Лекція 8

# Основи інформаційної безпеки

# План лекції:

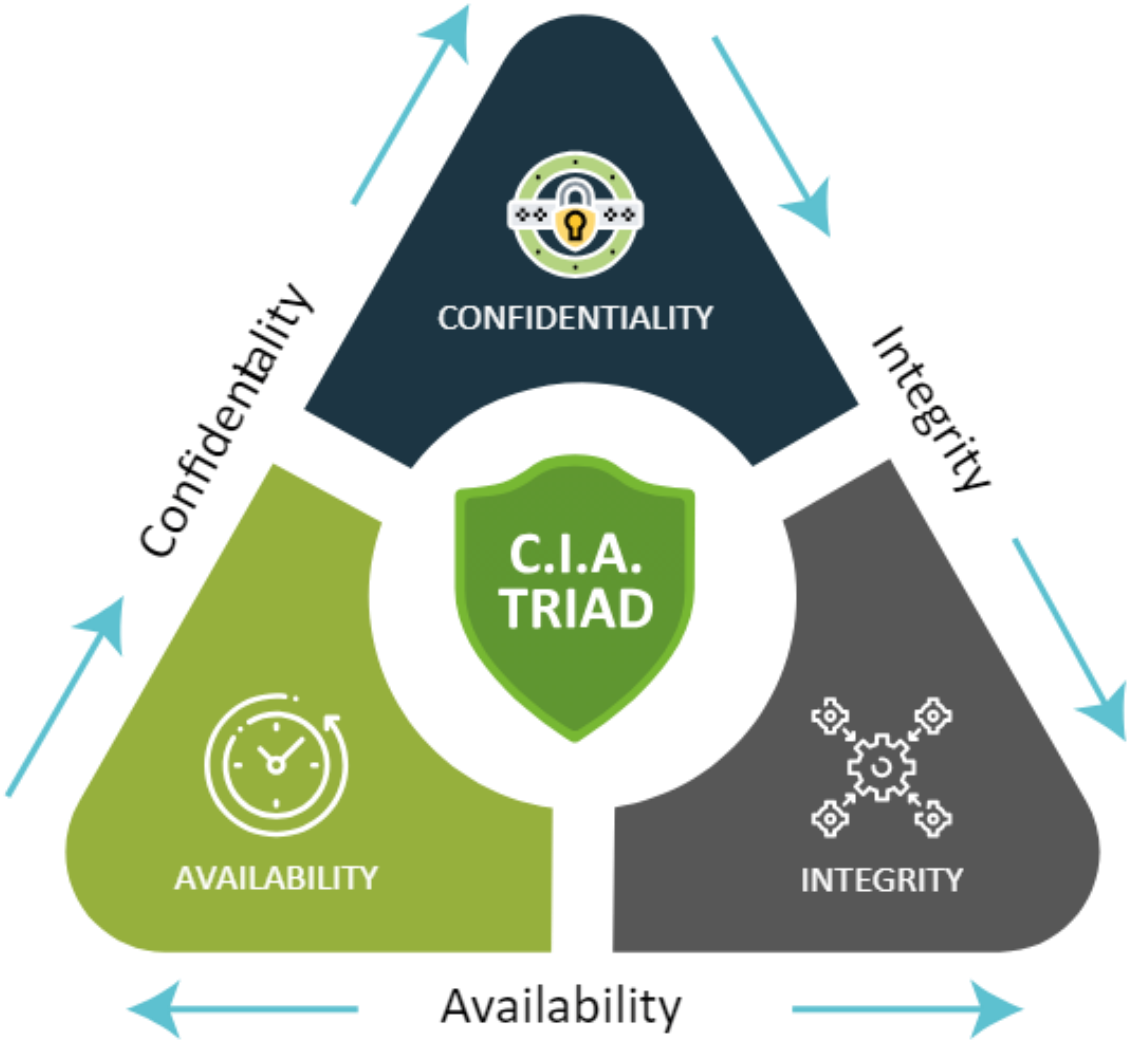
1. Основні положення інформаційної безпеки
2. Загрози під час роботи в Інтернеті
2. Шляхи захисту  даних

# Інформаційна безпека

— це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Також під **інформаційною безпекою** розуміють комплекс заходів, спрямованих на забезпечення захищеності даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення.

# Конфіденційність, цілісність і доступність



# Конфіденційність

Конфіденційність означає зберігання в таємниці.

В IT це означає зберігання наявних даних надійно прихованими від сторонніх очей.

Один із методів конфіденційності, який ви напевно використовуєте щодня, – це захист паролем.

# Цілісність

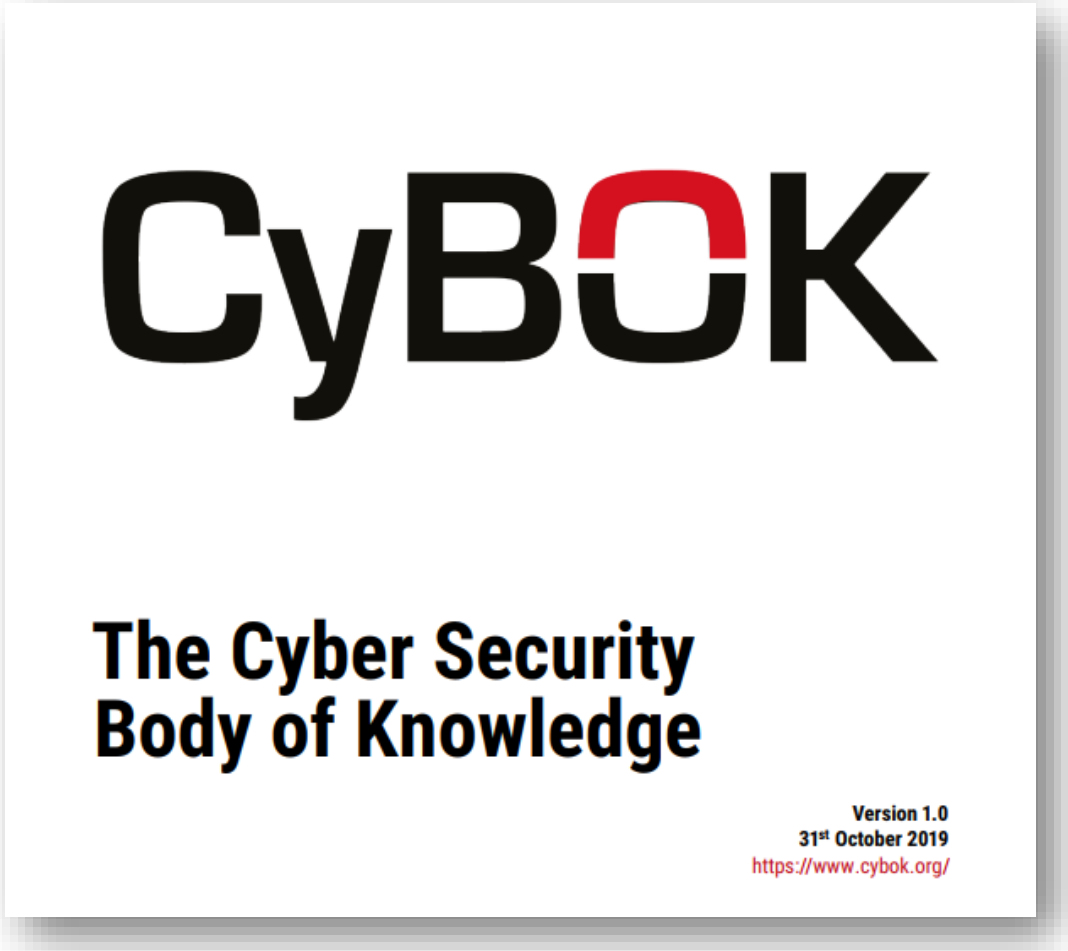
– це збереження даних точними й неспотвореними. Дані, які ми надсилаємо чи отримуємо, мають залишатися незмінними протягом усього процесу.

Уявіть, що ви завантажили файл з Інтернету. На вебсайті, з якого ви його завантажили, указано, що розмір файлу – 3 МБ. Але після завантаження виявилось, що справжній розмір файлу – 30 МБ. Це сигнал про небезпеку. Щось сталося під час завантаження, щось потенційно небезпечне.

# Доступність

Доступність означає, що наявна інформація легко доступна тим користувачам, яким вона необхідна. Це може означати багато речей, зокрема готовність до втрати даних або збою системи. Хакерські атаки мають на меті вкрасти у вас чимало речей: час, матеріальні цінності, вашу гідність. Іноді у вас крадуть час, який ви мусите витрачати на відновлення роботи сервісів.

# Основи інформаційної безпеки



# Загрози під час роботи в Інтернеті

Серед основних загроз використання комп'ютерних мереж для користувачів, виділяють:

- Комунікаційні ризики
- Контентні ризики
- Споживчі ризики
- Технічні ризики

# Комунікаційні ризики

**- ризики, що пов'язані зі спілкуванням у мережі та використанням онлайн-ігор:**

**БУЛІНГ** - залякування, приниження, цькування, переслідування, компрометація людей з використанням особистих або підробних матеріалів, розміщених в Інтернеті, надсилання повідомлень з використанням різних сервісів;

**КОМПРОМЕТУВАТИ** – виставляти в негарному вигляді, шкодити добрій славі;

**КІБЕР–ГРУМІНГ** - входження в довіру людини для використання її в сексуальних цілях;

**ОНЛАЙН – ІГРИ** – надмірне захоплення може призвести до втрати реальності, нерозуміння та несприйняття норм і правил людського співіснування, комп'ютерної залежності.

## Контентні ризики

**- ризики, що пов'язані з доступом до матеріалів, розміщених у мережі, матеріалів шкідливого характеру або таких, що не відповідають віковим особливостям розвитку дитячої психіки.**

Такі матеріали як правило містять:

- ✓ сцени насилля, жорсткої поведінки з людьми та тваринами;
- ✓ пропаганду расової або національної ненависті;
- ✓ рекламу або пропаганду використання тютюну, алкоголю та наркотиків, азартних ігор;
- ✓ пропаганду релігійних вірувань, заборонених законодавством, або спільнот, що не мають офіційних дозволів на свою діяльність;
- ✓ пропаганду шкідливих лікарських засобів і методів боротьби з хворобами, відмови від лікування;
- ✓ нецензурну лексику;
- ✓ матеріали для дорослих.

**Споживчі ризики** - **ризики, що пов'язані з порушенням прав споживачів:**

- ✓ реклама та продаж через мережу інтернет-магазинів низькоякісної продукції;
- ✓ купівля підроблених товарів відомих виробників;
- ✓ втрата коштів через невиконання обіцянок надіслати товар, невідповідність товару за якістю або за виробником (шахрайство);
- ✓ викрадання персональних даних для зняття коштів без відома користувача з його рахунків.

## Технічні ризики

**- ризики, що пов'язані з роботою шкідливих програм:**

- ✓ **Віруси**
- ✓ **Хробаки (черв'яки)**
- ✓ **Трояни**
- ✓ **Скрипт-віруси**
- ✓ **Дропери**
- ✓ **Боти**
- ✓ **Руткіти**
- ✓ **Експлойти**
- ✓ **Бекдори**
- ✓ **Шпигунські програми**
- ✓ **Рекламні модулі або Adware**

Загрозу також становить **фішинг та спам** як різновид інтернет-шахрайства.

# Шляхи захисту даних

Серед заходів безпеки, яких повинен дотримуватися кожен користувач, перше місце займає його особиста організованість і відповідальне ставлення до зберігання важливих даних.

Розрізняють три шляхи захисту даних:

- Захист доступу до комп'ютера
- Захист даних на дисках
- Захист даних в Інтернеті

# Захист доступу до комп'ютера

Для запобігання несанкціонованому доступу до даних, що зберігаються на комп'ютері, використовують ***облікові записи***.

Налаштування Windows – Облікові записи

**При щоденній роботі за комп'ютером використовуйте обліковий запис Windows без прав адіністратора.**
Це простий, безкоштовний і доступний кожному спосіб захисту від більшості шкідливих програм.

Захистити конфіденційну інформацію можна також шляхом архівування та встановлення пароля на архів. Такий спосіб захисту доцільно використовувати й під час листування.

# Захист даних на дисках

Для зберігання даних та їх захисту від пошкодження варто розділити жорсткий диск на ***кілька логічних розділів***.


На кожний диск, папку та файли локального комп'ютера, а також комп'ютера, підключеного до локальної мережі, встановлюються певні ***права доступу*** (***повний, тільки читання, доступ за паролем***).

**Встановіть антивірус одразу після встановлення операційної системи і постійно його оновлюйте.**

**Користуйтеся ліцензійними або з вільною ліцензією програмним забезпеченням, вчасно їх оновлюйте.**

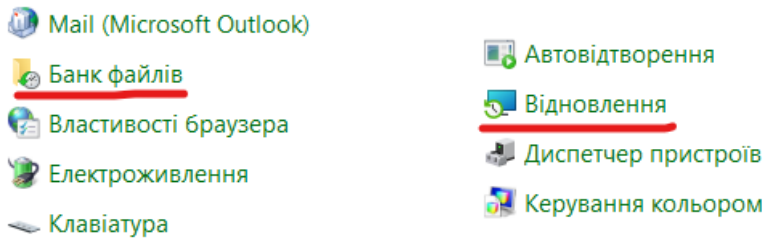
# Захист даних на дисках

Наведемо деякі рекомендації щодо запобігання втраті даних.

- ✓ Не зберігайте важливі дані на системному диску, робочому столі, у папках власної Бібліотеки ( Моя музика, Мої документи тощо), бо системний диск найчастіше підпадає під вплив шкідливих програм.
- ✓ Періодично робіть резервне копіювання важливої інформації. Для бекапу використовуйте зовнішні накопичувачі (оптичні CD- і DVD-диски, окремі жорсткі диски тощо) та зовнішні хмарні диски.

**!** **Після збереження даних на флеш-носії слід дотримуватися правил його безпечного вилучення. Тоді дані, що не встигли скопіюватися із буфера запису, не втратяться.**

Для резервного копіювання файлів і можливості відновлення операційної системи користуйтесь утилітами ОС Windows.



# Безпечне видалення даних

**Пам'ятайте, що у разі випадкового видалення інформації є можливість її відновити.**

Для видалення файлів і папок із можливістю їх відновлення використовують, як вам відомо, папку ***Кошик***.

***Не копіюйте нову*** інформацію на жорсткий диск. Вимкніть комп'ютер, зверніться у сервісний центр.

Якщо Ви досвідчений користувач:
- Використовуйте спеціальні програми : ***NTFS Recovery, UndeletePlus*** та інші

**Зберігайте робочі файли не на системному диску.**

Для повного стирання даних доцільно використовувати спеціальні програми, наприклад, ***Eraser, CCleaner***, які на місце видалених даних записують нові.

# Захист даних в Інтернеті

Для забезпечення інформаційної безпеки в Інтернеті недостатньо захистити дані на комп'ютері-клієнті або комп'ютері-сервері. Зловмисник може перехопити дані під час обміну ними через канали зв'язку. Захист даних забезпечується спеціальним криптографічним протоколом шифрування даних під час їхнього передавання.

**Захищений сайт** — це сайт, який використовує для обміну даними протоколи захищеного зв'язку.

Щоб визначити, що сайти **захищені**, слід звернути увагу на їхню ***URL-адресу*** — вона починається з *https://*. Це — протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протокол https зображається значок замка — це означає, що з'єднання захищене й більш безпечне.

Для захисту даних під час роботи в Інтернеті доцільно також використовувати підключення, захищене шифруванням.

Наприклад, за замовчуванням *Google* шифрує з'єднання з *Gmail*, а також при виборі інших сервісів *Google*, наприклад *Google Диск*, активується ***протокол шифрування SSL***, який використовується до завершення сеансу роботи.

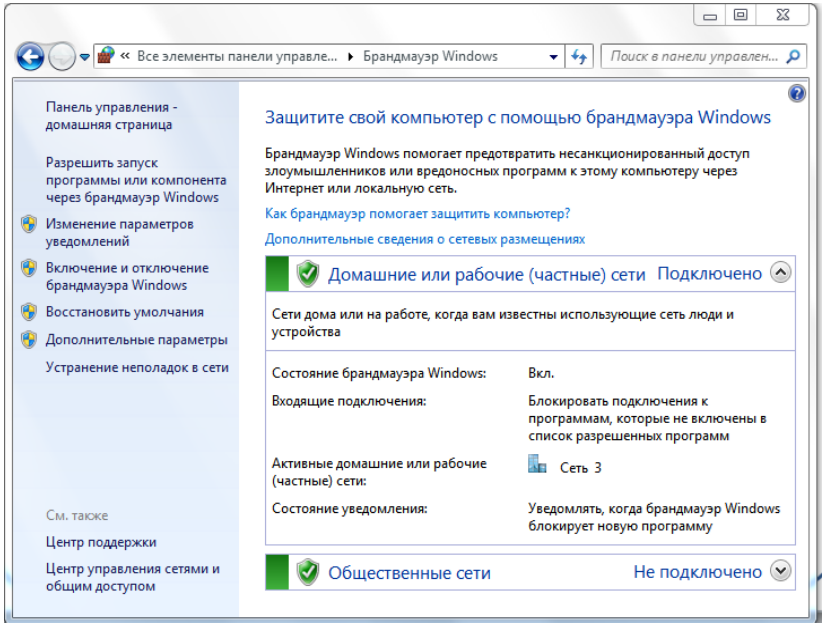
# Брандмауери

Для запобігання інтернет-загрозам між комп'ютером і мережею встановлюють перешкоди — міжмережеві екрани (нім. *Brandmauer*, англ. *Firewall* — вогнестійка стіна»).

**Брандмауер** — це технічний пристрій (маршрутизатор, роутер тощо) або програмний засіб для контролю даних, що надходять до комп'ютера через мережу.

Брандмауери захищають комп'ютер від зловмисного проникнення або потрапляння шкідливих програм. Але не запобігають витоку конфіденційної інформації користувача та завантаженню вірусів.

ОС Windows має вбудований персональний брандмауер.




Щоб увімкнути і налаштувати його, слід виконати команди:

**Пуск → Панель керування → брандмауер Windows.**

# *Засоби браузера, призначені для гарантування безпеки*

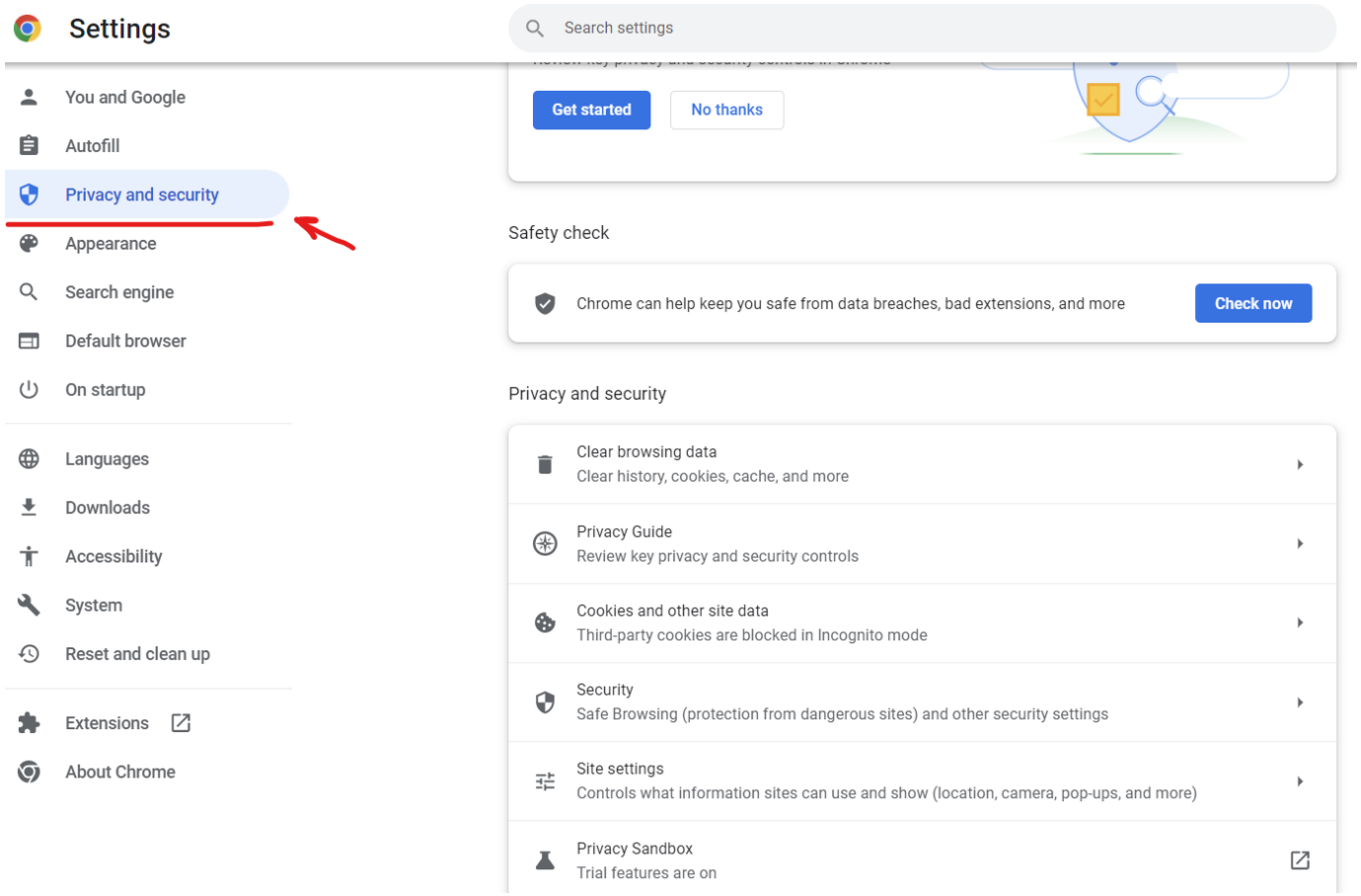
Браузери Mozilla Firefox, Safari, Opera, Google Chrome мають багато вбудованих засобів захисту.

Одним із найпопулярніших браузерів для комп'ютерів, телефонів і планшетів є Google Chrome, який:

- ✓ попереджає про відкриття сайта із загрозою фішингу або шкідливих програм;
- ✓ ізольовано відкриває веб-сторінки, що в разі загрози приводить до закриття лише однієї шкідливої веб-сторінки;
- ✓ дозволяє вимкнути збереження конфіденційних даних;
- ✓ надає можливість налаштувати показ спливних вікон.

# Браузер Google Chrome

Для налаштування засобів безпеки в браузері необхідно відкрити меню браузера за допомогою інструмента в правій частині вікна та обрати вказівку *Налаштування*. У вікні, що відкриється, слід обрати пункт Приватність та безпека.



Для уникнення ризиків, пов'язаних з роботою в Інтернеті, варто дотримуватися таких порад:

***Не розміщуйте в Інтернеті:***

- ✓ домашню адресу, номер телефона (як домашнього так і мобільного);
- ✓ розпорядок дня (свій або рідних);
- ✓ повідомлення про можливі тривалі подорожі або виїзд;
- ✓ фото, що можуть скомпрометувати вас або ваших знайомих тощо;

***Не надавайте незнайомим людям*** та не надсилайте через відкриті мережі персональні дані, дані про паролі доступу до поштових скриньок, екаунтів у соціальних мережах;

**Нікому і ніколи не повідомляйте особисту фінансову інформацію.**

***Суворо конфіденційні дані:***

- **Термін дії картки**
- **CVV-2 код**
- **PIN-код**

***Для переказу коштів достатньо:***

- **Імені власника картки**
- **Номеру картки**

# Уважно поводьтеся з паролями.

*Для створення паролів використовуйте:*

- **Складне слово чи вислів**
- **Великі і маленькі літери**
- **цифри**

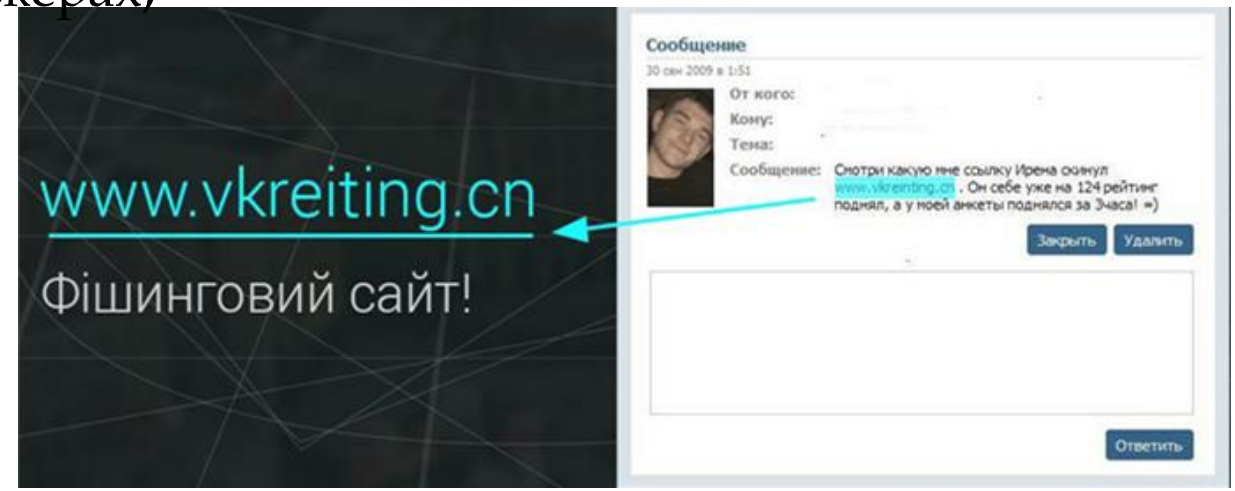
*Змінюйте паролі:*

- **Для нових акаунтів**
- **Періодично (раз на 3-6 міс.)**
- **У разі підозрілих ситуацій**

Привяжіть номер мобільного телефону до важливих акаунтів (двохфакторна авторизація)

***Не відкривайте*** вкладень до листів від незнайомих осіб;

Уважно ставтесь до посилань в повідомленях у соц. мережах та інших месенджерах;



***Не надсилайте*** СМС-повідомлення для отримання будь-яких послуг в Інтернеті;

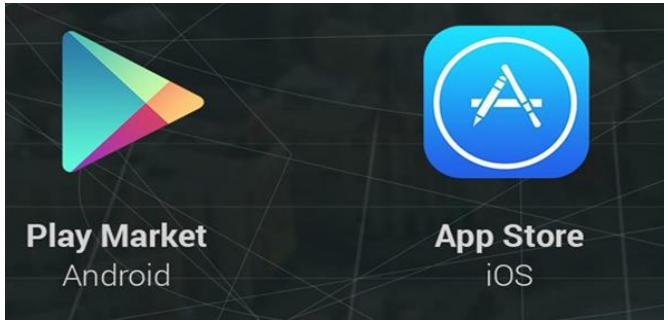
Використовуйте **окрему картку** для інтернет оплат;

Користуйтеся лише знайомими банкоматами, огляньте банкомат перед використанням;

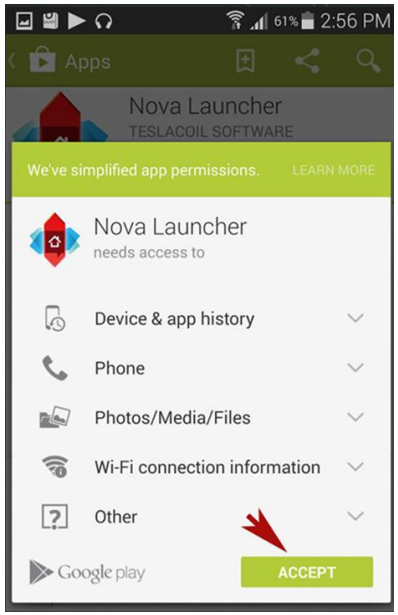
**Уважність** – практично єдиний спосіб захисту від скімінгу.

Всі вищезгадані поради стосуються і мобільних пристроїв (смартфонів, планшетів).

1. Встановлюйте мобільні додатки лише з офіційних магазинів.




2. Періодично перевіряйте ваші мобільні пристрої на предмет незнайомих додатків на головному екрані та в меню.




3. При встановленні та оновленні додатків уважно стежте за тим, які **дозволи вони вимагають**.

# Додаткові матеріали:

- Основні правила кібергігієни


- 31 days of cybersecurity awareness

# Дякую за увагу!