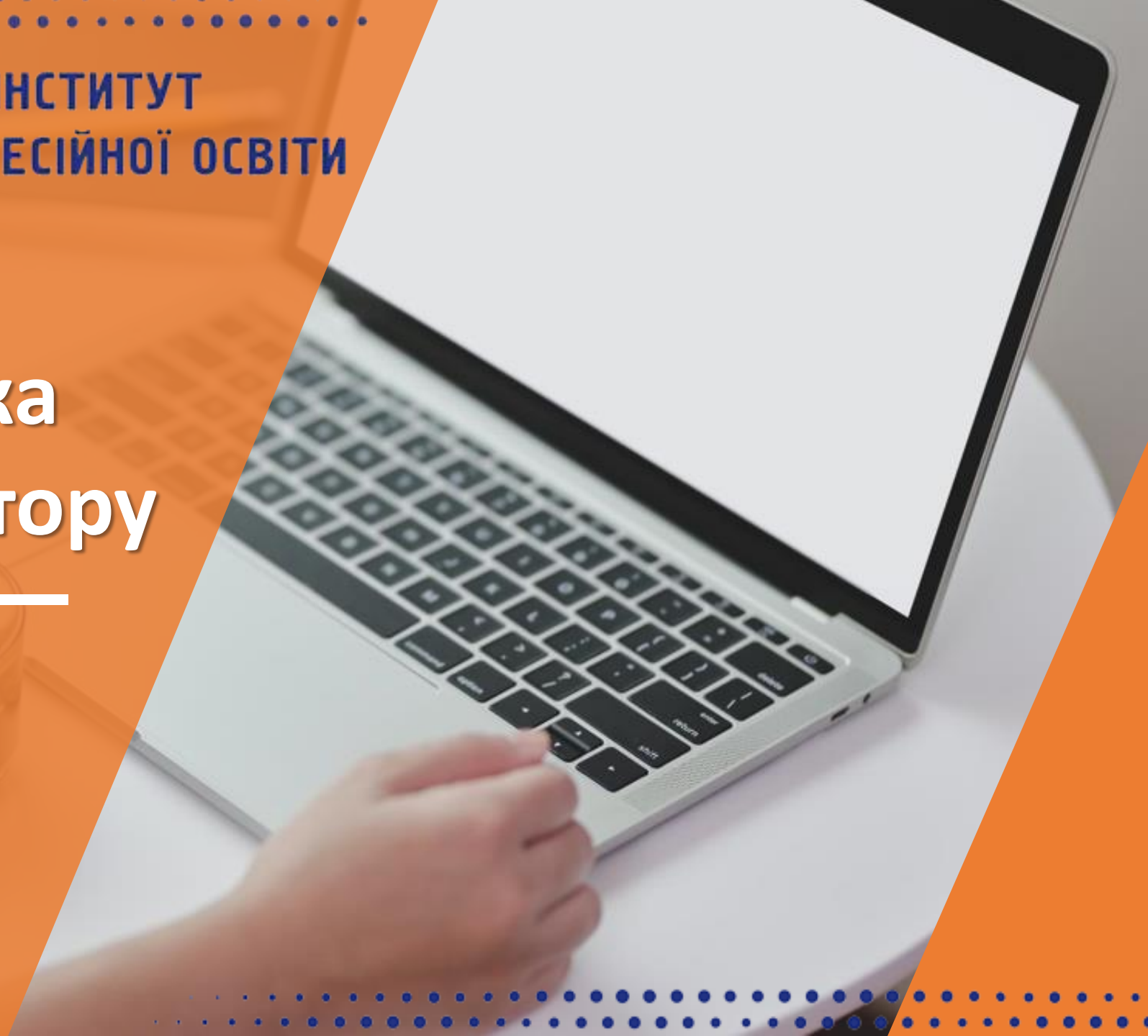
БІЛОЦЕРКІВСЬКИЙ ІНСТИТУТ
НЕПЕРЕРВНОЇ ПРОФЕСІЙНОЇ ОСВІТИ

Цифрова безпека освітнього простору

МАРАФОН БЕЗПЕКИ

Ірина Гончарова,
старша викладачка кафедри технологій навчання, охорони праці та дизайну



Хакерські атаки у світі

https://www.slovoidilo.ua/2021/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-xakerskyx-vijnax

Держспецзв'язку

❗ Російські хакери продовжують атакувати українську інфраструктуру, не гребуючи цивільними цілями

У І півріччі 2022 року Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, зафіксовано 1 350 кібератак.

✓ Галузі, які найбільше атакували російські хакери:

- Державні та місцеві органи влади
- Сектор безпеки та оборони
- Енергетичний сектор
- Фінансовий сектор
- Комерційний сектор
- Телеком-сектор і розробники
- Транспортна галузь

УНІАН
ІНФОРМАЦІЙНЕ АГЕНТСТВО

✓ Найпоширеніші типи кібератак:

- Шкідливий програмний код
- Втручання
- Спроби втручання
- Порушення вразливостей інформації
- Порушення доступності
- Шкідливий (образливий) вміст
- Відома вразливість
- Шахрайство

https://www.unian.ua/techno/v-ukrajini-za-pivroku-zafiksuvali-ponad-tisyachu-kiberatak-11900298.html

Поняття кібербезпеки

Cyber Security - забезпечення захисту даних

Електронна інформаційна мережа використовується для збору, обробки, зберігання та обміну великою кількістю цифрової інформації.

Кібербезпека – це сукупність технічних і соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз і впливів з небажаними наслідками, що походять від інтернет-середовища.

З початку 2022 року число виявлених кіберзагроз зросло на 20%, зокрема збільшилась кількість шпигунських програм та спам-листів!

Онлайн (online)-ідентифікація. Захист особистих даних

Чим більше часу ви проводите в Інтернеті, тим сильніше на ваше життя може вплинути ваша ідентичність як в Інтернеті, так і в офлайні.

Онлайн-ідентичність — це те, як ви представляєте себе іншим в Інтернеті.

Відповідно до Закону України «Про захист персональних даних»:

Персональні дані — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Незаконне отримання та оприлюднення (поширення) чужої особистої інформації є злочином.

Безпечне користування електронною поштою

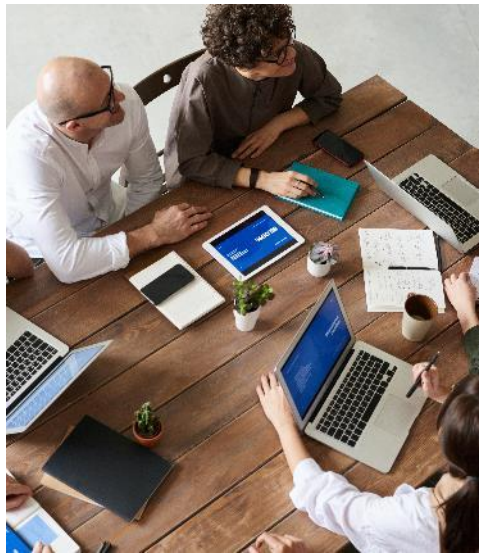
1

Особиста пошта

– зберігається на серверах компанії, яка надає послуги поштового сервісу;

– містить вашу приватну інформацію;

– використовується для реєстрації у соціальних мережах та на інших ресурсах.



2

Службова пошта

– показує вашу належність до організації – (vasyl@me.gov.ua);

– дані зберігаються на серверах вашої установи і адмініструються адміністратором закладу освіти;

– містить конфіденційну інформацію, яка стосується вашої організації.

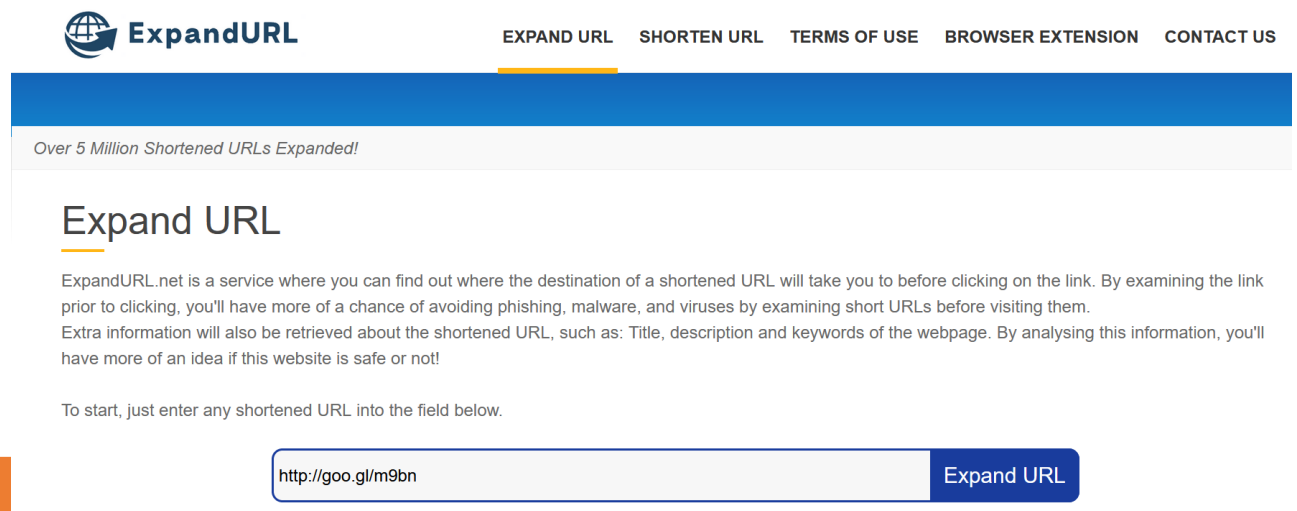
Безпечне користування електронною поштою

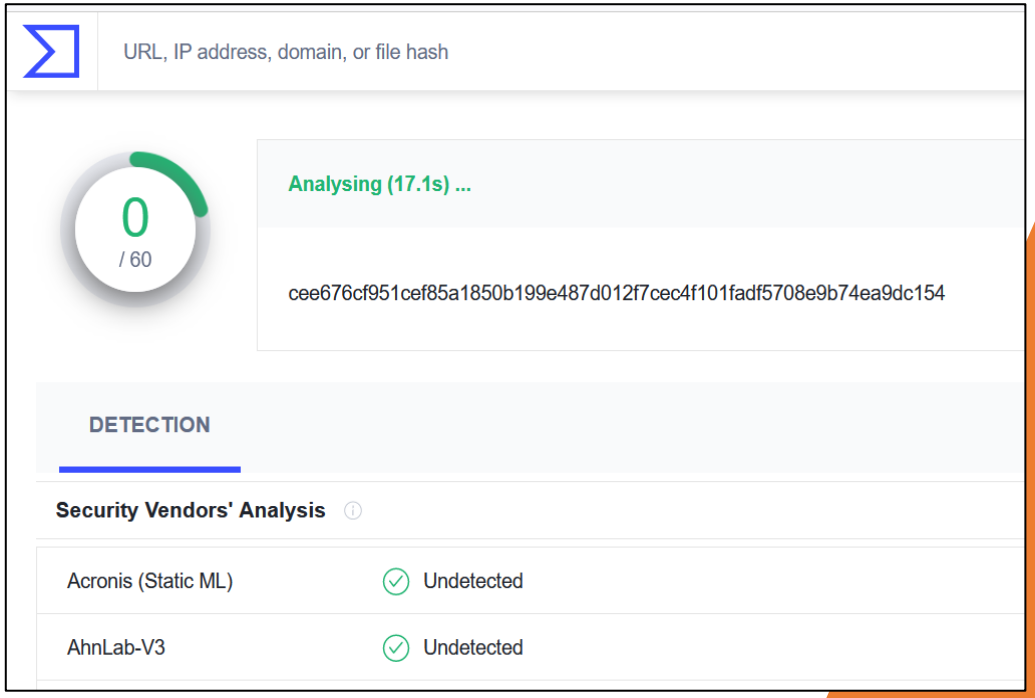
Приклад поганого паролю: rockandroll123
Приклад надійного паролю: T@8l3S0bk4hA7

https://virustotal.com сервіс для сканування файлу 50-ма антивірусними програмами

скорочені посилання (https://bit.ly/xxxxx) перевіряйте їх за допомогою сервісу

https://www.expandurl.net/



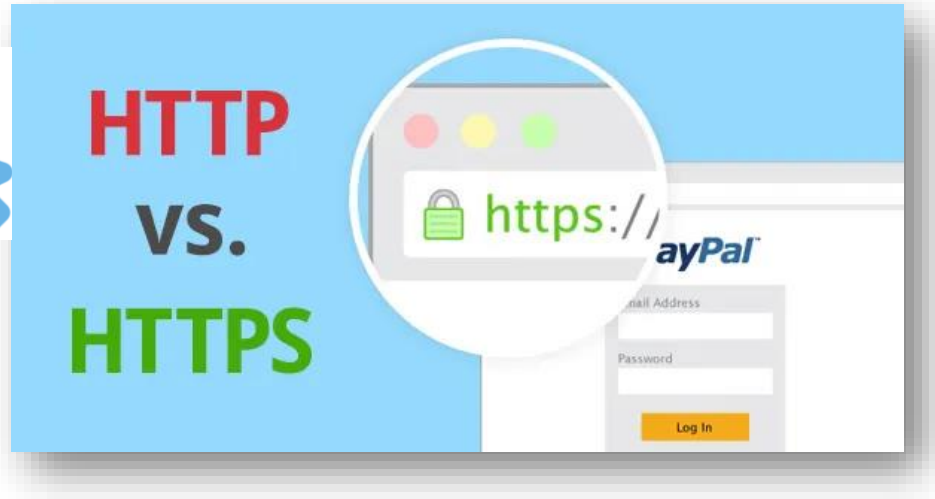


Безпечний інтернет

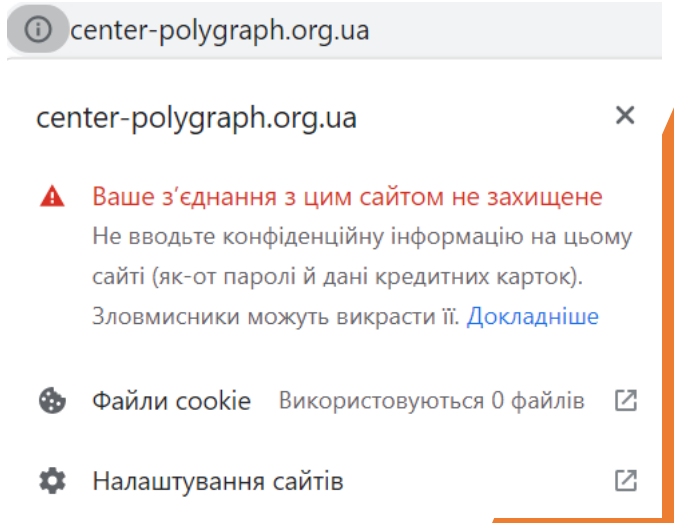
Браузер, Web browser – спеціальна програма, призначена для перегляду веб-сайтів

Для передачі використовується протокол HTTP або його безпечніша версія HTTPS.

безпечне з’єднання



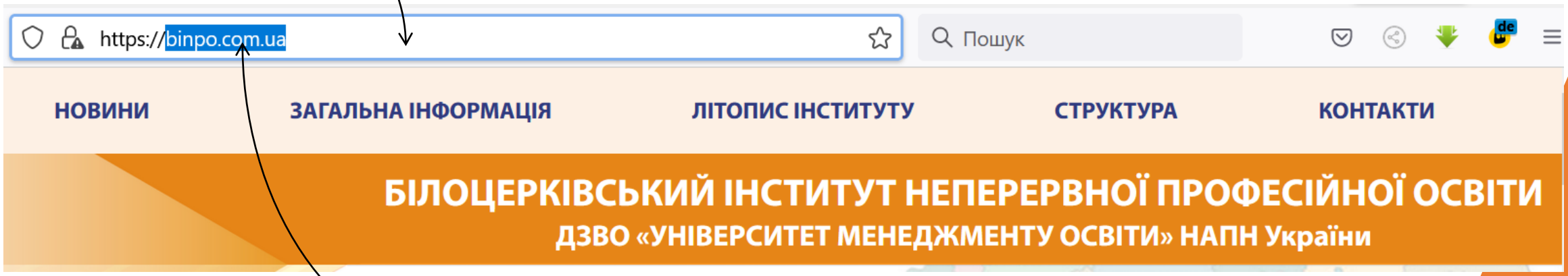
небезпечне з’єднання



Протокол – це набір правил передачі файлів (тексту, зображень, відео тощо) через мережу «Інтернет».

Безпечний інтернет

АДРЕСНИЙ РЯДОК
спеціальне поле, в якому вводяться адреси інтернет ресурсів; місце, куди ми вводимо доменне ім’я/домен



ДОМЕН
ім’я сайту

Важливо!!! ***accounts.google.com.evilwebsite.pe/EditPasswd***
шахрайське посилання, бо адреса має починатися з **accounts.google.com/**
(тобто, після.com мусить бути /, а не крапка).

Cookie

Cookie – це невеликі текстові файли, які зберігаються в комп’ютері під час відвідування певних веб-сторінок

- спрощують роботу в Інтернеті, зберігаючи потрібну інформацію;
- за допомогою файлів cookie сайти можуть запам'ятовувати ваш вхід в обліковий запис чи ваші уподобання, а також надавати вам персоналізований контент;
- файли cookie використовують статистику про перегляд сторінок та показу цільових оголошень.

Тимчасові

Постійні

Чому через браузер можуть реалізовуватись загрози?

– Браузери застарівають та з’являються вразливості, які експлуатуються хакерами віддалено.

– Хакери зламують легітимні сайти та розміщують на них шкідливий код та програми, і Ви можете навіть не знати про те, що стали жертвою.

– Зловмисники зламують публічні точки доступу до мережі «Інтернет» і намагаються перехопити інформацію користувачів.

Плагіни безпеки

Плагін – це програма, що розширює функції браузера, полегшує користування мережею

HTTPS Everywhere – попереджає про незахищене з'єднання. Це вільне і відкрите розширення для браузерів Google Chrome, Mozilla Firefox і Opera

AdGuard AdBlocker – Антибанер Adguard ефективно блокує всі види реклами на всіх веб-сторінках, навіть в Facebook, Вконтакте, на YouTube та інших вебсайтах!

Поради для безпеки у мережі Інтернет

01

Оновлюйте браузер та встановлені плагіни

02

Відвідуйте лише безпечні сайти з використанням протоколу HTTPS

03

Не завантажуйте підозрілі програми чи файли

04

Використовуйте надійні паролі

05

Використовуйте багатофакторну автентифікацію

06

Застосовуйте VPN від надійного провайдера

07

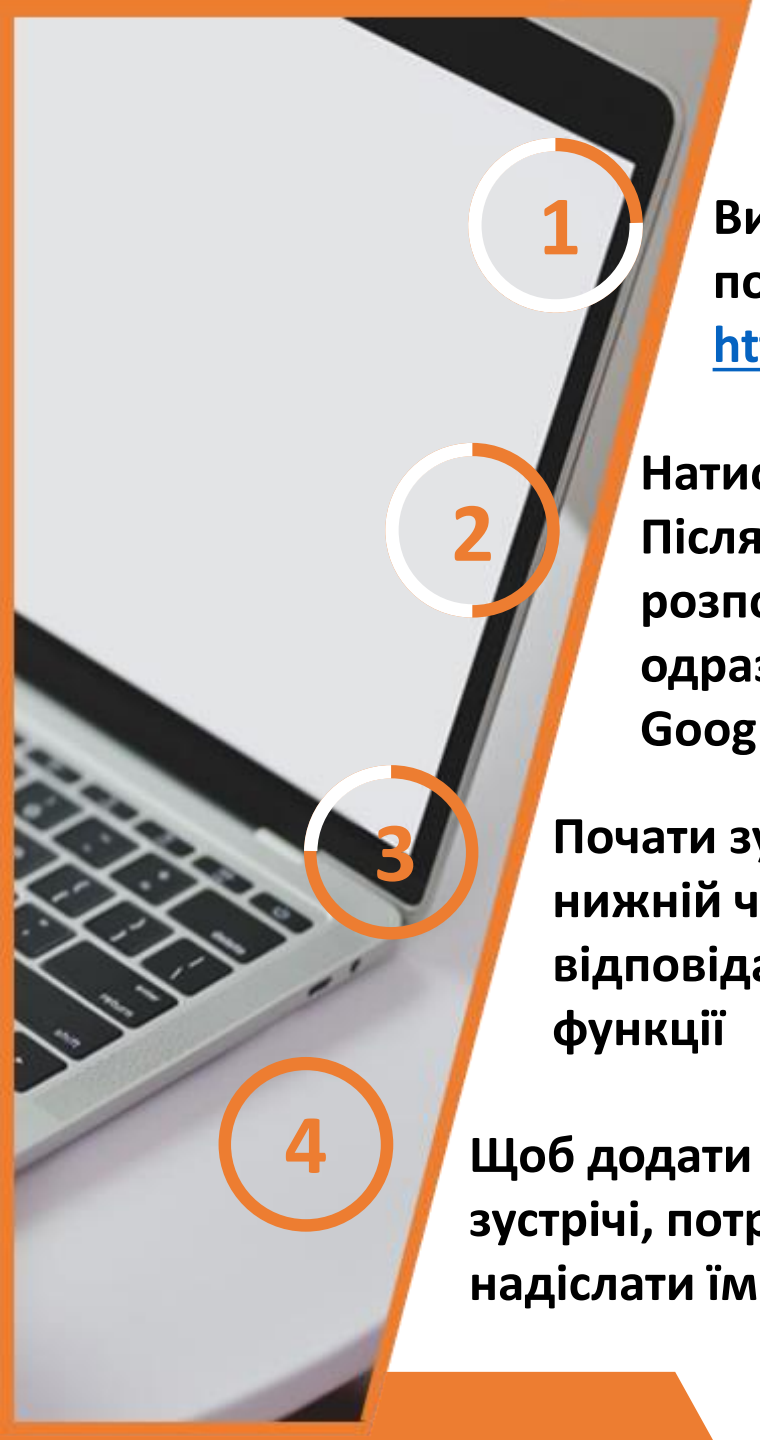
Вимкніть автоматичне збереження пароля в браузері

08

Використовуйте параметри приватного перегляду, щоб запобігти відстеженню файлів cookie

09

Використовуйте перевірені Wi-Fi мережі



Google Meet

1

Використовуйте офіційне послання https://meet.google.com/

2

Натиснути Нова зустріч. Після цього можна розпочинати конференцію одразу або спланувати у Google календарі

3

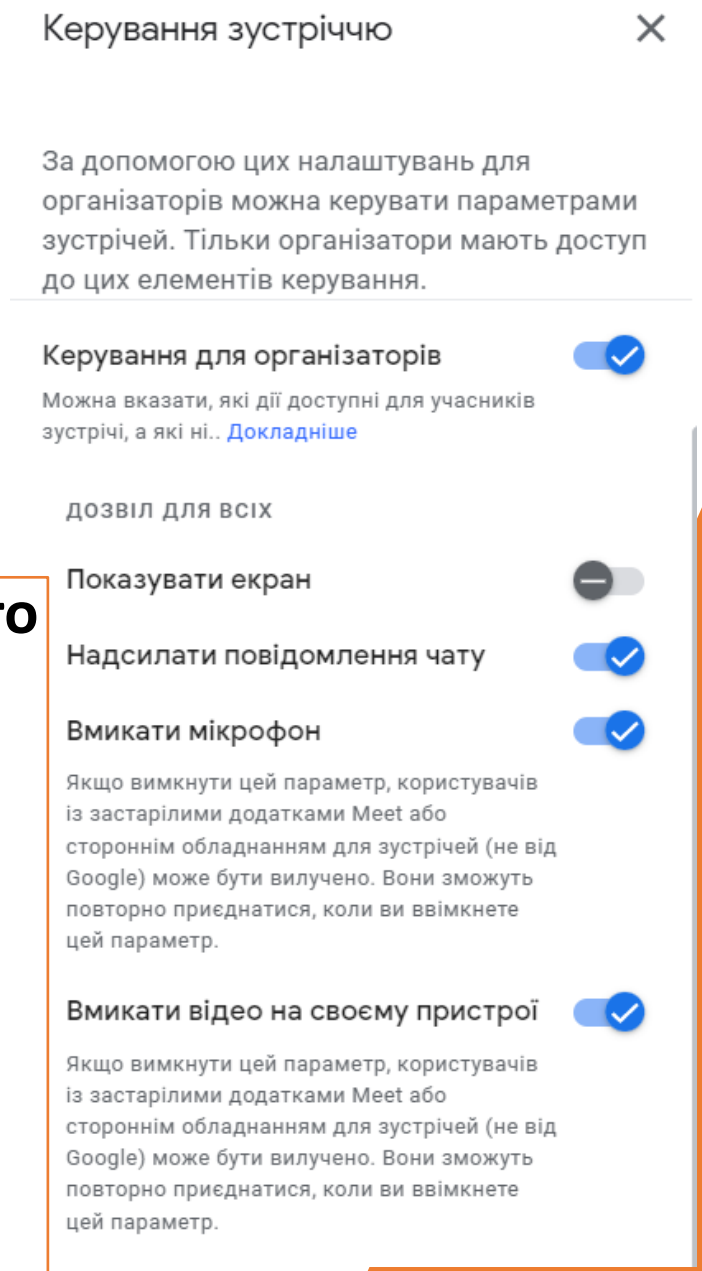
Почати зустріч. Кнопки в нижній частині екрана відповідають за відповідні функції

4

Щоб додати людей до зустрічі, потрібно надіслати їм запрошення

Інструкція з безпечного використання

- Реальні імена
- Список електронних пошт
- Ненадання посилання іншим
- Налаштування зустрічі правильно



Microsoft Teams

Зареєструватись в MS Office 365

Увійти в свій обліковий запис

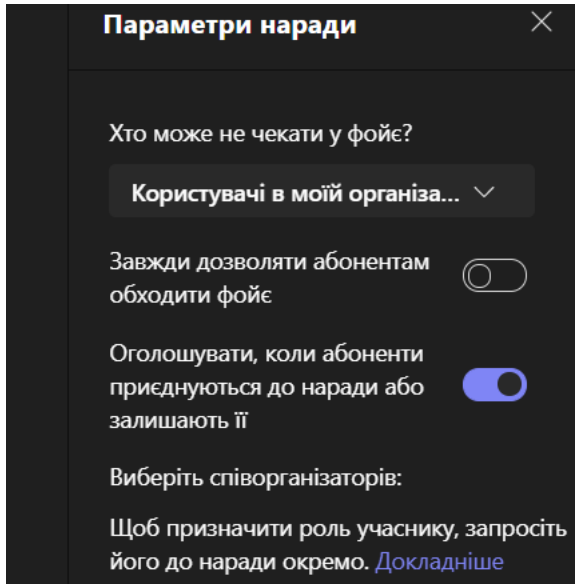
Завантажити та встановити програму MS Teams з офіційного сайту MS Office 365

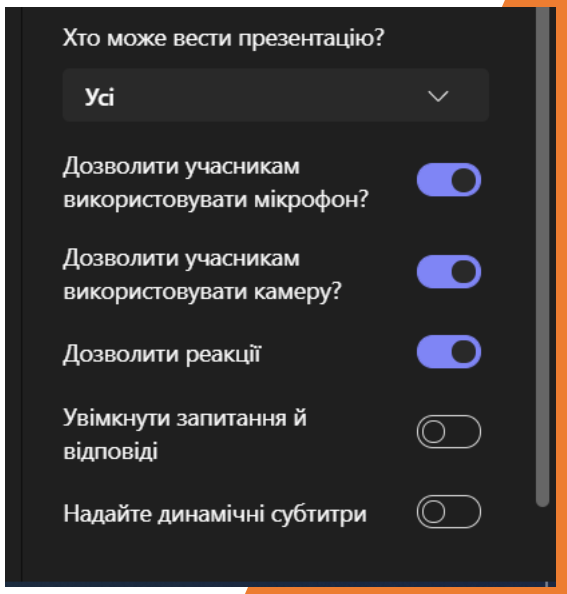
Після інсталяції ввести свій аккаунт MS Office 365

Інструкція з безпечного використання

- Реальні імена
- Список електронних пошт
- Ненадання посилання іншим
- «Очікування у фойє». Першим заходить організатор. Презентацію веде організатор

Інтерфейс програми





Zoom

Зареєструватись в Zoom
https://zoom.us/

Завантажити та встановити програму Zoom з офіційного сайту
https://zoom.us/download

Увійти в свій обліковий запис

Натиснути Нова зустріч. Після цього можна розпочинати конференцію одразу або спланувати у Google календарі

Інструкція з безпечного використання

- Реальні імена
- Список електронних пошт
- «Зачиніть двері», коли всі на місці
- Ненадання посилання та паролю іншим
- «Очікування у залі». Першим заходить організатор. Презентацію веде організатор