2. КЕРУВАННЯ ПАРОЛЯМИ

2.1. Аутентифікація користувача.

2.2. Створюємо надійний пароль.

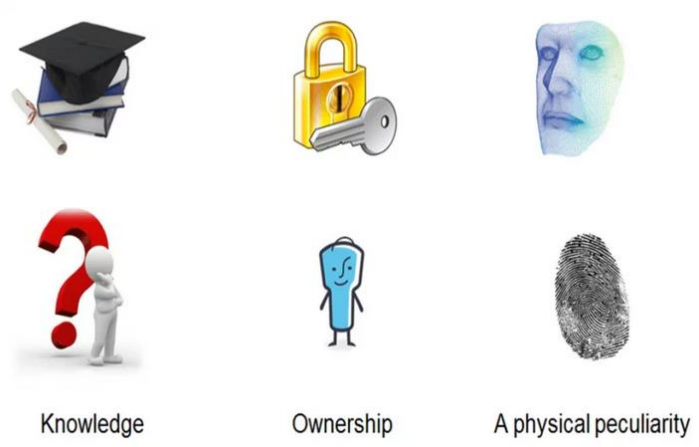
2.3. Менеджери паролів.

2.1. Аутентифікація користувачів.

Аутентифікація користувача – процедура встановлення за допомогою спеціальних програмних засобів достовірності користувача. Аутентифікація користувача включає дві процедури – ідентифікацію та верифікацію.

Підсистема аутентифікації користувачів – найважливіший компонент системи інформаційної безпеки. Ця підсистема підтверджує особу користувача інформаційної системи і тому повинна бути надійною та адекватною, тобто, виключати всі помилки в наданні доступу.

Наявні методи аутентифікації різні за ступенем надійності, та, як правило, з посиленням захисту різко зростає ціна систем, що вимагає при виборі засобів аутентифікації аналізу ризиків та оцінки економічної доцільності застосування певних заходів захисту.



Засоби аутентифікації можна розділити на три групи у відповідності з існуючими принципами:

- принцип «що ви знаєте» («you know»), що лежить в основі методів аутентифікації за паролем;

- принцип «що ви маєте» («you have»), коли аутентифікація здійснюється за допомогою магнітних карт, токенів та інших пристроїв;
- принцип «хто ви є» («you are»), що використовує персональні властивості користувача (відбиток пальця, структуру сітківки ока тощо).

Системи строгої аутентифікації використовують два чи більше факторів при аутентифікації користувачів.

На цей час аутентифікації першої групи («you know») є найбільш економічними за вартістю, але одночасно й найменш надійними. Пароль користувача можна підглянути, перехопити в каналі зв'язку, чи просто підібрати. Якщо політика безпеки вимагає застосування складних паролів, користувачам важко їх запам'ятовувати, і нерідко на самому видному місці з'являються паперові листочки із записами паролів.

Наслідки особливо небезпечні в системах, де використовується принцип «єдиного входу», коли співробітник застосовує один пароль для аутентифікації та роботи з багатьма корпоративними додатками й джерелами інформації. Часто, не усвідомлюючи важливості аутентифікації, працівники практикують передачу особистого пароля колегам.

Системи строгої аутентифікації, побудовані на факторі «you know» і «you have», надають більше можливостей для посилення захисту. Наприклад, роботу токенів, які генерують одноразові паролі, дуже складно підробити, а сам пароль не може бути повторно використаний.

Прикладами можуть служити пристрої RSA SecureID і Vasco Digipass. Найбільш актуальне застосування цих пристроїв в таких областях, як електронна комерція, включаючи Інтернет-банкінг, або для організації захисту ключових з точки зору безпеки користувачів (адміністраторів інформаційної системи та керівників).

Наприклад, подвійна аутентифікація користувача пластикової банківської картки є ефективним засобом підвищення безпеки платежів, здійснюваних з використанням мобільних пристроїв. Для підвищення безпеки Інтернет–платежів компанією Visa застосовується технологія двофакторної

аутентифікації платежів із використанням пластикових карт 3D-Secure. Користувачам карток цієї платіжної системи надається послуга Verified by Visa. Крім логіна і пароля користувачеві пропонується запит на підтвердження володіння пластиковою карткою. Це може бути одноразовий код, який надсилається банком у SMS-повідомленні на мобільний пристрій користувача. У цьому випадку необхідна інтеграція банку з оператором мобільного зв'язку.

При всьому різноманітті існуючих механізмів аутентифікації, найбільш поширеним із них залишається парольний захист. Для цього є декілька причин:

- відносна простота реалізації – механізми парольного захисту зазвичай не вимагає залучення додаткових апаратних засобів;
- традиційність – механізми парольного захисту є звичними для більшості користувачів автоматизованих систем і не викликають психологічного несприйняття – на відмінну, наприклад, від сканерів малюнка сітківки ока.

Блокування мобільних пристроїв.

1) Свайп – абсолютно ненадійний. Це просто захист екрана від випадкового натискання, що оберігає від незапланованих дій. Цей спосіб може вважатися більш-менш прийнятним, лише коли пристрій дійсно не містить будь-якої особистої інформації та повинен бути завжди доступний відразу для декількох осіб.

2) Графічний ключ – слабкий чи середній рівень безпеки. Для недорогих пристроїв на базі Android графічний ключ став популярним методом блокування екрану. Проте слід пам'ятати, що графічний ключ досить легко підглянути через плече. А у разі не надто чистого екрану його іноді можна побачити за слідами пальця.

3) PIN-код – середній або високий рівень безпеки. Ступінь захисту безпосередньо залежить від довжини та складності коду. Наприклад, PIN-код у вигляді 0000 вгадати зовсім не складно. Безпека визначається тим, наскільки швидко та непомітно для сторонніх осіб користувач вводить код.

4) Пароль – високий рівень безпеки. Пароль вважається вже серйозною мірою захисту смарт-пристрою, і при достатній складності підібрати його по-справжньому важко. Як недоліки можна відзначити, що складний пароль незручно вводити, а оскільки більшість користувачів розблокує екрани своїх пристроїв часто, метод ускладнює роботу з гаджетами.

5) Відбиток пальця – високий рівень безпеки. Сканер відбитків пальців став дуже популярним і широко використовується. На останніх моделях він спрацьовує швидко та зручно. До мінусів цього способу відноситься неможливість скористатися сканером відбитків у деяких ситуаціях. Наприклад, якщо руки мокрі або спітнілі. Зчитувач не спрацює і тоді, коли палець забруднений чи травмований. Іноді досить того, що рука огрубіла від холоду.

6) Розпізнавання обличчя – безпека цього способу залишається спірною. виробники стверджують, що цей метод вкрай надійний, але користувачі відзначають, що іноді технологія дає збій і розблокує екран побачивши фотографії користувача або когось із його родичів. Ще один недолік – періодичні збої при розблокуванні в темряві.

7) Сканер райдужної оболонки ока – високий рівень безпеки. По суті, райдужка ока схожа на відбитки пальців – вона унікальна для кожної людини і тому не піддається імітації. І, на відміну від відбитка пальця, ця технологія не потребує фізичного контакту. Однак хотілося б відзначити, що хоч дана функція вже працює на сучасних пристроях, відбувається це поки що досить повільно і вимагає певних зусиль. Зокрема, для розблокування телефон потрібно досить близько піднести до очей, і навіть у цьому випадку можливі збої. Проблеми виникають і при поганому освітленні, носінні окулярів або лінз. Крім того, деякі користувачі цієї технології скаржаться, що від сканування у них болять очі.

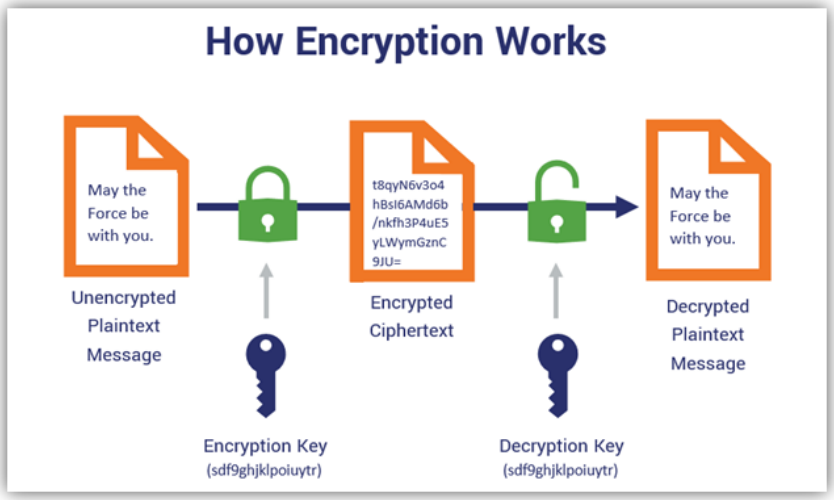
8) Smart Lock – середній рівень безпеки. Android у своїх пристроях пропонує, окрім традиційних способів розблокування екрану, ще й додаткові варіанти, що підвищують комфорт та швидкість користування телефоном. Це означає, що у певних ситуаціях автоматичне блокування екрана вимикається,

якщо телефон вирішує, що загрози безпеці немає. Наприклад, розпізнавання руху означає, що в ситуації, коли телефон розпізнає рух вашого тіла, він буде готовий до роботи після першого розблокування. Ця функція активна, поки телефон залишається в русі або, можливо, в руці власника. Крім того, для пристроїв на базі Android можна встановити безпечні місця, тобто місця зі спрощеним доступом до пристрою. Крім цього, у рамках функції Smart Lock можна призначити розпізнавання довірених додаткових пристроїв. Це означає, що телефон можна відкривати без зайвих паролів, поки поблизу нього знаходиться додатковий пристрій (наприклад, смарт-годинник).

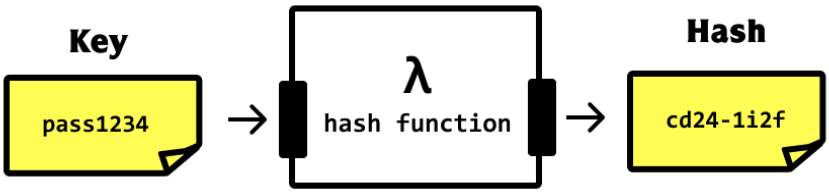
2.2. Створюємо надійний пароль.

Комп'ютерні системи, які використовують паролі для автентифікації, повинні певним чином визначати правильність введеного пароля. Найпростішим способом вирішення даної проблеми є зберігання списку всіх допустимих паролів для кожного користувача. Недоліком такого методу є те, що в разі несанкціонованого доступу до списку, зловмисник дізнається всі паролі. Більш поширений підхід полягає у зберіганні значень криптографічної хеш-функції від парольної фрази.

У межах кібербезпеки поняття «пароль» не треба плутати з поняттям «ключ». Із криптографічної точки зору це зовсім різні поняття. Пароль – це таємне слово або певна послідовність символів, призначена для підтвердження особи або її прав. Але комп'ютерні програми не використовують паролі безпосередньо для шифрування, вони з паролів отримують ключі. Ключі шифрування – це рядки бітів (0 або 1) різної довжини, найбільш часто використовуються 40, 64 і 128-бітові ключі.



Ключі з паролів отримують за допомогою спеціальної операції – хешування. Хешування – це досить складна криптографічна функція, яка отримує на вході рядок будь-якої довжини, і генерує на виході рядок бітів фіксованої довжини (хеш). Хешування володіє двома основними властивостями: навіть незначні зміни вхідного рядку призводять до повної зміни вихідного хеш-значення; по відомому хеш-значенню практично неможливо підібрати вихідний рядок.



Злочинець може отримати пароль із використанням методів соціальної інженерії чи за допомогою технічних (програмних) засобів. Для злому паролів в більшості випадків використовується перебір. Програмне забезпечення генерує різні варіанти паролів й повідомляє якщо був знайдений правильний. У деяких випадках персональний комп’ютер здатний видавати мільйони варіантів на секунду.

Час, необхідний для злому пароля є пропорційним довжині та складності цього пароля. Також швидкість перебору залежить від криптографічного функції, яка застосовується для генерації хешей пароля.

Для стійких криптоалгоритмів (коли атакуючий може лише генерувати і перевіряти паролі) існують 2 основних методи злому паролю: атака перебором і

за словником. Атака перебором використовується тоді, коли відсутня додаткова інформація щодо паролю й зловмисник пробує всі можливі паролі. Якщо зловмисник знає, що пароль – це певне реальне слово, він може використовувати атаку за словником. Тоді в якості можливих паролів перевіряються тільки слова із словника. В словнику міститься менше 100 000 слів, тому їх можна перевірити дуже швидко – в більшості випадків це займає лише декілька секунд.

Поєднання двох описаних вище атак називається «атака по складах». Вона використовується в тому випадку, якщо пароль спотворений або являє собою неіснуюче слово. Тоді зломщик може об’єднувати склади, щоб підібрати потрібне слово.

Найпотужніша – «атака на основі правил». Вона може бути використана у тих випадках, коли атакуючий володіє деякою інформацією про пароль, який він хоче зламати. Наприклад, йому відомо, що пароль складається зі слова і одно- або двозначного числа. Він пише правило, і програма генерує тільки відповідні паролі (user1, mind67, snapshot99 тощо). Або інший приклад: атакуючий знає, що перша буква у верхньому регістрі, друга – голосна і що пароль не довше 6 символів. Така інформація може зменшити кількість можливих паролів в 20–30 разів. Цей метод включає всі атаки — перебором, за словником і по складах.

Складність пароля зазвичай оцінюють в термінах інформаційної ентропії, яка вимірюється в бітах. Кількістю «бітів ентропії» в паролі називається логарифм за основою 2 від числа спроб, необхідних для того, щоб точно вгадати пароль. Наприклад, для визначення паролю із 40-бітною складністю

необхідно провести 2^{42} (4 398 046 511 104) спроб, перевіривши всі можливі варіанти. Кожен новий біт ентропії збільшує складність паролю вдвічі, отже, вдвічі ускладняється й завдання для зловмисника. В середньому зловмиснику доводиться випробувати половину можливих варіантів для успішного підбору пароля.

Паролі, які створені людьми, зазвичай недостатньо випадкові – у середньому 40 біт ентропії, це пов'язано із поганим сприйняттям ймовірності людьми (наприклад, число 20 здається менш ймовірним за число 17). Також, намагаючись обрати випадкові послідовності символів для створення паролю, люди не використовують усі символи абетки рівномірно (наприклад, літера «е» використовується набагато частіше за літеру «f).

На складність пароля впливають такі чинники:

- кількість символів у паролі. Чим більше знаків у послідовності, тим краще. У комбінації з 5 знаків є велика ймовірність швидкого злому. А на підбір послідовності з 20 знаків можуть піти роки;
- чергування великих і малих літер. Приклади: пароль dfS123UYt з використанням регістра заголовних букв на порядок складніше цієї ж комбінації, але лише з маленькими літерами – dfs123uyt;
- символьні набори – різноманітність типів символів підсилює стійкість;
- Якщо скласти пароль із маленьких й великих літер, цифр та спеціальних символів довжиною в 15-20 знаків, шанси його підібрати практично нульові. Дуже важливо рівномірно розподілити знаки у паролі. Але зазвичай користувачі цифри та спеціальні символи ставлять у кінець пароля, а великі літери на початок – Okn@333.Приклад рівномірного розподілу символів у паролі – kIs$t0cHk@.

Орієнтовний час підбору паролів різної складності:

- дата народження 12071996 – 0,003 секунди;
- ім'я з великої літери Maksim і малої maksim – максимум півсекунди;

- поєднання, що складається з букв і цифр 7s3a8f1m2a – близько доби;
- vSA-DFRLLz – 1 рік;
- поєднання iu2374NDHSA) DD – 204 млн років.

У наступній таблиці наведено приблизний час повного перебору паролів у залежності від їх довжини. Вважається, що в паролі можуть використовуватися 36 різних символів (латинські букви одного регістра та цифри), а швидкість перебору складає 100 000 паролів в секунду.

Кількість знаків	Кількість варіантів	Стійкість	Час перебору
1	36	5 біт	менше секунди
2	1296	10 біт	менше секунди
3	46656	15 біт	менше секунди
4	1679616	21 біт	17 секунд
5	60466176	26 біт	10 хвилин
6	2176782336	31 біт	6 годин
7	78364164096	36 біт	9 днів
8	$2,821\ 109\ 9x10^{12}$	41 біт	11 місяців
9	$1,015\ 599\ 5x10^{14}$	46 біт	32 роки
10	$3,656\ 158\ 4x10^{15}$	52 біта	1162 роки
11	$1,316\ 217\ 0x10^{17}$	58 біт	41823 роки
12	$4,738\ 381\ 3x10^{18}$	62 біта	1505615 років

Прикладами широко розповсюджених, але дуже примітивних та ненадійних паролів є такі:

- послідовності й повтори: 12345, 337799, 10011001, abcde, aaaabbbb;
- дати народження: 13051990, 19900513, 0513;
- номери телефону: 0508765432, 0661543210;
- відомі цифрові комбінації: «102», «911», «777»;
- поширені слова: password, administrator;
- Ваше ім’я, імена родичів або домашніх тварин: anton, alex, sveto4ka, barsik, kesha;
- географічні назви: Ukraine, Mississippi, pacificocean;
- системне ім’я користувача або його частини: guest, user, default;

- адреси електронної пошти: example@ukr.net, pochta@gmail.com;
- клавіатурні послідовності символів: qwerty, Asdfg.

Спортивні паролі — одні з найулюбленіших, особливо серед чоловіків. Найбільш очевидні приклади: football, baseball. Назви популярних у вашому регіоні спортивних команд та імена гравців, навіть у поєднанні з важливими для локальної спортивної історії датами: LevsKi1914, DinAmO1975 також є слабкими паролями.

Любов, довіра, ненависть та інші емоції — ще одна популярна тема для створення паролів. Їх можна розділити на дві категорії: прості комбінації: iloveyou, loveme, trustno1 чи почуття до певних людей. Злочинці можуть мати певну інформацію про вас. Тому не варто використовувати пароль IloveAnn чи (жартома, звичайно,) HategeorGe, особливо якщо це імена ваших жінки або чоловіка. Поширені паролі на тему природи на кшталт flower і sunshine залишаються одними з найпростіших для зламу. Серед найпопулярніших фантастичних є dragon, princess, ninja і superman. Паролі такого типу теж дуже легко зламати.

SplashData.com

позиція	**2017**	**2018**	**2019**	**2020**	**2021**
1.	123456	123456	123456	123456	123456
2.	password	password	23456789	123456789	123456789
3.	12345678	123456789	qwerty	qwerty	qwerty
4.	qwerty	12345678	password	parol	parol
5.	12345	12345	1234567	1234567	1234567
6.	123456789	111111	12345678	12345678	12345678
7.	letmein	1234567	12345	12345	12345
8.	1234567	sunshine	iloveyou	iloveyou	iloveyou
9.	football	qwerty	111111	111111	111111
10.	iloveyou	iloveyou	23123	123123	123123

NordPass.com, 2020

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213

Принципи створення стійкого пароля:

- логін і пароль не повинен бути ідентичним;
- пароль не повинен складатися з особистої інформації (дата народження, телефон тощо);
- пароль не повинен складатися виключно з літер;
- створювати новий пароль для кожного окремого сервісу;
- використовувати двофакторну автентифікацію (за наявності);
- не зберігати паролі у браузері;
- не вводити паролі на сайтах без протоколу HTTPS (за його допомогою шифруються всі дані між клієнтом і сервером, що створює повну конфіденційність інформації користувача, наприклад паролі або банківські реквізити);
- нікому не довіряти та не називати пароль;
- враховувати довжину паролю – бажано не менше 10 символів;
- міняти пароль щоразу, коли здається, що його могли вкрасти. В інших випадках змінювати пароль не рідше ніж раз на 6 місяців.

У той же час, новий пароль не повинен бути простою модифікацією діючого, наприклад, шляхом зміни однієї цифри: h0lst1, h0lst2, h0lst3.

Рекомендації щодо створення унікальних паролів для різних сервісів:

- для критично важливих ресурсів (поштова скринька, платіжні системи, месенджери та соцмережі) використовувати складні та довгі паролі з довільними комбінаціями верхнього та нижнього регістру, цифр та спеціальних символів. Наприклад: S9Scap$iDPRZ;
- для важливих ресурсів (навчальні сайти, альтернативна поштова скринька) – паролі, де довжина важливіша за складність. Наприклад: hrGbWzeCjZSqUl;
- для не дуже важливих ресурсів (форуми, розважальні портали) вигадати прості, але не примітивні паролі. наприклад: metHalPh.

Методи створення стійких паролів.

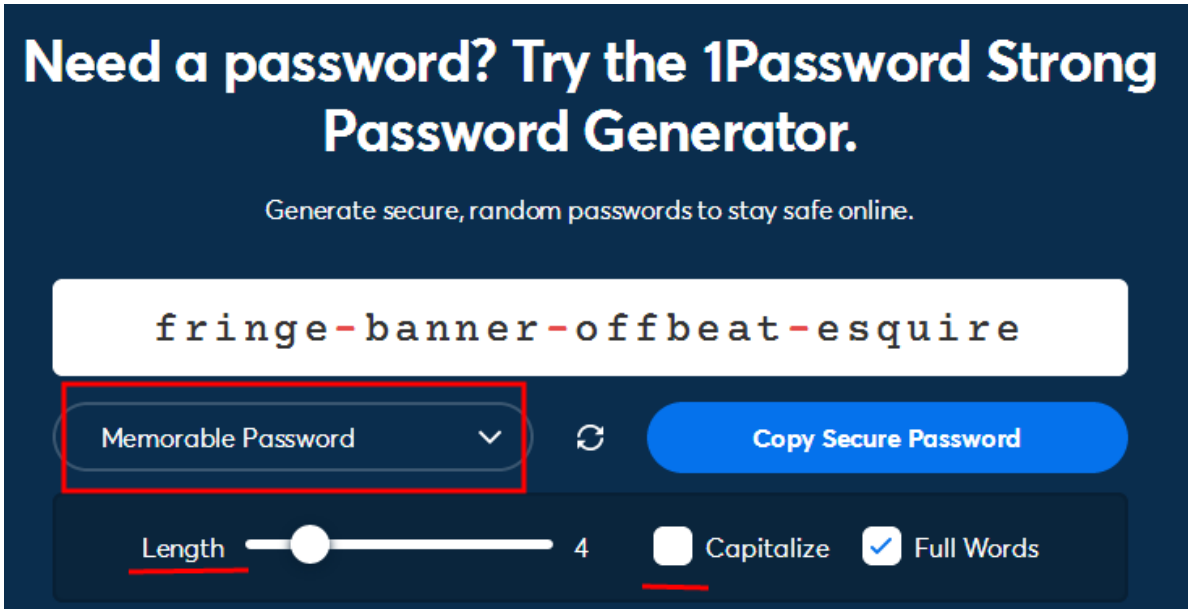
При створенні стійких паролів виникають дві проблеми – вигадати складний пароль та запам’ятати його.

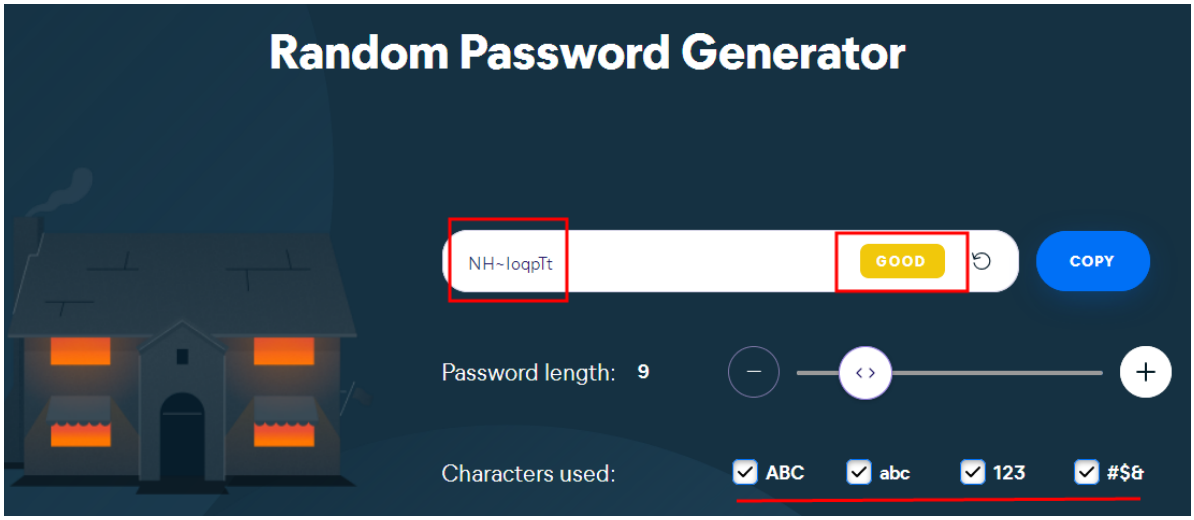
Якими б відповідальними не були люди, вони створюють паролі за шаблонами власного мислення, і це відомо зловмисникам. Дослідження та аналіз паролів показали, що 40% із них можна підібрати, використовуючи програмні методи. Часто людина, яка складає пароль, вказує в ньому те, що має безпосереднє відношення до неї та/або її оточення.

1. Найбільш стійкими є паролі, які створені за допомогою «генераторів паролей» – спеціалізованих сервісів, зокрема й хмарних. Наприклад, KeePass чи https://1password.com/password-generator/. При автоматичній генерації виключається взаємозв’язок між паролем та особистістю користувача. випадково обраний пароль створюється з величезного масиву даних і підібрати його дуже складно.

Але такі паролі є найбільш складними для запам’ятовування, наприклад, T2tgU#&y59kUOo чи 84aP@E&39uzxC1ka0. Якщо ви вирішили записати такий пароль (на папері чи у текстовий файл), то врахуйте, що не потрібно зберігати записаний пароль у доступному місці: приклеєному на робочий стіл або

захований під клавіатуру, оргтехніку; на робочому столі комп'ютера в текстових файлах (краще сховати в архів із нескладним парольним захистом); чи у браузері.



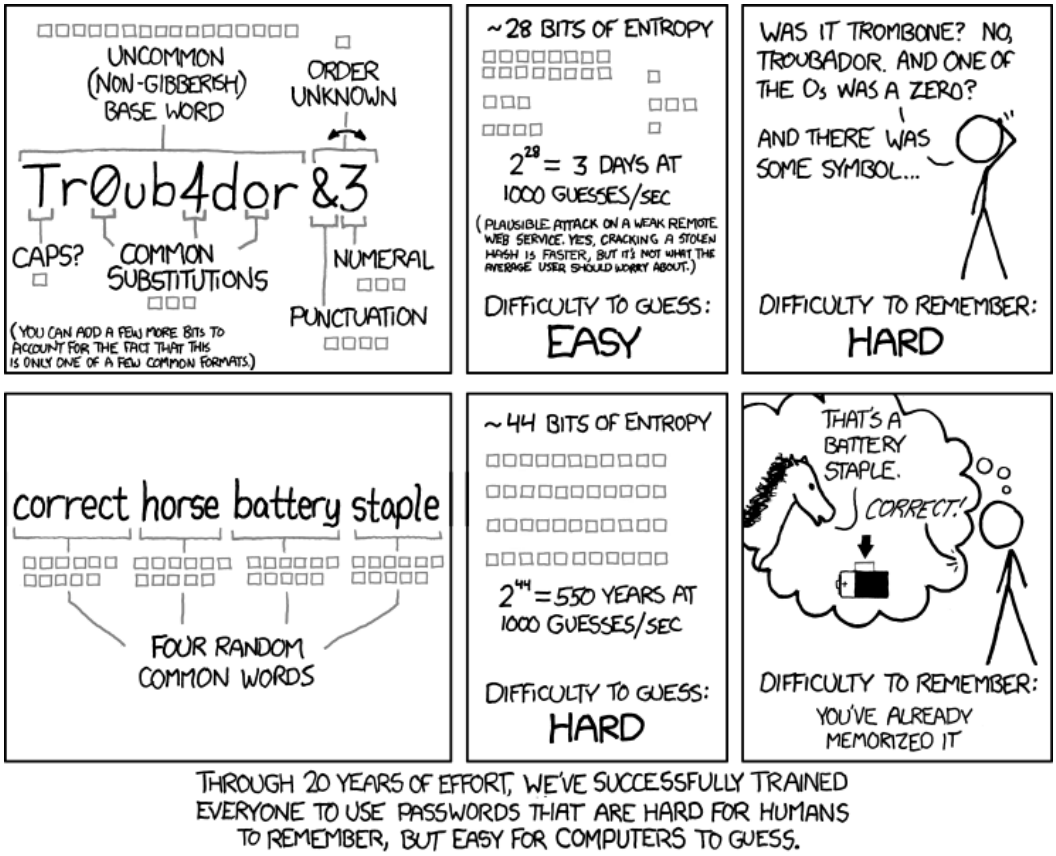


Краще завести спеціальний блокнот з паролями й тримати його у надійному місці. Американський криптограф Брюс Шнайєр рекомендує записувати паролі на маленьких шматочках паперу та зберігати у гаманці. Інший варіант – скористатися менеджером паролів.

2. При грамотному підході довжина пароля має пріоритет над його складністю, оскільки у рази збільшується кількість варіантів перебору. Марк Бернетт, дослідник у галузі безпеки, у своїй книзі Perfect passwords пише, що пароль завдовжки 12-15 знаків надійніший, ніж короткий, складений із

довільної послідовності символів, з використанням спеціальних символів та літер верхнього регістру. Таку ж думку має й Ден Уілер – IT-фахівець із Dropbox. Замість T@MQ36n^iL можна успішно використовувати correcthorsebatterystaple.

Проте, проста парольна фраза, така як iloverocknroll, передбачувана і тому зловмиснику її легше вгадати, у порівнянні з більш коротким паролем 9j%a#F,0.



3. вирішити проблему використання дуже складних варіантів допоможуть мнемонічні паролі, які добре запам’ятовуються. Спочатку треба скласти (вигадати) якусь фразу-нісенітницю (каламбур), що не має жодного практичного сенсу: ГЛОКАЯ КЕЗДРА МІНОРИТЬ БОКРЕНЯ. Далі беремо від однієї до трьох чи більше перших літер із кожного слова та записуємо відповідні їм літери латиною:

ГЛ	КУ	МІ	БО
UK	RE	VS	,J

Результат: «ukrevs,j».

Пароль можна покращити шляхом додавання між слогами певної дати (див. метод 5), краще у зворотному порядку, зміною регістру літер (наприклад, кожна друга літера – велика) та додаванням спецсимволів:

%uK2rE1vS0,J1.

4. Певною модифікацією методів 2 та 3 є такий прийом. В основі пароля лежить нетривіальне та довге слово української мови (чи іншої, за винятком англійської), можливо, вузький професіональний термін, чи застаріле, діалектичне слово: професорсько-викладацький, перехняблюватися, дихлордифенілтрихлорметилметан (*інсектицид проти шкідників, побутова назва ДДТ*), *екстрадихлордифенілтрихлорметилметан*.

Шляхом трансформації кириличних букв у англійські, отримаємо надійний пароль:

ghjatcjhcmrj-dbrkflfwmrbq,

gtht[yz,k/dfnbcz,

lb[kjhlbatyiknhb[kjhvtnbkvtnfy.

5. Цифровий метод. За основу паролю вибираємо Ваші пам’ятні дати. Але це не повинен бути Ваш день народження або день початку сімейного життя! Подія має бути виняткової важливості, але про неї повинні знати лише ви. Наприклад, день, коли ви вперше втекли з уроку або зламали підбор.

Оскільки основу пароля складають цифри, доцільно перемішати їх із літерами. Приклад: 22.10.1993 та 16.03.2021 Замініть точки, що розділяють день, місяць і рік, на будь-яку букву, наприклад маленьку англійську «l» (ель). Між двома датами поставимо «!». Нулі замінимо на літери «O»:

«22l1Ol1993!16lO3l2O21».

Цифровий метод можна вдосконалити, якщо проводити певні розрахунки з датами, що лежать в основі паролю. Наприклад, перемножити дві дати між собою: 22101993×2021=44668127853. За допомогою програми калькулятор можна перевести це число в шістнадцятирічну систему числення: досить натиснути кнопку Hex: A666D8A6D.

6. Метод мастер-пароля. Для того, щоб спростити створення унікальних паролів для різних сервісів можна скористатися наступним методом (але більш надійним буде використання абсолютно різних паролів для кожного сервісу!). Створюємо мастер-пароль, наприклад, A666D8A6D. Далі, за певним алгоритмом, додаємо до цієї основи ідентифікатор певного сервісу. Наприклад, ставимо символ «+» й додаємо 4 літери, які характеризують вебресурс:

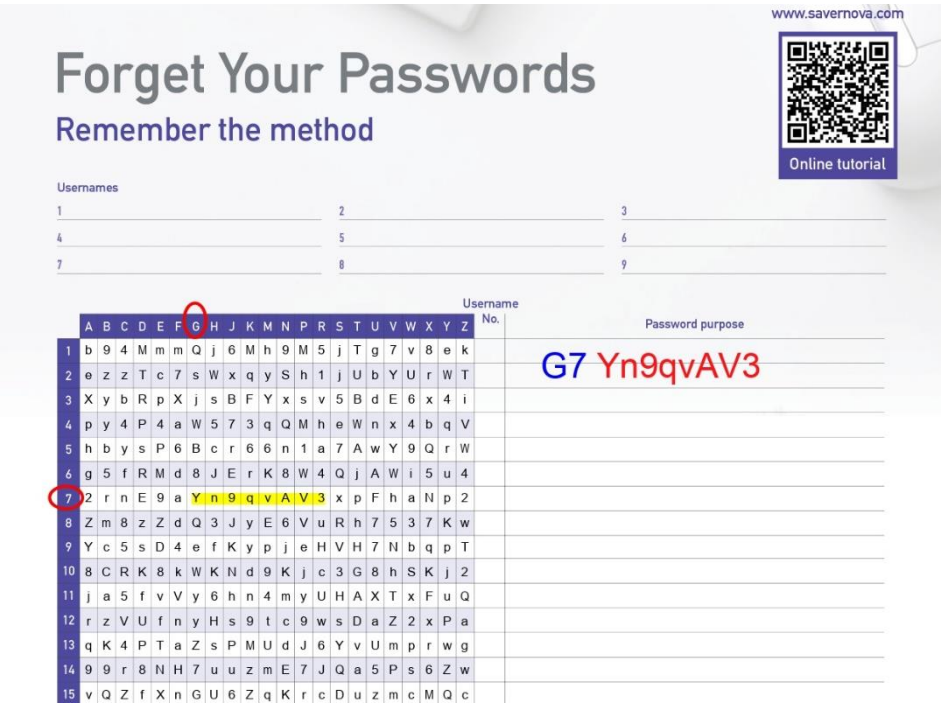
A666D8A6D+bank – для фінансових справ;

A666D8A6D+twit – соціальні мережі;

A666D8A6D+mail – електронна пошта.

7. Графічний метод. Створіть візуально контури геометричної фігури або будь-якого предмета на клавіатурі вашого комп'ютера. використовуйте символи, за якими проходять лінії. Важливо: фігура не повинна бути примітивною, наприклад квадратом.

8. Карта паролів (https://www.savernova.com/). визначте Ваш метод читання, який використовуватиметься кожного разу. Він складається з початкової точки та напряму руху. Такі паролі задовольняють сучасні критерії безпеки, їх важко зламати; якщо користувач втратить картку, це також не проблема: без особистого методу читання карта непотрібна. Кожна картка є унікальною.



Для перевірки стійкості створених паролів доцільно скористатися відповідними онлайн-сервісами, наприклад:

https://exploit.in/passcheck/,

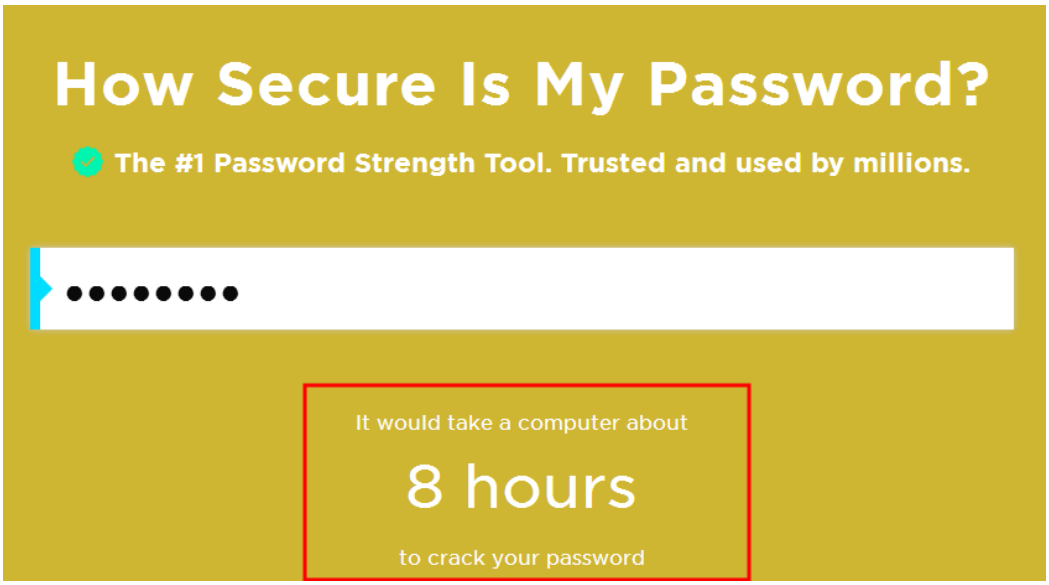
https://zillya.ua/check-password,

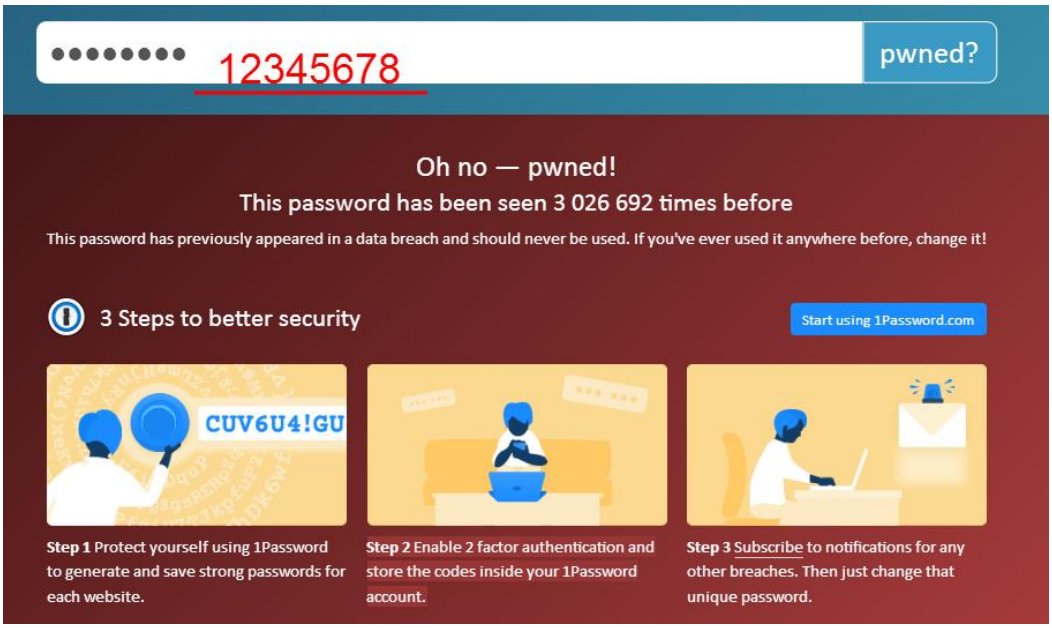
https://www.security.org/how-secure-is-my-password/.

Сервісі, що містять бази з реальними паролями, які раніше були розкриті в результаті порушення даних:

https://haveibeenpwned.com/Passwords, https://breachalarm.com/,

https://pwnedlist.com/query.





Інциденти:

- компанія «Нутелла» порадила передплатникам використовувати як надійний пароль слово Nutella;
- один із співробітників Білого дому загубив на автобусній зупинці папірець, на якому було записано незахищений пароль від електронної пошти;
- у Google стажувався студент з Індії, який зміг отримати доступ до супутника компанії через адміністративну панель, просто залишивши поля введення логіну та пароля порожніми;
- дані понад 14 мільйонів виборців штату Техас стали доступними в режимі онлайн оскільки сервер не захистили паролем;
- співробітники Організації Об'єднаних Націй зберігають документи у Trello та Google Docs, які не захищені паролем. За посиланнями вони стають доступними для всіх бажаючих.

2.3. Менеджери паролів.

Для надійного зберігання великої кількості сильних паролів, які важко запам'ятати, доцільно використовувати менеджери (диспетчери) паролів – спеціалізовані програмні продукти для роботи з паролями, PIN-кодами. Менеджери паролів мають наступні переваги:

- гарантована безпека важливих даних – сервіс дає можливість зберігати не лише ідентифікатори, а також PIN-коди від банківських карт, номери рахунків тощо;
- генерування унікальних послідовностей – більшість програм оснащені спеціальним інструментом, який генерує оригінальні випадкові комбінації символів за заданими параметрами. Вони захищені від підбору, адже не містять будь-якої особистої інформації користувача;
- спрощення авторизації – програма запам'ятовує послідовності для конкретних ресурсів і під час повторного входу автоматично заповнює необхідні поля. Функція автозаповнення не застосовується до програм і додатків, але в такому разі можна просто скопіювати потрібний пароль;

- відсутність потреби запам’ятовувати всі комбінації – вони містяться в одному сервісі, тож Вам потрібно запам’ятати лише майстер-пароль.

Менеджер паролів може бути реалізовано як онлайн-сервіс, бути вбудованим до браузеру чи інстальований в операційну систему Вашого пристрою. Менеджер використовує досить потужне шифрування AES, яке практично не піддається зламу з довжиною ключа у 256 біт. Таку базу можна розблокувати тільки за допомогою використання правильного майстер-паролю, отже, користувачу необхідно запам’ятати лише один надійний пароль.

Менеджер паролів Вашого браузера дозволяє без додаткового програмного забезпечення зберігати всі паролі та надійно синхронізувати їх між своїми пристроями. Обліковий запис, з яким синхронізовано Ваш браузер, може бути захищений двоступеневою автентифікацією.

Але вбудовані до браузеру менеджери мають й недоліки – менші потужність та обмежений функціонал, у порівнянні зі спеціальними програмними засобами; прив’язка до певного браузера та, інколи, й операційної системи.

Спеціалізовані менеджери паролів мають розширений функціонал, який полегшує доступ до паролів, ліцензійних ключів, Wi-Fi-кодів тощо. Такі менеджери паролів мають функції спільного використання паролів та системи попередження, які вказують слабкі та повторно використані паролі, повідомляють, коли пароль, який ви використовуєте, було виявлено в базах даних паролів, які зазнали витоку.

Перевагу треба надавати менеджерам паролів, які існують вже багато років та мають відкритий код.

Кампанія Avast надає такі поради щодо вибору менеджеру паролів:

- безпека – наявність функцій керування паролями для додатків і сайтів, попередження про витік даних із сайтів, на яких ви зареєстровані;
- багатофакторна автентифікація;
- генератор безпечних паролів;
- безпечна синхронізація паролів для різних пристроїв;
- автоматичне оновлення паролів для зламаних сайтів;
- зручність використання, наприклад, автозаповнення паролів;
- розширення для браузера;
- менеджер паролів для програм;
- функція «Електронний гаманець» – зберігає номери Ваших кредитних карток та інші платіжні реквізити у захищеному вигляді, автоматизуючи процес їхнього введення при покупці;
- екстрений доступ для інших користувачів – дозволяє членам сім'ї або колегам отримати доступ до важливих облікових записів у разі надзвичайної ситуації;
- багатоплатформні рішення.