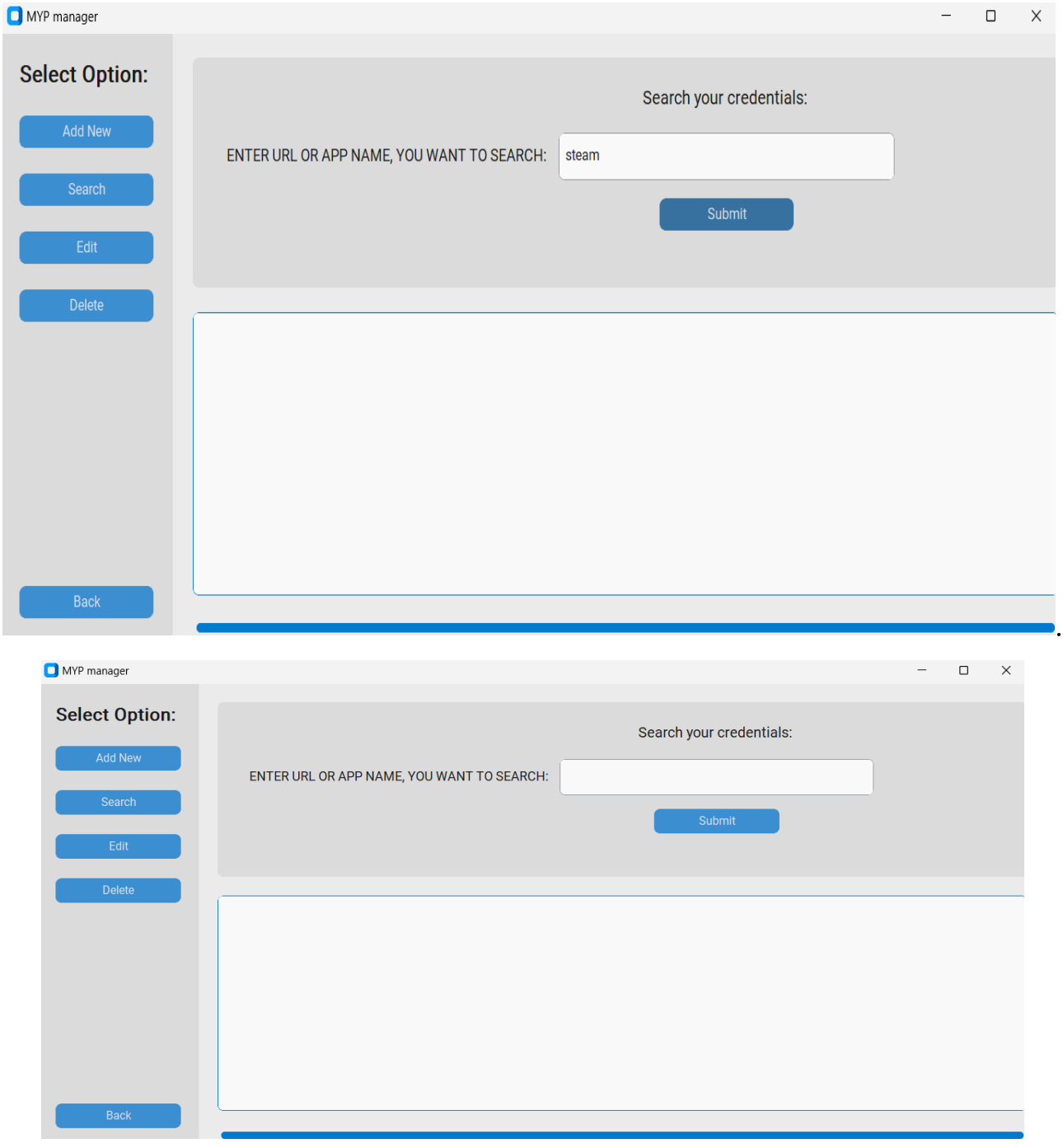


Рисунок 3.11 – Результат роботи функції видалення

3.3 Оцінка ефективності

Розглянемо наскільки менеджер паролів MYPmanager ефективніший в порівнянні з іншими представленими менеджерами паролів. Для оцінки ефективності я провів атаки на паролі в цих менеджерах паролів (атака проводилась при ситуації, коли у хакерів був доступ до паролів але тільки у зашифрованому вигляді) та, зібравши результати експерименту, представив їх у таблиці. Всі атаки проводились на паролі одного і того самого користувача, але у різних менеджерах паролів.

Таблиця 3.1 – Результат атак на менеджери паролів

Назва Менеджера Паролів	Кількість Проведених Атак	Зламано Паролів	Стійкі Паролі	Відсоток Зламаних Паролів
Bitwarden	100	15	85	15%
KeePass	100	12	88	12%
Dashlane	100	13	87	13%
Keeper	100	10	90	10%
LastPass	100	7	95	7%
MYPmanager	100	5	98	5%

Як ми бачимо мій менеджер паролів витримав проведену кількість атак і зміг захистити більше паролів в порівнянні з іншими. Цим і можна виділити його серед інших як дуже ефективне програмне забезпечення. Зображення атаки на нього можна переглянути на рисунку 1.32.

Нижче ми можемо розглянути скріншоти того як проводилася атака на мій менеджер паролів, та те що паролі були видобуті фішингом у зашифрованому вигляді та потім брутфорсом перебиралися.

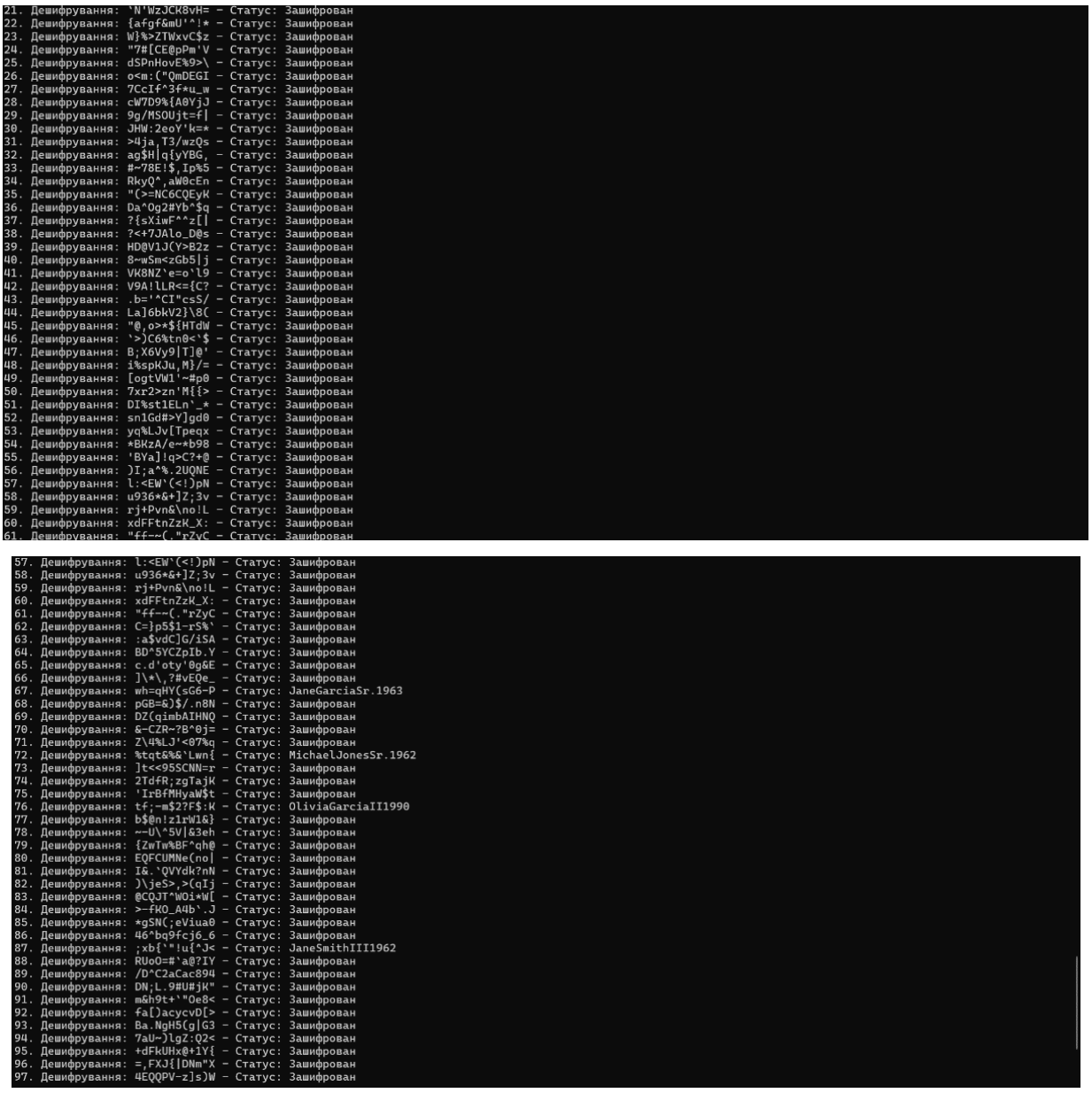


Рисунок 3.12 – Атака на менеджер паролів MYPmanager

І як ми можемо побачити всього вийшло взламати 5 паролів і всі вони не рекомендуються до введення адже там вказуються особисті данні такі як рік народження ім’я та фамілія.

3.4 Висновки до розділу

У третьому розділі цього дослідження описано процес розробки та впровадження програмного забезпечення, яке захищає облікові записи від

фішингу на основі менеджерів паролів. Основна мета полягала в тому, щоб створити інструмент, який надійно захищає дані користувача, одночасно забезпечуючи простоту використання та додаткові функції безпеки без додаткових витрат для користувачів.

У цьому розділі детально описані етапи розробки програмного забезпечення, починаючи від аналізу існуючих рішень на ринку та виявлення їх недоліків і закінчуючи описом особливостей розробленого менеджера паролів. Було виділено основні аспекти, які відрізняють створений менеджер від аналогів, зокрема його покращений захист та здатність запобігати фішинговим атакам.

Процес розробки включає створення інтерфейсу користувача, налаштування методів захисту зашифрованим паролем та інтеграцію функції багатофакторної автентифікації.

Особливу увагу було приділено простоті використання, що є ключовим фактором забезпечення високого рівня безпеки, оскільки для ефективності інструменту потрібне активне використання користувачем.

Основною ідеєю для створення мого програмного забезпечення а саме менеджера паролів MYPmanager послужив проведений експеремент проведений з усіма менеджерами паролів, переглянувши їх було вирішено створити менеджер паролів який буде відрізнятися від них усіх але і в той же момент буде чимось схожим на них.

Кожен з них має якісь переваги та недоліки, в якомусь більша частина функціоналу є платною ще не може бути доступним для усіх користувачів, десь інтерфейс схожий на безлад та незрозумілий для простих користувачів, та ще дуже багато іншого.

Тому зібравши всю інформацію до купи зваживши все, створено менеджер паролів особливий в усьому та водночас дуже схожим на інші менеджери паролів.

Загалом результат впровадження програмного забезпечення полягає в тому, що створений менеджер паролів задовільно відповідає встановленим вимогам і значно підвищує рівень безпеки користувачів, захищаючи їх від фішингових атак та інших загроз, пов’язаних із крадіжкою облікових даних.

ВИСНОВКИ

Усі зусилля були зосереджені на справжньому питанні захисту облікових записів від фішингу, що надзвичайно важливо в сучасному цифровому світі. У цій дипломній роботі розглядаються основні види фішингу, способи захисту від фішингу, існуючі інструменти захисту паролем, а також плюси та мінуси менеджерів паролів. На основі аналізу було розроблено та впроваджено антифішингове програмне забезпечення на основі менеджера паролів.

Перший розділ цього дослідження стосувався аналізу фішингу та його різновидів. Фішинг вважається однією з найпоширеніших і найефективніших форм кіберзлочинності завдяки своїй здатності швидко пристосовуватися до нових ситуацій і змінювати методи.

Я зміг дізнатися про різні типи фішингу, такі як фішинг, китобійний фішинг, фармінг і SMS-фішинг, і детально зрозуміти, як вони працюють.

Важливим аспектом цього дослідження було вивчення методів боротьби з фішингом, таких як використання унікальних надійних паролів, обережне поводження з електронною поштою, перевірка безпеки веб-сайту та використання програмного забезпечення для захисту від фішингу. Розділ завершується підкресленням необхідності комплексного підходу до боротьби з фішингом, який включає технічні інструменти, навчальні програми та дотримання вимог безпеки в Інтернеті.

Друга частина цієї роботи стосується облікових записів та їх захисту. Були розглянуті заходи захисту паролями, включаючи використання надійних унікальних паролів і використання багатофакторної автентифікації, включаючи ключі безпеки, одноразові паролі та біометричні дані. Особливу увагу приділено менеджерам паролів, які дозволяють користувачам безпечно зберігати та керувати паролями. Мій аналіз показує, що менеджери паролів пропонують значні переваги, включаючи простоту використання, можливість генерувати складні паролі та автоматично заповнювати форми входу, а також покращити безпеку

користувачів. Однак було виявлено деякі недоліки, зокрема необхідність довіряти диспетчеру паролів і ризик порушення безпеки, якщо сам менеджер зазнає атаки хакера. Важливість захисту вашого облікового запису підкреслюється такими передовими методами: використання надійних паролів, обмеження привілеїв та контроль підозрілої активності.

Розділ 3 описує процес розробки та впровадження програмного забезпечення, яке захищає облікові записи на основі менеджера паролів від фішингу. Основна мета полягала в тому, щоб створити інструмент, який надійно захищає дані користувача, одночасно забезпечуючи простоту використання та додаткові функції безпеки. Процес розробки включає створення інтерфейсу користувача, налаштування методів захисту зашифрованим паролем та інтеграцію функції багатофакторної автентифікації. Під час розробки було зосереджено на простоті використання. Це важливий елемент для забезпечення високого рівня безпеки. Оскільки для ефективності цього інструменту необхідне активне використання користувачем, створений із впровадженням програмного забезпечення менеджер паролів значно підвищить рівень безпеки користувача, відповідаючи встановленим вимогам, і Ви зможете захистити своїх користувачів від фішингових атак і інших загроз, пов’язаних із захищеними обліковими даними, крадіжками.

Таким чином, це дослідження робить висновок, що системи захисту облікових записів на основі менеджерів паролів є ефективним засобом захисту від фішингу. Проведені дослідження та впровадження програмних продуктів підтвердили потенціал подальшого впровадження та вдосконалення цих технологій для забезпечення кібербезпеки в сучасних умовах. Програмне забезпечення, розроблене, пропонує високий рівень захисту завдяки сучасним процедурам шифрування та багатофакторній автентифікації, що робить його цінним інструментом у боротьбі з кіберзлочинністю.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Аркелоф Дж. Фішинг хто і як маніпулює вашим вибором. США.
2. ВАЖЛИВІСТЬ ВИКОРИСТАННЯ МЕНЕДЖЕРІВ ПАРОЛІВ У СУЧАСНОМУ СВІТІ - Наукові конференції. Наукові конференції. URL: http://www.konferenciaonline.org.ua/ua/article/id-535/ (дата звернення: 11.03.2024).
3. Всесвітній день паролів: 5 поширених помилок під час створення комбінації для входу. Malware Protection & Internet Security | ESET. URL: https://www.eset.com/ua/about/newsroom/press-releases/security-tips/vsemirnyy-den-paroley-5-rasprostranennykh-oshibok-pri-sozdanii-kombinatsii-dlya-vkhoda/ (дата звернення: 10.05.2024).
4. Економічна правда. Як надійно і безпечно зберігати паролі від сайтів. Економічна правда. URL: https://www.epravda.com.ua/publications/2021/08/14/676885/ (дата звернення: 23.04.2024).
5. Захист від фішингу. ESKA. URL: https://eska.global/blog/antifishing-kak-zashititsya-v-sovremennyh-realiyah (дата звернення: 15.04.2024).
6. Кібершахрайство: фішинг. вішинг. смішинг. бейтінг. Правовой дом "КОПИРАЙТ". URL: https://kopirait.com.ua/kibershahrajstvo-fishyng-vishyng-smishyng-bejting/ (дата звернення: 16.05.2024).
7. Менеджер паролів, що це таке і для яких цілей він потрібен - HackYourMom. HackYourMom. URL: https://hackyourmom.com/pryvatnist/menedzher-paroliv-shho-cze-take-i-dlya-yakyh-czilej-vin-potriben/ (дата звернення: 18.04.2024).
8. Навіщо потрібен менеджер паролів та як правильно його обрати? | CyberCalm. CyberCalm | Кіберзахист та кібербезпека простою мовою. URL: https://cybercalm.org/novyny/navishho-potriben-menedzher-paroliv-ta-yak-pravylno-jogo-obraty/ (дата звернення: 11.04.2024).

9. Рикова В. Для чого потрібен менеджер паролів і який обрати. ms.detector.media.
URL: https://ms.detector.media/kiberbezpeka/post/29917/2022-07-26-dlya-chogo-potriben-menedzher-paroliv-i-yakyy-obraty/ (дата звернення: 13.05.2024).

10. Учасники проектів Вікімедіа. Фішинг – вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Фішинг (дата звернення: 16.05.2024).

11. Фішинг та цільовий фішинг: поради по захисту. Домени – перевірка та реєстрація доменів в Україні | Imena.ua. URL: https://www.imena.ua/blog/phishing-and-target-phishing/ (дата звернення: 17.04.2024).

12. Фішинг – що це таке, суть, визначення, види та приклади фішингу. Termin.in.ua.URL: https://termin.in.ua/fishynh/

13. Хто я - Жодна система не є безпечною, 204 / режисер Б. о Дар. URL: https://www.sonypictures.com/

14. Чому варто використовувати менеджер паролів? 2024 рік. GizmoBase. URL: https://www.twinstrata.com/uk/why-you-should-use-a-password-manager/ (дата звернення: 18.05.2024).

15. Що таке Фішинг? Види фішингових атак і захист від них | EXBASE. EXBASE - create crypto wallet online | Cryptocurrency Wallet. URL: https://exbase.io/uk/wiki/fishing-i-zakhist-vid-nogo (дата звернення: 19.05.2024).

16. Який спосіб обміну паролями зі співробітниками є найбезпечнішим? - Klik Ukraine Support Support - IT сервіс провайдер. Klik Ukraine Support Support - IT сервіс провайдер. URL: https://www.kliksolutions.com.ua/great-info/yakyj-sposib-obminu-parolyamy-zi-spivrobitnykamy-ye-najbezpechnishym/ (дата звернення: 17.04.2024).

17. Як надійно захистити паролем файли та накопичувачі- Kingston Technology. Kingston Technology Company.

URL: https://www.kingston.com/ua/blog/data-security/securely-password-protect-files-and-drives (дата звернення: 15.05.2024).

18. Anderson R., Anderson R. J. Security engineering: a guide to building dependable distributed systems. Wiley, 2001. 640 p.

19. Ferguson N., Schneier B., Kohno T. Cryptography engineering: design principles and practical applications. Wiley & Sons, Incorporated, John, 2011. 384 p.

20. Schneier B. Applied cryptography: protocols, algorithms, and source code in C, 2nd edition. Wiley, 1995. 784 p.

21. Безпека паролів: як створити та зберігати надійні паролі. ClearVPN. URL: https://clearvpn.com/blog/ua/yak-stvoriuvaty-i-zberihaty-paroli/ (дата звернення: 23.04.2024).

22. Використання Google Chrome як парольного менеджера - Як?. Як?. URL: https://yak.dslua.org/articles/google-chrome-yak-parolnyi-menedzher/ (дата звернення: 17.05.2024).

23. ДСТУ ISO/IEC 27001:2015 інформаційні технології. методи захисту системи управління інформаційною безпекою. вимоги (ISO/IEC 27001:2013; cor 1:2014, IDT). БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910 (дата звернення: 29.04.2024).

24. ЕМА – асоціація ЄМА. Асоціація ЄМА. URL: https://www.ema.com.ua/ (дата звернення: 11.05.2024).

25. Запам’ятовування паролів і заповнення веб-форм в internet explorer 11 - підтримка від microsoft. Microsoft Support. URL: https://support.microsoft.com/uk-ua/windows/запам-ятовування-паролів-і-заповнення-веб-форм-в-internet-explorer-11-6883f6ce-0d1c-c2b9-e21e-705976d1c886 (дата звернення: 15.03.2024).

26. Захист П. Н. Міжнародна конференція "Захист права на інформацію в Україні" : зб. тез доп., Львів, 20-21 груд. 2007 р. Львів : [ЕПЛ], 2008. 56 с.

27. Лєнков С. В., Балабін В. В., Грищак О. М. Гарантування стійкості функціонування спеціального програмного забезпечення за допомогою методу

«паролів». Ukrainian information security research journal. 2008. Т. 10, № 3(39). URL: https://doi.org/10.18372/2410-7840.10.5495 (дата звернення: 14.05.2024).

28. Мехед Д. Б., Ткач Ю. М., Базилевич В. М. Дослідження технологій впливу та методів протидії фішингу. Ukrainian information security research journal. 2019. Т. 21, № 4. С. 246–251. URL: https://doi.org/10.18372/2410-7840.21.14338 (дата звернення: 17.05.2024).

29. Приклади фішингових листів | Binance Support. Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins. URL: https://www.binance.com/uk-UA/support/faq/приклади-фішингових-листів-360020817051 (дата звернення: 21.04.2024).

30. Танашкіна М. Д. Фішинг - як вид шахрайства в Інтернеті. Правникъ. 2018. № 2 (весна). С. 87–89.

31. Фішинг глосарій corefy. Corefy. URL: https://corefy.com/uk/glossary/phishing (дата звернення: 11.05.2024).

32. Хлистун В. В. Метод синтезу паролів підвищеної складності : thesis. 2016. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/5118 (дата звернення: 1.05.2024).

33. Cert-ua. cert.gov.ua.
URL: https://cert.gov.ua/recommendation/16904 (date of access: 1.04.2024).

34. IT-фахівці розповіли, навіщо потрібен менеджер паролів і як правильно його вибрати. Новини України - останні новини України сьогодні - УНІАН. URL: https://www.unian.ua/science/it-fahivci-rozpovili-navishcho-potriben-menedzher-paroliv-i-yak-pravilno-yogo-vibrati-novini-11052392.html (дата звернення: 22.04.2024).

35. LIAPP | The easiest and powerful mobile app security solution. LOCKINCOMPANY.
URL: https://liapp.lockincomp.com/?utm_term=owasp%20top%2010&utm_campaign=SEARCH_EN&utm_source=adwords&utm_medium=ppc&hsa_acc=2452270088&hsa_cam=19755849814&hsa_grp=163387924207&h

sa_ad=693473947629&hsa_src=g&hsa_tgt=kwd-353745812087&hsa_kw=owasp%20top%2010&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKCAjwmrqzBhAoEiwAXVpgoiHWmmwfvM8yEiRkPs3VzYiBxaqO56N1VmriBJ_Frx6_7iyV3u5v8BoCK14QAvD_BwE (date of access: 16.06.2024).

36. Micrsoft.URL: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf (date of access: 15.05.2024).

37. NISTSP800-63digital identity guidelines. URL: https://pages.nist.gov/800-63-3/ (date of access: 5.05.2024).

38. Protecting you against phishing. Google Online Security Blog. URL: https://security.googleblog.com/2017/05/protecting-you-against-phishing.html (date of access: 6.04.2024).

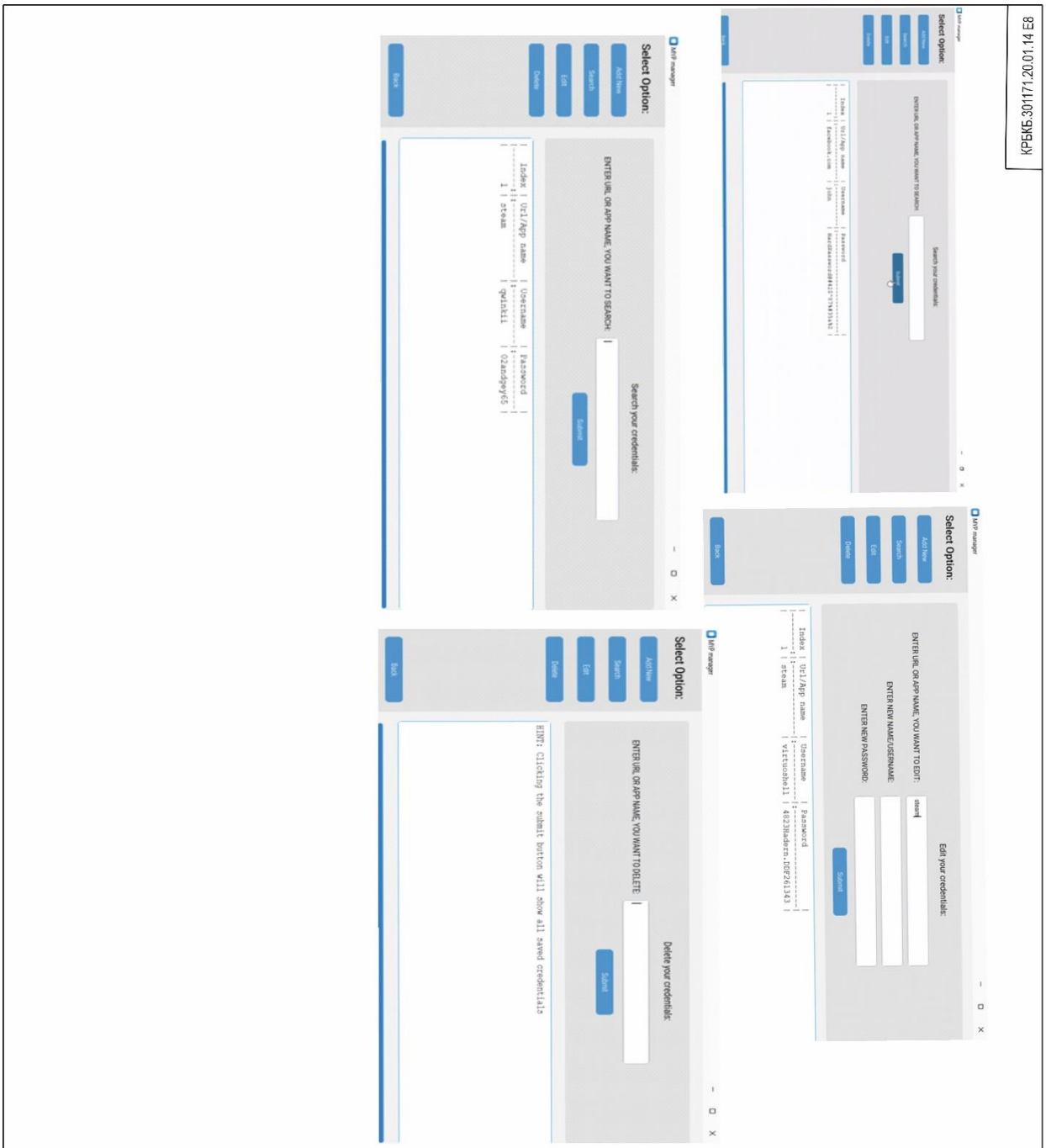
39. Rud A. Як створити надійний пароль для сервера, і чому це важливо? | блог hyperhost.ua. Український хостинг провайдер HyperHost. Купити хостинг для сайту. URL: https://hyperhost.ua/info/uk/yak-stvoriti-nadiinii-parol-dlya-servera-i-comu-ce-vazlivo?gad_source=1&gclid=CjwKCAjwmrqzBhAoEiwAXVpgos449jNTYGKJa1M78ep2q-0JqF-4dlNPcGRtNxyzhKwncX5KW3rIFhoCdWYQAvD_BwE (дата звернення: 19.04.2024).

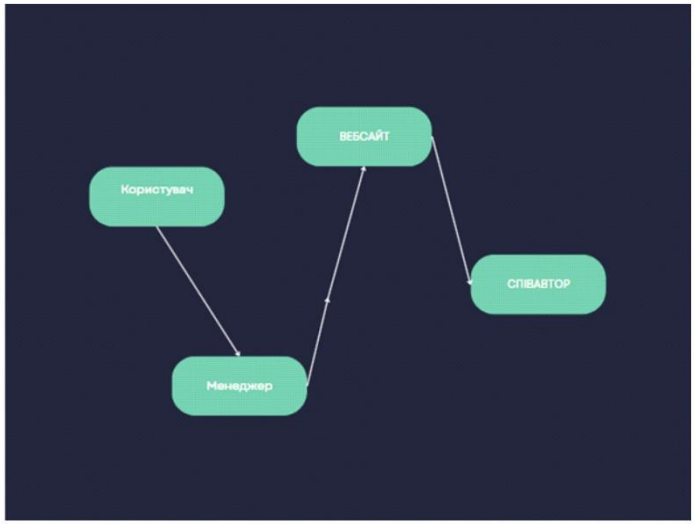
40. Zillya! - Правила незламного пароля. Zillya! Антивірус – український антивірус. URL: https://zillya.ua/index.php?q=pravila-nezlamnogo-parolya (дата звернення: 10.05.2024).

ДОДАТОК А

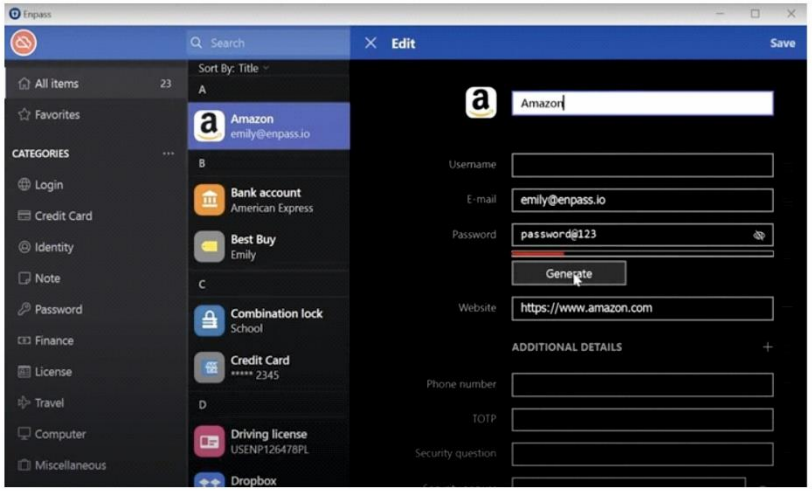
(Обов’язковий)

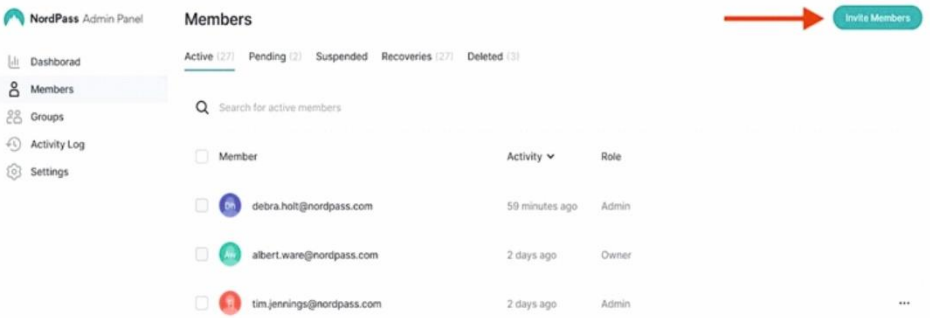
Копії графічної частини

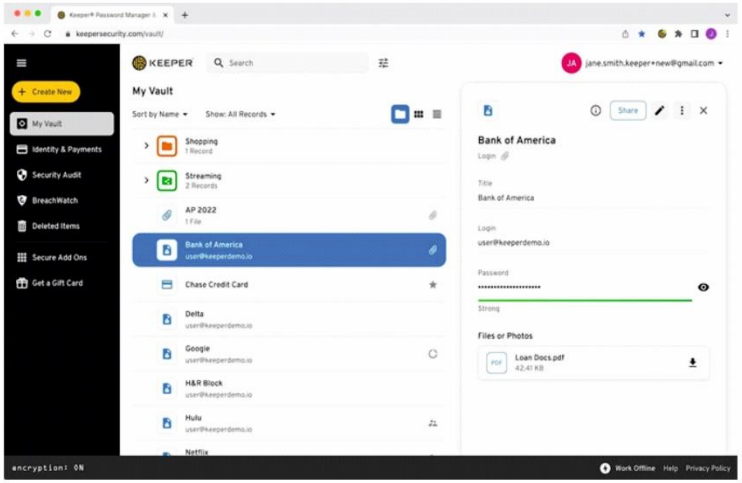


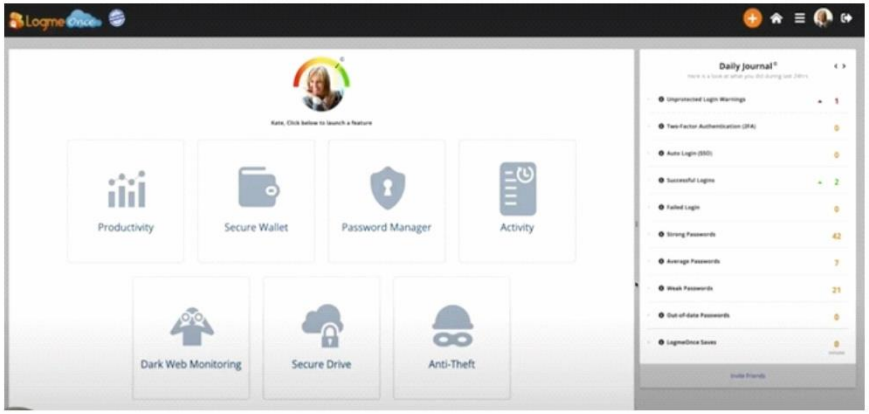


					КРБКБ.200109.20.01.10 Е8			
Зм	Арк.	№ докум.	Підпис	Дата	Система захисту облікових записів від фішингу на основі менеджера паролів	Літ	Маса	Масштаб
Розроб.		Козодой А.В.				У		
Перевір.		Тітова В.Ю.			Структурні схеми	Аркуш	Аркушів	1
Н.контр.		Мостовий С.В				ХНУ, КБ-20-1		
Т.контр.								
Затверд.		Кльоц Ю.П.						









					КРБКБ.200109.20.01.10 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту облікових записів від фішингу на основі менеджера паролів	Літ / Маса / Масштаб
Розроб.		Козодой А.В.				У
Перевір.		Тітова В.Ю.			Менеджери паролів	Аркуш / Аркушів 1
Н.контр.		Мостовий С.В				
Т.контр.						ХНУ, КБ-20-1
Затверд.		Кльоц Ю.П.				

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Козодой Андрія Владиславовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

3.06.24р
дата

підпис

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Козодой Андрій Владиславович
Тема: «Система захисту облікових записів від фішингу на основі менеджеру паролів»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 73;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці системи захисту облікових записів від фішингу на основі менеджеру паролів. В роботі проведено дослідження існуючих методів захисту облікових записів користувачів, зокрема менеджерів паролів, та аналіз їх ефективності. Було розроблено програмну реалізацію системи, проведено її тестування та оцінку рівня безпеки.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було розглянуто існуючі засоби фішингу та його різновиди, проведено порівняльний аналіз методів захисту від фішингу. У другому розділі було проаналізовано існуючі засоби захисту паролів, розглянуто менеджери паролів, визначено їх переваги та недоліки. У третьому розділі наведено реалізацію системи захисту облікових записів від фішингу на основі менеджеру паролів, проведено оцінювання її ефективності.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, у процесі реалізації системи було визначено, що використання менеджерів паролів суттєво підвищує захист інформаційних систем від несанкціонованого доступу в порівнянні з традиційними методами автентифікації.

5. Негативні сторони кваліфікаційної роботи: з тексту роботи не зрозуміло, які саме методи шифрування та атуентифікації були використані для розробленої системи

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 18 » червня 2024 . _____ (підпис)

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Назва: Система захисту облікових записів від фішингу на основі менеджеру паролів

Автор: Козодой Андрій Владиславович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 98,97%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ