Мукачівський ліцей №6 Мукачівської міської ради

Безпека в інтернеті

Як уникнути ризиків у цифровому світі

ДЛЯ УЧНІВ 7–9 КЛАСІВ

Підготував вчитель інформатики
Чекан Крістіан-Юрій Вікторович

ЦИФРОВИЙ СВІТ

Чому це важливо?

Ми щодня користуємось інтернетом для спілкування, ігор, навчання та дозвілля. Цифрові технології стали невід'ємною частиною нашого життя.

Але інтернет — це інструмент, який потребує відповідального використання. Все залежить від того, як ми ним користуємось і які рішення приймаємо онлайн.

Соціальні мережі

Соціальні мережі — частина нашого життя

Сьогодні майже кожен із нас щодня користується соціальними мережами:

- спілкуємося з друзями
- ділимося фото та відео
- читаємо новини та коментарі

Але разом із можливостями **соціальні мережі приховують і небезпеки**:

- фейкові акаунти та шахраї
- фішинг і викрадення особистих даних
- кібербулінг та психологічний тиск
- небезпечні посилання й маніпуляції

Пропоную переглянути коротке відео, яке покаже, чому в інтернеті важливо бути уважними та обачними. (https://youtu.be/xJu-qN0KDcI?si=EguAS0Slkc9Mw913)

Що таке ризики в інтернеті?

Безпека під загрозою

Ситуації, які можуть нашкодити твоїй фізичній або цифровій безпеці

Репутація та образ

Дії, що можуть зіпсувати твою репутацію серед друзів, у школі чи в соцмережах

Фінансові втрати

Шахрайство, яке може призвести до втрати грошей — твоїх або батьків

Психологічний вплив

Контент або ситуації, що негативно впливають на настрій, самооцінку та психічне здоров'я

Основні види ризиків

Кібербулінг

Цькування, образи та приниження в онлайн-просторі

Шахрайство

Спроби викрасти твої дані або гроші через обман

Небезпечний контент

Інформація, яка може шкодити або вводити в оману

Витік особистих даних

Розголошення приватної інформації без твого контролю

⚠ УВАГА

Кібербулінг: що це таке?

Кібербулінг — це...

- Образи та приниження в коментарях
- Погрози через повідомлення
- Поширення неправдивої інформації
- Створення фейкових сторінок
- Публікація особистих фото без дозволу

Кібербулінг відбувається в соціальних мережах, месенджерах, онлайн-іграх та на форумах. Це систематичне цькування, яке може серйозно вплинути на самооцінку та психологічний стан.

На відміну від звичайного булінгу, кібербулінг може тривати 24/7 і досягти дуже широкої аудиторії за лічені хвилини.

Шахрайство в інтернеті

Просять пароль

Запитують твій пароль або код підтвердження.

Повідомлення про виграш

Повідомляють про незапланований приз або лотерею.

Невідкладні дії

Тиснуть діяти терміново, щоб налякати тебе.

Підозрілі посилання

Посилання ведуть на незнайомі або підроблені сайти.

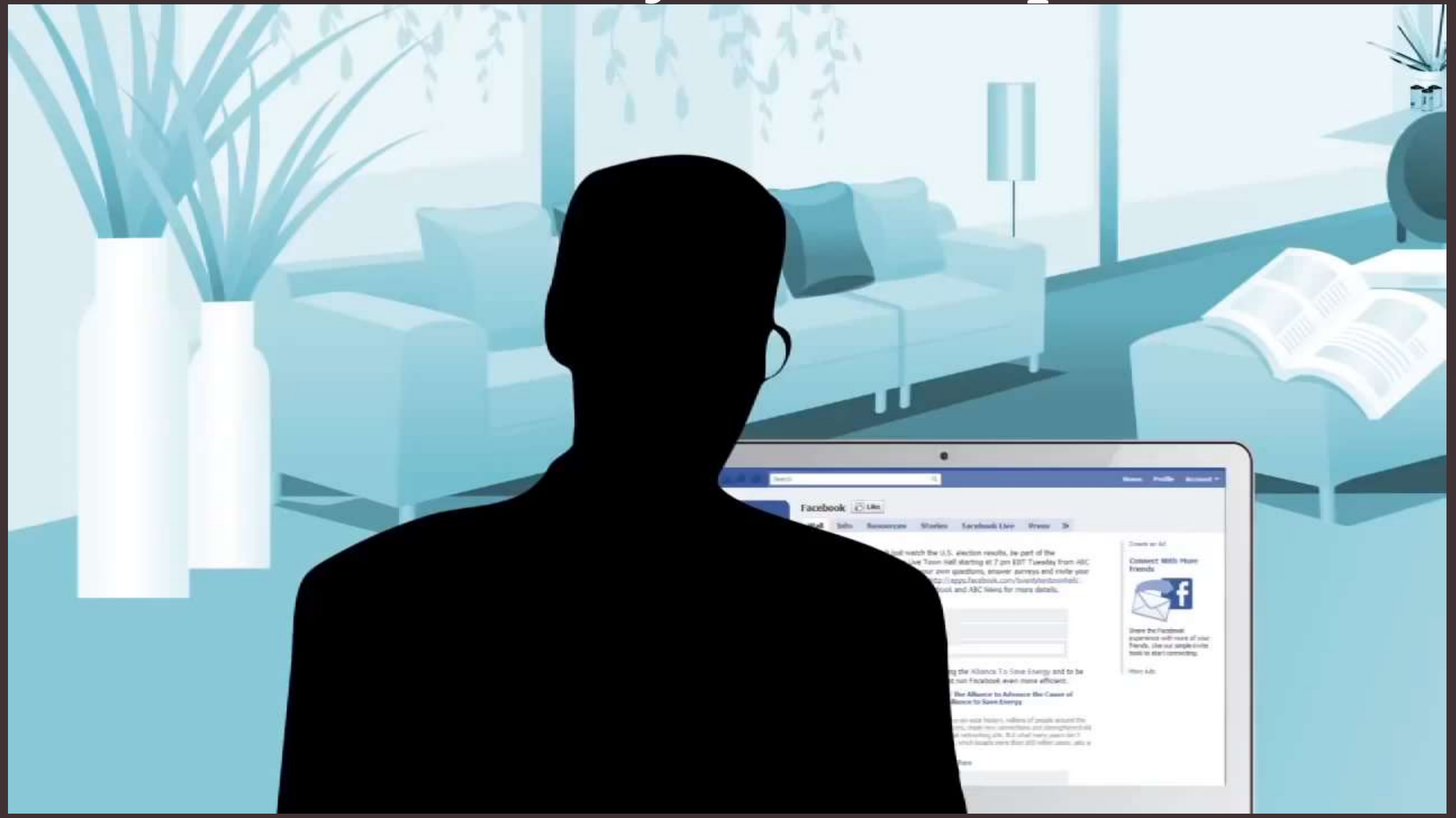
Шахраї використовують різні тактики, щоб отримати доступ до твоїх облікових записів або грошей.

Ознаки шахрайства:

- Просять пароль, код підтвердження або банківські дані
- Повідомляють про виграш у конкурсі, в якому ти не брав участі
- Вимагають термінових дій ("до кінця дня", "зараз або ніколи")
- Надсилають підозрілі посилання з помилками в адресі

> **Золоте правило:** Ніхто — ні друзі, ні банк, ні підтримка сервісу — не має права просити твій пароль.

10 способів захисту від шахрайства

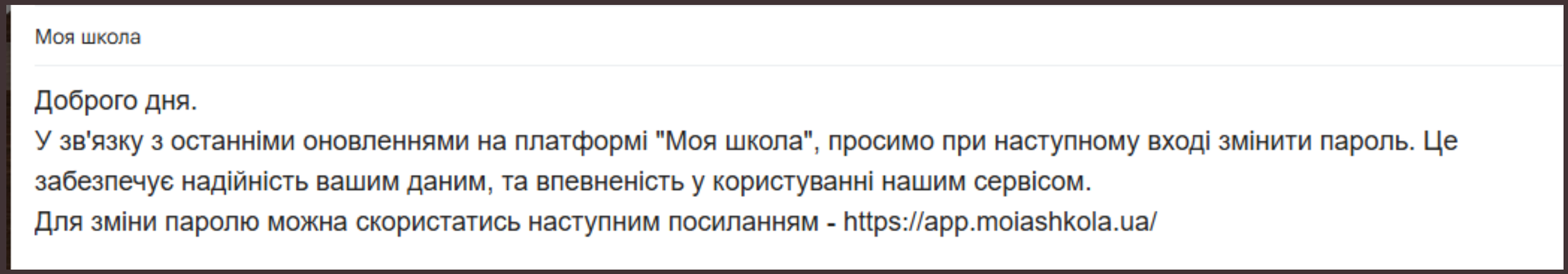


https://youtu.be/YgB7pT09z20?si=6uutL5lPZMoxA3qv

Фішинг

Увага!

Наступний приклад демонструється **виключно з навчальною метою** для ознайомлення з принципами роботи фішингу.



Небезпечний контент

Сцени насильства

Відео та зображення жорстокості, які можуть травмувати психіку

Небезпечні челенджі

Виклики, що загрожують здоров'ю або життю

Фейкова інформація

Неправдиві новини та маніпуляції, які вводять в оману

Такий контент може викликати страх, стрес, тривогу і призвести до неправильних рішень. Важливо критично оцінювати те, що ти бачиш онлайн, та перевіряти інформацію з надійних джерел.

КОНФІДЕНЦІЙНІСТЬ

Особиста інформація

Що належить до особистих даних?

Номер телефону
Може бути використаний для спаму та шахрайства

Домашня адреса
Дозволяє дізнатися, де ти живеш

Особисті фото
Можуть бути використані не за призначенням

Паролі та коди
Ключі до всіх твоїх облікових записів

Запам'ятай!

Це те, що НЕ можна публікувати бездумно або ділитися з незнайомими людьми.

Раз опублікована інформація може залишитися в інтернеті назавжди.

Як захистити себе онлайн?

Складні паролі

Використовуй комбінацію літер, цифр та спецсимволів. Мінімум 8-10 символів.

Унікальні паролі

Для кожного сервісу — окремий пароль. Якщо один зламають, інші залишаться захищеними.

Закриті профілі

Налаштуй приватність так, щоб твої пости бачили лише довірені люди.

Обережність із незнайомцями

Не додавай у друзі людей, яких не знаєш у реальному житті.

Захист починається з тебе!

Пам'ятай: інтернет все запам'ятовує

Думай перед публікацією

Постав собі запитання: "Чи хотів би я, щоб це побачили через 5 років? Чи не соромно мені буде за це?"

Зупинись
Подумай перед публікацією

Оціни
Чи може це комусь нашкодити?

Прийми рішення
Публікувати чи ні?

Те, що потрапляє в інтернет, залишається там назавжди — навіть після видалення. Скріншоти, репости та копії можуть існувати роками.

Якщо проблема вже сталася

Алгоритм дій

01 Не відповідай

Припини будь-яке спілкування з кривдником

02 Зроби скріншоти

Збережи докази: повідомлення, коментарі, посилання

03 Заблокуй

Обмеж доступ кривдника до свого профілю

04 Розкажи дорослому

Зверніться до батьків, вчителя або психолога

Діяти швидко і правильно — це захистити себе та інших.

Допомога — це нормально

Батьки

Вони найбільше турбуються про тебе і завжди готові підтримати

Вчителі

Мають досвід і можуть допомогти розібратися в ситуації

Шкільний психолог

Професійна підтримка в складних емоційних моментах

> **Просити допомогу — не соромно.** Це ознака розуму і турботи про себе. Ти не один — поруч завжди є люди, які готові підтримати.