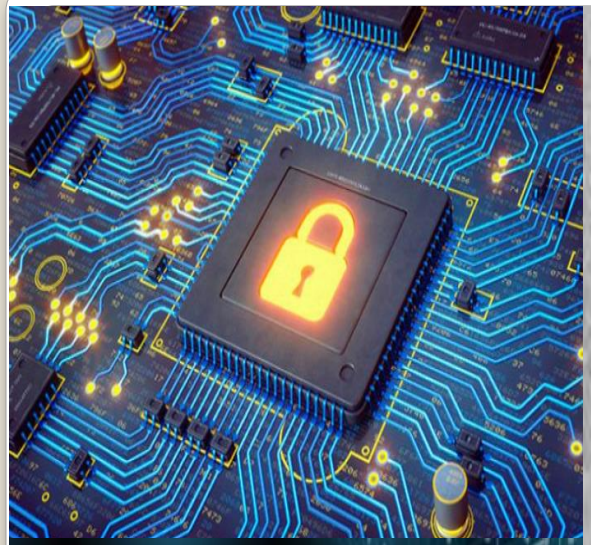


Я. БЕЗПЕКА.

КІБЕРПРОСТІР

КІБЕРГІГІЄНА
під час війни

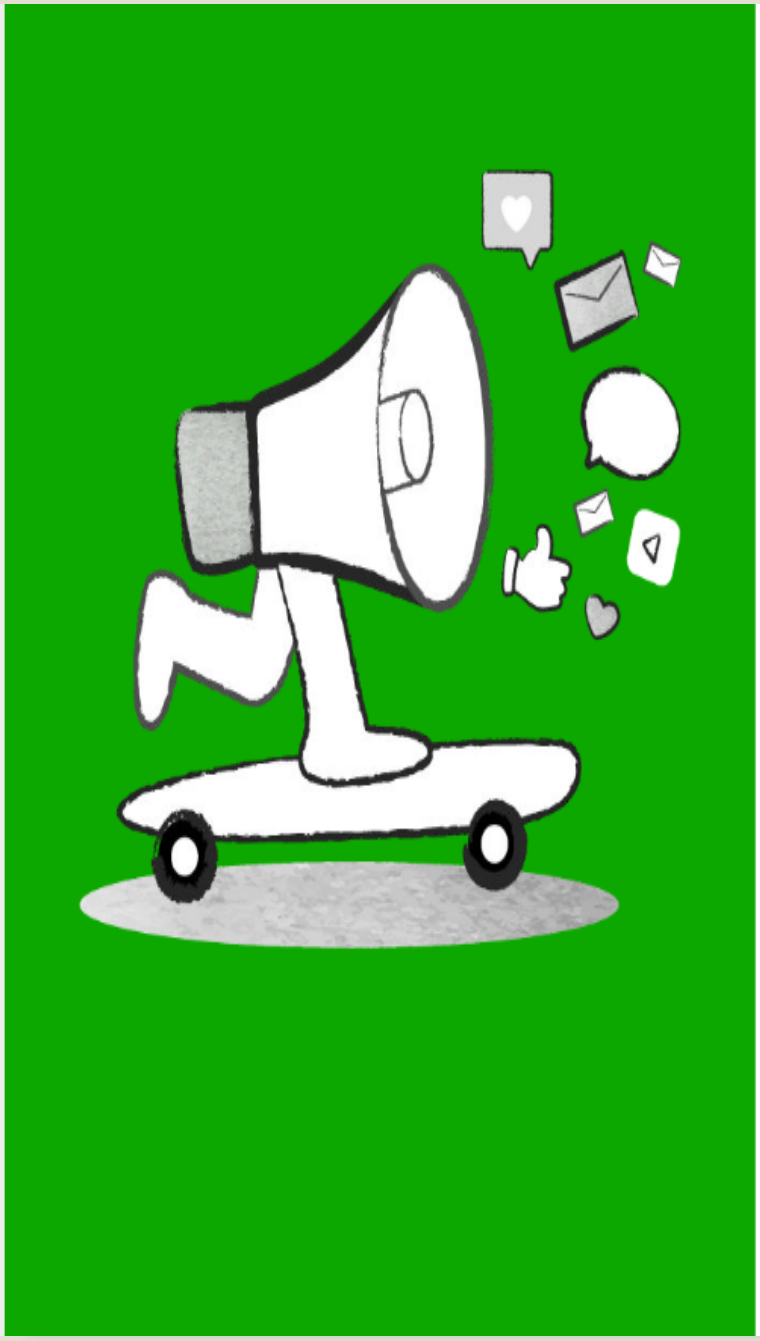
Безпека – це сукупність елементів та зв’язків між ними.
Цими елементами є ми, а зв’язками – наші знання про них.
Ігор Ярич

Персональні та корпоративні дані, їх конфіденційність

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

Персональні дані:

- ім'я, по батькові, прізвище;
- адреса;
- номери телефонів;
- паспортні дані;
- національність;
- освіта;
- сімейний стан;
- релігійні та світоглядні переконання;
- стан здоров'я;
- матеріальний стан;
- дата й місце народження;
- місце проживання та перебування тощо.



Персональні та корпоративні дані, їх конфіденційність

Згода суб'єкта персональних даних — добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

У сфері **електронної комерції** згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-комунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу
на обробку своїх персональних даних.

(***Закон України «Про захист персональних даних»***)

Персональні та корпоративні дані, їх конфіденційність

Обробка персональних даних — будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

(Закон України «Про Захист персональних даних»)

Що таке «база персональних даних»?

База персональних даних є впорядкованою сукупністю логічно пов'язаних даних про фізичних осіб:

- що зберігаються та обробляються відповідним програмним забезпеченням, є базою персональних даних в електронній формі;
- що зберігаються та обробляються на паперових носіях інформації, є базою персональних даних у формі картотек.

Персональні дані одночасно можуть бути упорядковані і в електронній формі, і у формі картотек (ст. 2 Закону)

Як захистити персональні дані?

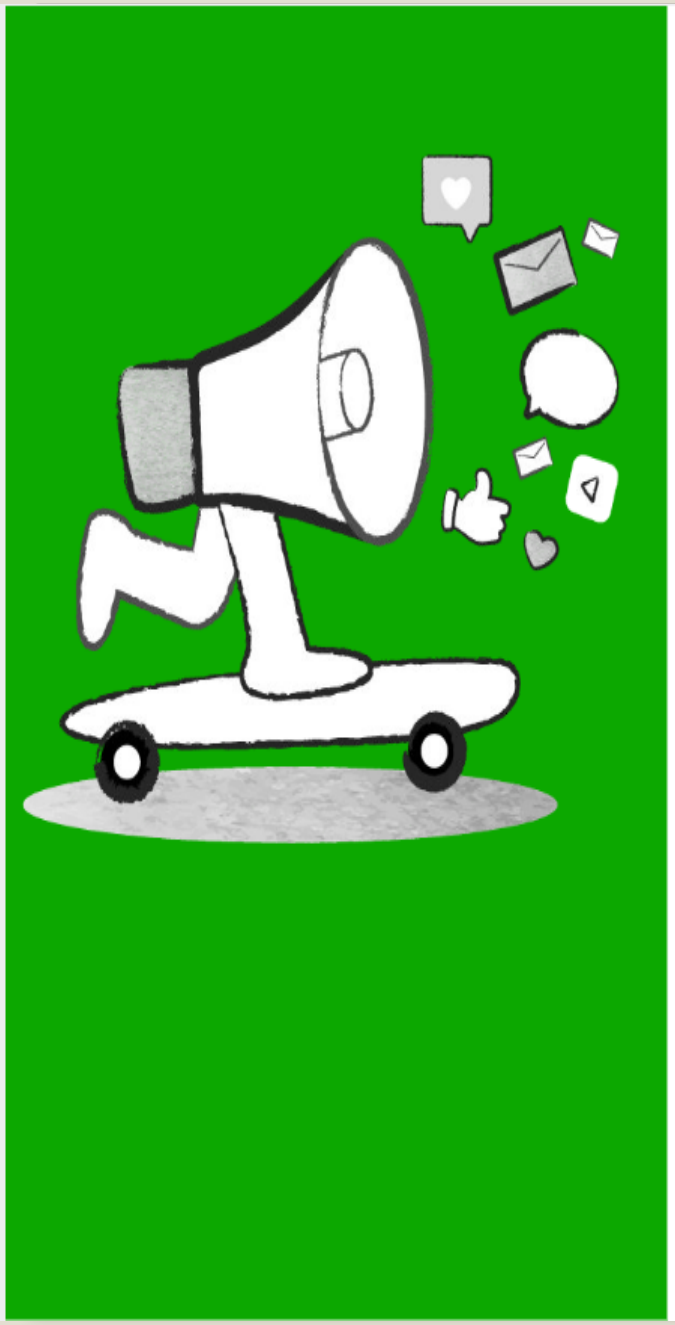
1) Не зберігати відскановані копії документів (паспорт, ідентифікаційний код, свідоцтво про народження тощо) у хмарних сховищах (Dropbox, Google Drive тощо), на пошті чи у відкритих мережевих папках на комп'ютері.

2) Не залишати оригінали чи копії таких документів без нагляду, зберігати їх удома в надійному місці.

3) Надаючи особисті дані в мережі інтернет, звернути увагу на символ замку в лівій частині адресного рядка: якщо він не зелений, а червоний
чи жовтий, це може означати, що сайт ненадійний, тому подумайте, перш ніж залишати важливу інформацію на такому сайті.

Статус безпеки сайту буде зазначено ліворуч від вебадреси

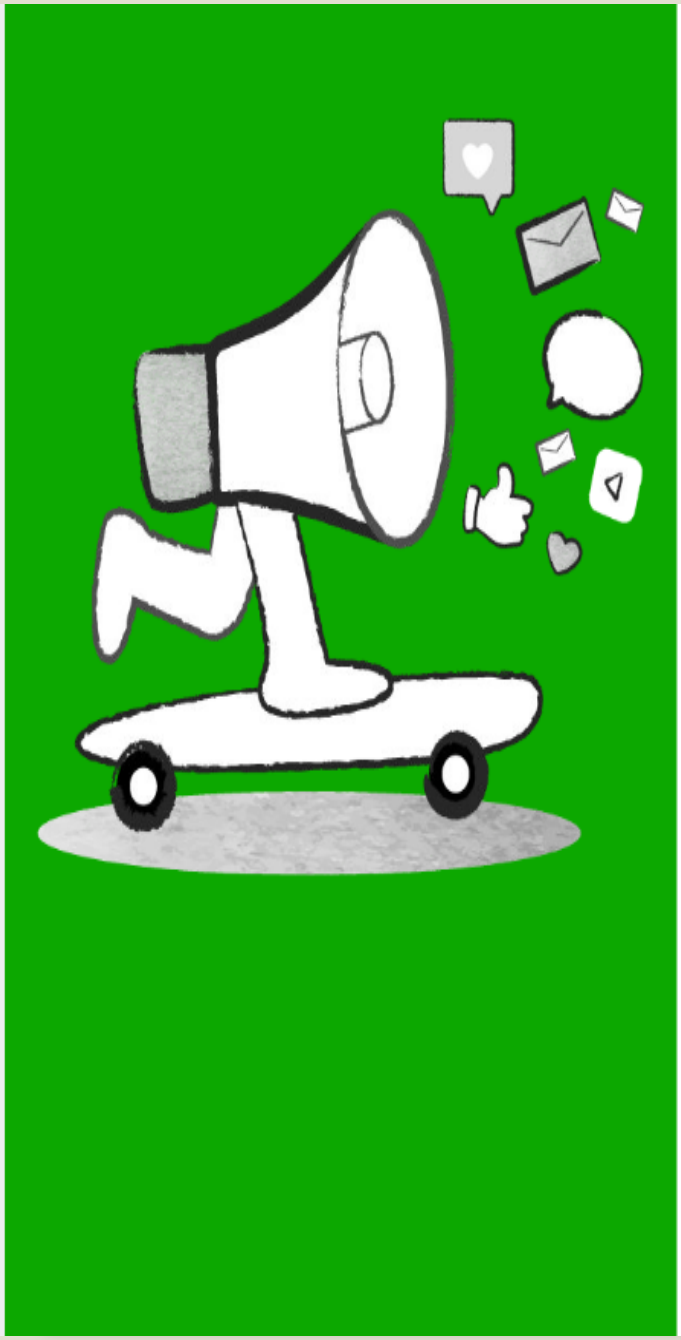
- З'єднання безпечне
- Є додаткова інформація або з'єднання незахищене
- З'єднання незахищене або небезпечне



Корпоративні дані, їх конфіденційність

Корпоративні дані — це дані, які спільно використовуються співробітниками організації, як правило, між відділами чи географічними регіонами.

Корпоративні дані означають будь-які дані, які зберігаються будь-якою з компаній, включаючи, але не обмежуючись цим, дані, які пов'язані з її фінансами, податками, працівниками, клієнтами, постачальниками та бізнесом.

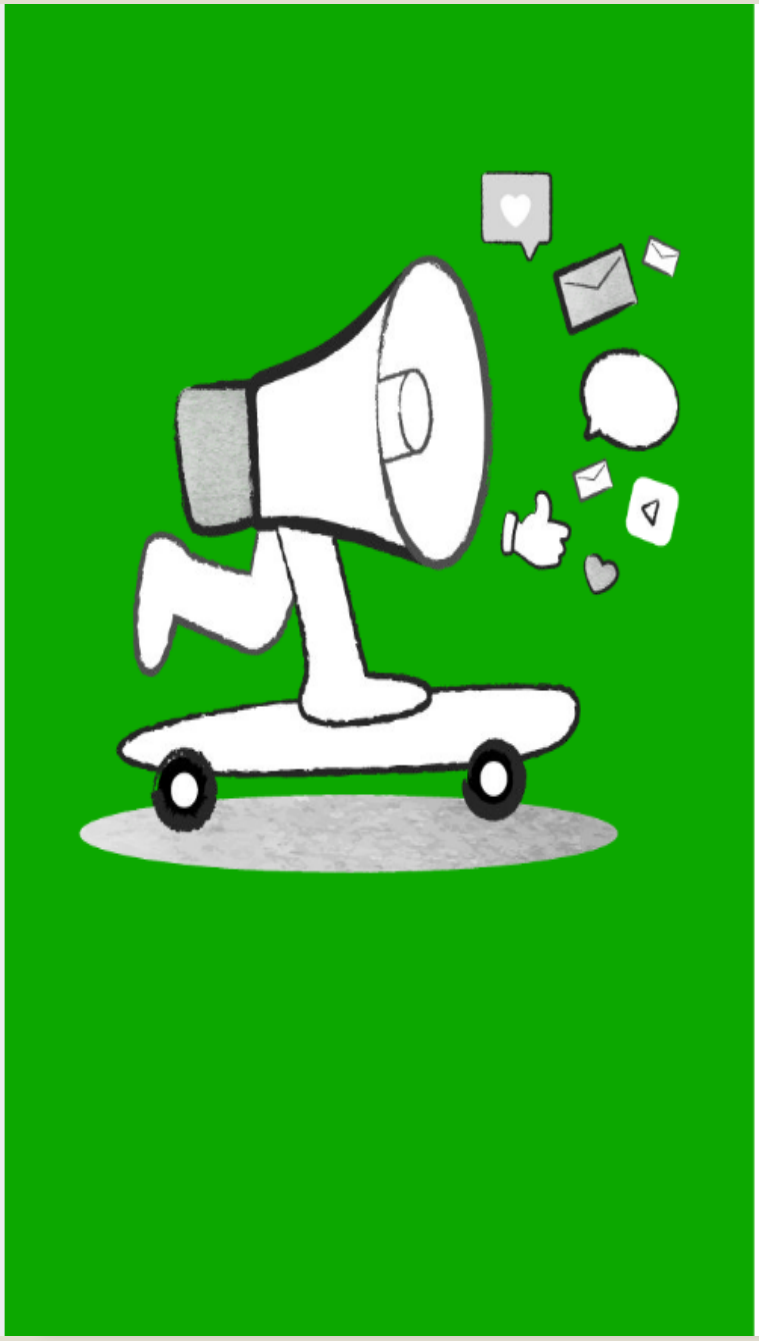


Корпоративна пошта

Корпоративна пошта — це електронна пошта, яку використовують спеціально для певної компанії. Її основна відмінність від особистої пошти — це безпосередньо адреса.

Можливості корпоративної пошти:

- проглядання обговорень;
- автозбереження;
- розвинений список контактів;
- пошук за вмістом листів та прикріплених файлів;
- убудований чат тощо.



Безпека корпоративних пристроїв

- Захист від програм-вимагачів.
- Захист даних за допомогою шифрування.
- Захист акаунтів IT-адміністраторів та власників бізнесу.

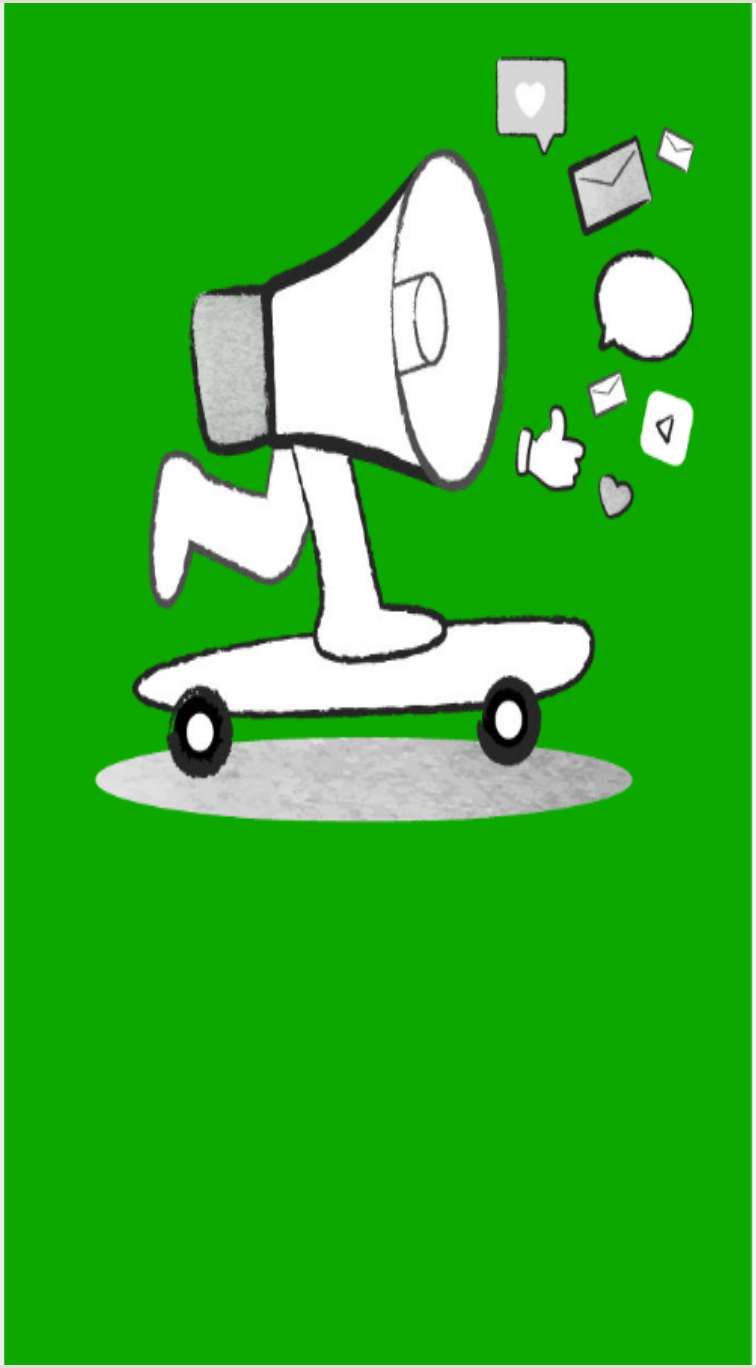
Персональні дані в соціальних мережах та мобільних застосунках

Cookies — це маленькі текстові файли, які зберігаються на вашому комп'ютері, планшеті чи мобільному телефоні. Завдяки cookies сайти можуть збирати інформацію, зокрема про місцезнаходження користувача, про найбільш відвідувані ним сторінки, час перебування на сайті, залишені коментарі, мовні налаштування і навіть про ім’я та фото профілю, якщо така інформація збережена у браузері.

Як видалити всі файли cookie

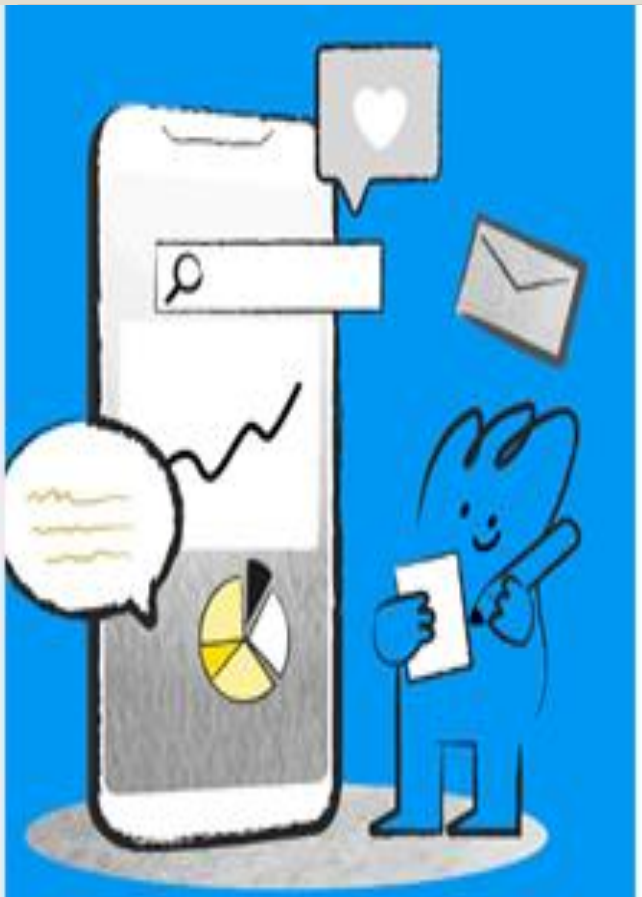
Важливо: якщо видалити файли cookie, ви вийдете з облікового запису на всіх веб-сайтах, а збережені параметри буде видалено.

1. Відкрийте Chrome на комп'ютері.
2. Угорі праворуч натисніть значок ⋮ > Налаштування ⚙.
3. Натисніть **Конфіденційність і безпека** > **Файли cookie й інші дані із сайтів**.
4. Натисніть **Переглянути всі дані сайтів і дозволи** > **Видалити всі дані**.
5. Щоб підтвердити свій вибір, натисніть **Очистити**.



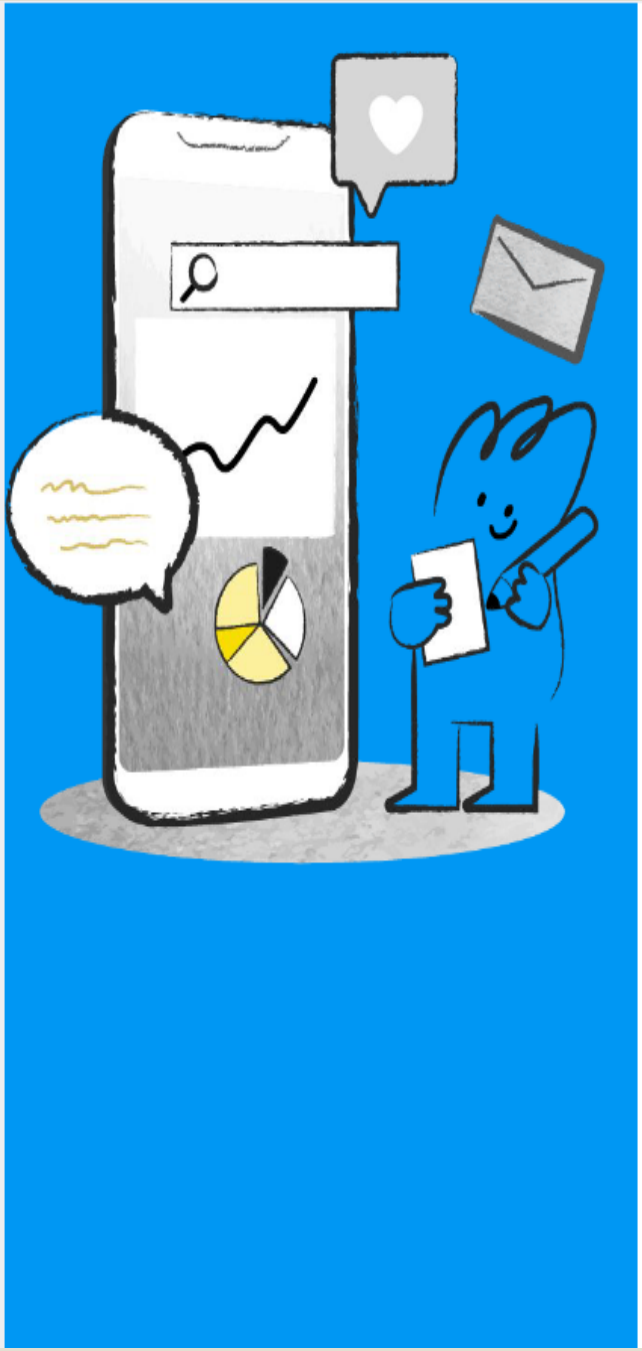
Чи «ховаються» віруси у QR-кодах?

- Скануйте QR-коди тільки з перевірених джерел, утримуйтеся від зчитування QR-кодів, які випадково потрапили вам на очі.
- Якщо QR-код веде на вебсайт, упевніться у правильності написання його адреси.
- Користуйтеся антивірусами, які попередять про небезпеку в разі відкриття файлів із вірусами.
- Будьте особливо обачними, використовуючи QR-код для платежів.
- Звертайте увагу, чи не наклеєний один QR-код поверх іншого.



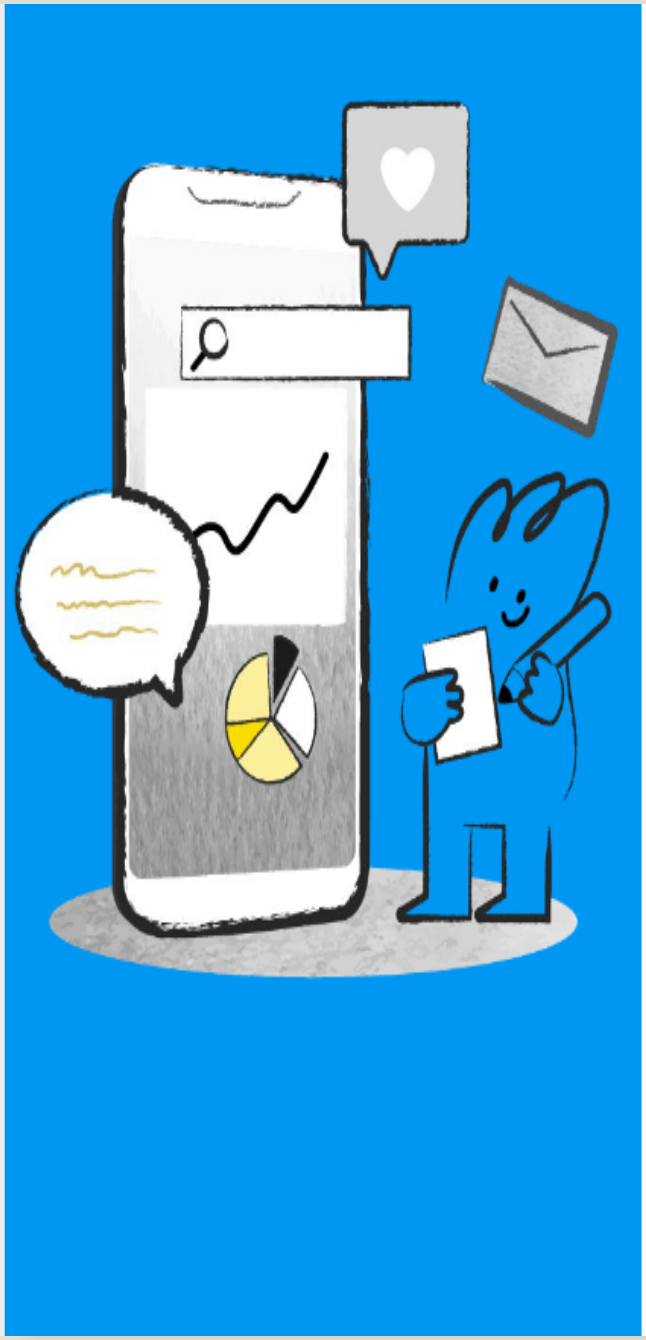
Захист цифрових пристроїв, персональних даних і електронних (цифрових) освітніх ресурсів

Комп'ютерний вірус — спеціально написана невелика за розмірами програма, яка може створювати свої копії, впроваджуючи їх у файли, оперативну пам'ять, завантажувальні області тощо (заражати їх), та виконувати різноманітні небажані дії.



Як визначити, що на комп’ютері є вірус?

- припинення роботи або неправильна робота програм, які раніше функціонували успішно;
- неможливість завантаження операційної системи;
- зменшення вільного обсягу пам'яті;
- уповільнення роботи комп'ютера;
- затримки під час виконання програм, збої в роботі комп'ютера;
- раптове збільшення кількості файлів на диску;
- зникнення файлів і каталогів або перекручування їхнього вмісту;
- незрозумілі зміни у файлах;
- зміни дати і часу модифікації файлів без очевидних причин;
- незрозумілі зміни розмірів файлів;
- видача непередбачених звукових сигналів;
- виведення на екран непередбачених повідомлень або зображень.



Захист від спаму

Спам (англ. *Spam*) — це масове розсилання рекламних листів, повідомлень користувачам, які не давали на це своєї згоди.

Використовується з метою залучення в процес маркетингу власників електронних пошт. Повністю захиститися від спаму неможливо, але можна звести до мінімуму ймовірність його потрапляння до особистої електронної пошти. Не повідомляйте нікому електронну адресу.

- Не вказуйте e-mail в опитувальниках.
- Майте окремий e-mail для важливих справ.
- Не публікуйте e-mail у відкритому доступі.
- Приховуйте інформацію про себе.
- Налаштовуйте параметри приватності.
- Умикайте антиспам-системи.
- Забороніть спливаючі вікна в браузері.

Найпоширеніші види кіберзлочинів

Кардинг – шахрайські операції з кредитними картками (реквізитами кредитних карток), які не погоджені власником картки. Це може бути крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через інтернет без участі власника картки. У будь-якому разі основною метою злочинців є отримання доступу до чужих грошових коштів. Для досягнення цієї мети зловмисники вигадують різноманітні способи отримання потрібної інформації в неуважних і легковірних громадян. Одним із таких способів є фішинг.

Фішинг – шахрайські дії, спрямовані на виманювання реквізитів картки у її власника. Зазвичай власник кредитної картки сам добровільно повідомляє шахраям потрібну інформацію.

Фішинг буває кількох видів:

- СМС-фішинг, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку. Варіацій СМС-повідомлень безліч, тому потрібно бути особливо уважними й обачними, якщо ви отримуєте повідомлення.
- Інтернет-фішинг, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів тощо. На жаль, не всі уважно перевіряють назву сайту, уводячи дані кредитної картки, що на руку кібершахраям.
- Вішинг — це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків (шахраї часто представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити якісь дії зі своїм рахунком).

Скімінг – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами. Для отримання даних злочинці використовують міні-камери або змінні клавіатури.

Шимінг – модернізований різновид скімінгу. У цьому разі шахраї використовують майже непомітний прилад, який розміщують усередині картридера. Таким чином дані кредитки копіюються непомітно.

Онлайн-шахрайство — фальшиві інтернет-аукціони, інтернет-магазини, сайти й телекомунікаційні засоби зв'язку.

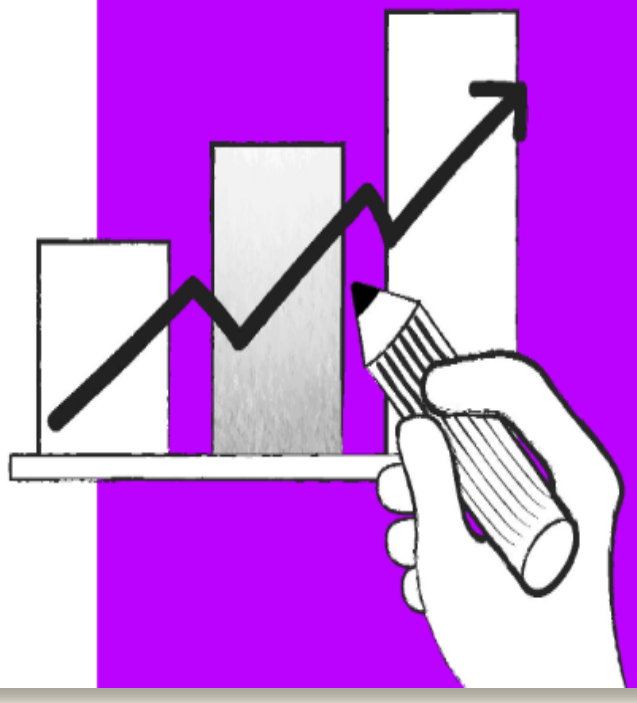
Піратство — протиправне розповсюдження об'єктів інтелектуальної власності в Інтернеті.

Мальваре — створення та поширення вірусів і шкідливого програмного забезпечення.

Протиправний контент — контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства.

Рефайлінг — незаконна підміна телефонного трафіку.

Є шахрайські схеми, коли власник електронного гаманця надає доступ шахраям до своїх акаунтів і вони переводять десятки тисяч доларів на інший гаманець. Кіберполіція кваліфікує цей вид злочину як шахрайство з використанням електронно-обчислювальної техніки.



Пропаганда – це навмисний цілеспрямований вплив на аудиторію через поширення різними комунікативними каналами недостовірної (неповної, неточної, спотвореної) інформації, спрощених (однобічних) суджень, спеціально створених міфів, стереотипів, оцінок, а також прихованого чи відкритого нав'язування якоїсь однієї позиції, ідеї для спонукання й змушування людей робити те, на що вони не наважилися б, маючи достовірну (повну, різнобічну) інформацію.

Інформаційна війна – це сукупність інформаційних дій, застосовуваних сторонами, які протистоять одна одній, для досягнення певних цілей. Зазвичай мета інформаційної війни полягає в досягненні інформаційної переваги над супротивником і формуванні такого інформаційного середовища, що сприяло б реалізації інших (неінформаційних) дій (політичних, дипломатичних, економічних тощо).

Негатив містить політична й ідеологічна пропаганда.

Найбільшу небезпеку несе в собі пропаганда війни, національної, расової, релігійної ненависті, що підбурює до дискримінації, ворожості, насилля.

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

- **інформаційна безпека** — це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

В залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином :

- як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод людини і громадянина.

- ОСНОВНИМИ ЗАВДАННЯМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВВАЖАЮТЬСЯ: ДОСТУПНІСТЬ, ЦІЛІСНІСТЬ, ЩО ВКЛЮЧАЄ АВТЕНТИЧНІСТЬ, А ТАКОЖ КОНФІДЕНЦІЙНІСТЬ. КІБЕРБЕЗПЕКА Є НЕОБХІДНОЮ УМОВОЮ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

З технічної точки зору, залежно від результату шкідливих дій, можна виділити такі види загроз інформаційній безпеці:

- отримання несанкціонованого доступу до секретних або конфіден-ційних даних;
- порушення або повне припинення роботи комп'ютерної інформаційної системи;
- отримання несанкціонованого доступу до керування роботою комп'ютерної інформаційної системи;
- знищення та спотворення даних.

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

- несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем,

наприклад у результаті цілеспрямованої хакерської атаки — дій, що спрямовані на порушення штатного режиму функціонування системи, порушення доступності її сервісів, отримання несанкціонованого доступу до конфіденційних відомостей, порушення цілісності даних тощо;

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

- інтернет-шахрайство, наприклад фішинг — вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо;

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

- потрапляння в інформаційну систему шкідливого програмного забезпечення:

вірусів	мережевих хробаків	троянських програм	клавіатур-них шпигунів	рекламних систем та ін.

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

- потрапляння комп'ютера до ботнет-мережі (англ. botnet від robot і network — робот і мережа) через приховане встановлення програмного забезпечення, яке використовується зловмисником

для виконання певних, найчастіше протиправних, дій з використанням ресурсів інфікованих комп'ютерів.

ПЛАКАТ-ПАМ'ЯТКА «БЕЗПЕЧНИЙ ІНТЕРНЕТ»

Смартфон, планшет чи комп'ютер з доступом до інтернету відкривають перед тобою безліч можливостей. Пам'ятай про правила безпеки, і тоді вони будуть твоїми надійними помічниками для розваг та навчання.

1/ ЗАХИСТИ
СВОЇ ОСОБИСТІ ДАНІ

Використовуй надійні паролі та не повідомляй їх нікому.

Не пиши в інтернеті дані, які можуть використати зловмисники: домашню адресу, номер мобільного.

2/ ВЧИСЬ
ЗАХИЩАТИСЯ ВІД ВІРУСІВ

Віруси часто ховаються й маскуються. Надавай перевагу офіційним сайтам, коли завантажуєш програми.

Не відкривай підозрілі листи, ніколи не переходь за посиланням та не завантажуй додатки з таких листів.

3/ НЕ ДАЙ
СЕБЕ ПОГРАБУВАТИ

На сайтах з оголошеннями водяться шахраї. Безпечніше замовляти товари на сайтах, де є післяплата.

Не повідомляй в інтернеті дані платіжних карток. Їх не повинні знати навіть працівники банку.

4/ ПОДУМАЙ,
ПЕРШ НІЖ ПУБЛІКУВАТИ ЩОСЬ

Інформацію, яку ти публікуєш в інтернеті, часто неможливо видалити повністю. Навіть, якщо на сайті є така функція, хтось може скопіювати дані і поширювати їх вже після того, як ти видалиш.

Фото чи відео твоїх друзів можна публікувати лише за їх згоди.

5/ НЕ ГОДУЙ
ХЕЙТЕРІВ СВОЄЮ УВАГОЮ

Якщо зібрати всі образливі та беззмістовні повідомлення користувачів інтернету, вийде обсяг більший за всі твої шкільні підручники з 1 по 11 класи.

Подумай, чи варто витрачати час на те, щоб читати або писати такі повідомлення.

6/ ВЧИСЬ
ШУКАТИ ДОКАЗИ

Навіть великі інформаційні видання інколи публікують неправдиві новини. Чого ж варто очікувати від маленьких сайтів чи блогерів, які намагаються якомога швидше висловити свою думку?

Не поспішай вірити всьому, про що пишуть чи говорять

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

- «крадіжка особистості» (англ. Identity Theft — крадіжка персональних даних) — несанкціоноване заволодіння персональними даними особи, що дає можливість зловмиснику здійснювати діяльність від її імені.

ЗАГРОЗИ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Ви знаєте, що смартфони — це мобільні телефони, доповнені функціями персонального комп'ютера, зі своєю операційною системою та іншим програмним забезпеченням.

Тому для смартфонів характерні ті самі загрози, що і для стаціонарних комп'ютерів:

- ***віруси***
- ***троянські програми***
- ***мережеві хробаки***
- ***рекламні модулі та ін.***

Як і стаціонарні комп'ютери, смартфони можуть потрапити до ботнет-мережі.

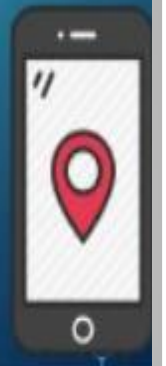
ЗАГРОЗИ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Найчастіше смартфон постійно увімкнений, має підключення до мережі Інтернет, завжди розташований поруч із власником, містить різноманітні пристрої введення/виведення:

мікрофон

відео-камеру

GPS-навігатор та ін.



Зі смартфоном нерідко зв'язані грошові рахунки — в оператора мобільного зв'язку або банківські рахунки. Усе це підсилює небезпеку.

ЗАГРОЗИ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Існують шпигунські програми, які зловмисники використовують для шпигування за користувачем смартфона. Використовуючи їх, можна:

перехоплювати повідомлення про всі здійснені дзвінки	*показувати вміст СМС-листування*	*показувати дані про відвідані сайти*
знімати камерою телефона оточення користувача	*визначати його місце розташування*	*включати мікрофон і записувати всі розмови*

ЗАГРОЗИ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Ще один аспект загроз для користувачів мобільних телефонів полягає в роботі з платними послугами.

Підписка з використанням СМС на онлайн-гру, певний сайт, будь-який сервіс, який вимагає регулярну оплату, можуть призводити до списування з рахунку значних коштів. Іноді такі СМС можуть надсилатися троянськими програмами.

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

Для того щоб максимально уникнути загроз під час роботи в Інтернеті, варто дотримуватися певних правил.

Наведемо поради, що надані CERT-UA (англ. Computer Emergency Response Team of Ukraine — команда України з редагування на комп'ютерні надзвичайні події):

спеціалізованим структурним підрозділом Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України (cert.gov.ua).

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

Поради, що надані CERT-UA:

1. Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.
2. Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.
3. Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

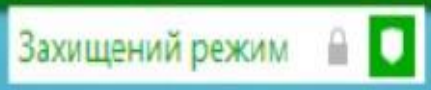
4. Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.

5. Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.

6. Установіть фільтр спливаючих вікон у браузері.

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

7. Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера та URL-адреси веб-сайтів, щоб визначити, чи не підроблений сайт ви відвідуєте.



8. Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

9. Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет. Дуже легко розмістити дані в мережі Інтернет, але дуже складно їх видалити з неї.

10. Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

Також для дуже важливих акаунтів використовуються унікальні зовнішні накопичувачі та зчитувачі біометричних даних. Для користувачів смартфонів є окремі рекомендації:

- ✓ не телефонуйте на незнайомі номери;
- ✓ уважно контролюйте послуги, на які ви підписуєтеся;
- ✓ установлюйте мобільні додатки лише з офіційних магазинів: PlayMarket (Android), AppStore (iOS);
- ✓ уважно стежте за тим, які дозволи вимагає програма під час установлення та оновлення програмного забезпечення на мобільних пристроях.

Поради щодо безпеки в Інтернеті

Використовуйте Антивірус

Використовуйте надійні паролі

Періодично змінюйте паролі

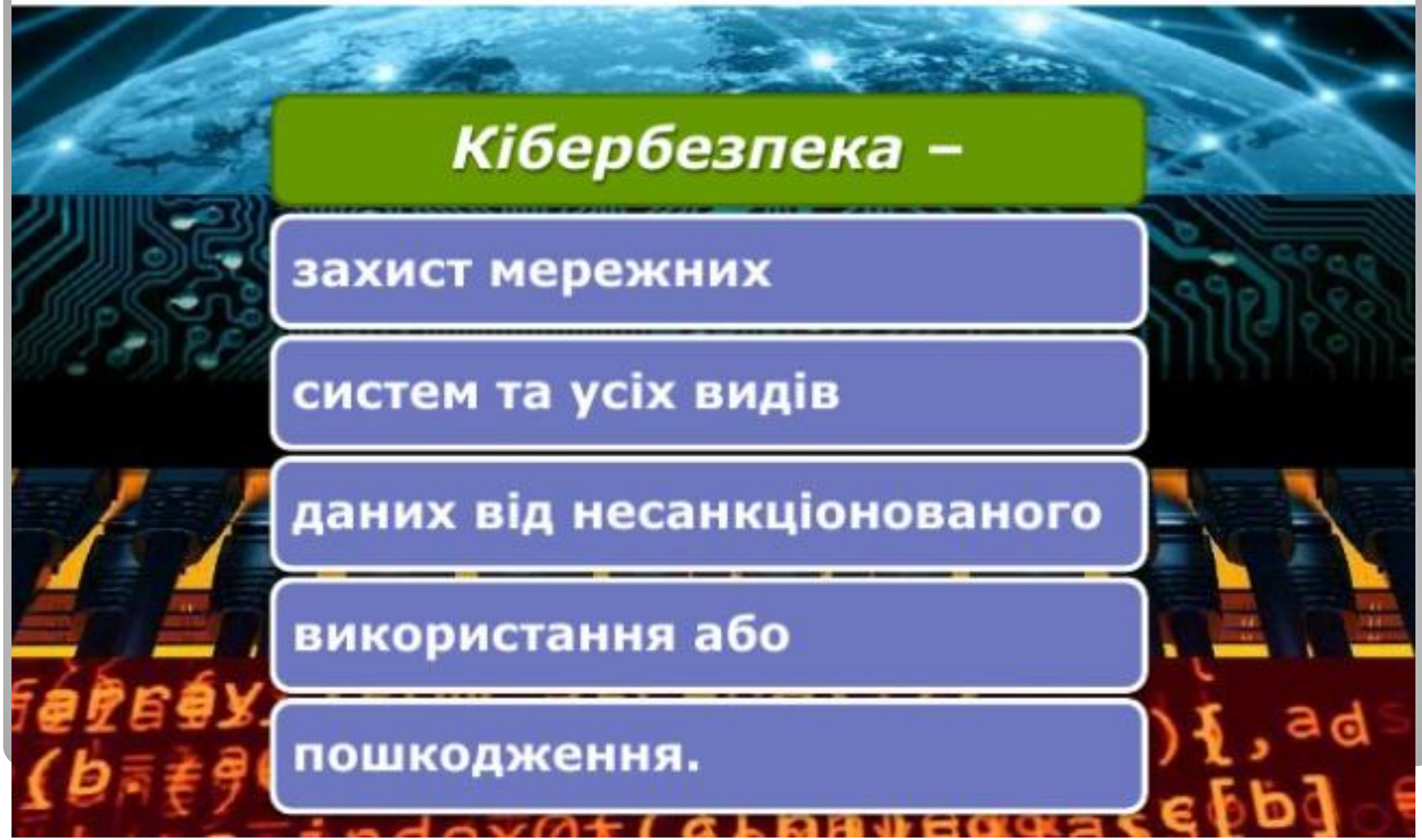
Не відвідуйте підозрілі веб-сайти

Не діліться особистою інформацією

Використовуйте 2-во рівневу аутентифікацію

Оновлюйте Програмне Забезпечення

Що таке кібербезпека?



Кібербезпека –

захист мережних

систем та усіх видів

даних від несанкціонованого

використання або

пошкодження.

Основні правила кібергігієни

від CERT-UA

Дізнайтесь, як не стати жертвою кібершахрайства

1. Використовуйте ліцензійні/легалізовані операційні системи та інші програмні продукти. Своєчасно і систематично їх оновлюйте.

2. Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.

3. Використовуйте програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.

4. Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SDD, HDD тощо)та налаштуйте функцію «відновлення системи».

5. Уникайте використання інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях).

6. Під час використання віддаленного доступу необхідно обмежити доступ за допомогою "білого списку"(IP whitelisting) .

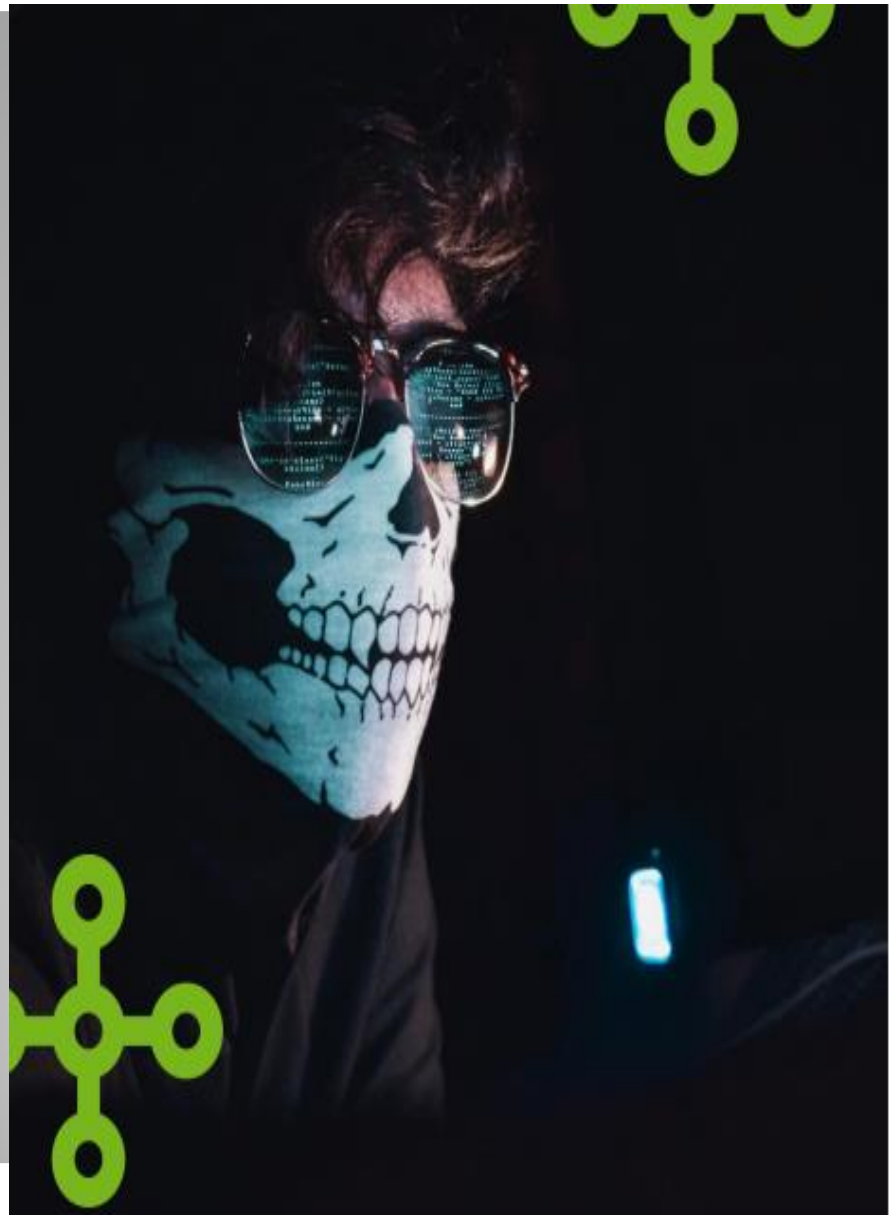
7. Встановіть обмеження кількості введення помилкових логінів/паролей. Регулярно переглядайте журнали логування, планувальник завдань та автозавантаження на предмет несанкціонованих дій

8. Регулярно змінюйте паролі, не зберігайте автентифікаційні дані в легкодоступних місцях (наприклад на робочому столі). Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass).

Використовуйте стійкі паролі, зокрема такі що:

- містять не менше 8 символів;
- містять літери, цифри та спеціальні символи;
- не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо);
- не використовуються в будь-яких інших акаунтах.

9. Будьте обережні щодо випливаючих вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читайте вміст цих вікон та не "схвалюйте" і не "приймайте" нічого похапцем.



10. Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу. Існують техніки зламування комп'ютера, що спрацьовують ще до того, як ви відкриєте файл на флешці і задовго до того, як ваш антивірус його просканує.

Якщо ви знайшли пристрій всередині офісу або на вулиці, чи отримали його поштою або з доставкою, чи незнайомець дав вам його з проханням роздрукувати документ, або просто відкрити та перевірити його вміст – є велика ймовірність, що пристрій є небезпечним.

- Довіряйте лише власним пристроям та будьте обережні з пристроями, які отримуєте від інших людей по роботі або в інших цілях.
- При підключенні пристроїв забезпечте їх автоматичну перевірку на наявність шкідливого програмного забезпечення.
- Відключайте автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

11. Під час користування інтернет-ресурсами (інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами, онлайн-іграми) не відкривайте підозрілі посилання (URL), особливо ті, що вказують на веб-сайти, які ви зазвичай не відвідуєте.

- **Будьте уважним до проявів інтернет-шахрайства. Найпоширенішим засобом уведення в оману в мережі інтернет є фішинг.**

Особливу увагу варто звертати на доменне ім'я інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, gooogle.com тощо). В іншому разі є велика ймовірність перейти на фішингову сторінку, зовні ідентичну справжній, та самостійно «віддати» власні автентифікаційні дані.

- **У разі необхідності введення автентифікаційних даних упевніться в тому, що використовується захищене з'єднання HTTPS, перевіряйте SSL-сертифікат веб-сайту, щоб переконатися, що він не клонований або не підроблений.**
- **Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами на кшталт tinyurl.com, bit.ly, ow.ly тощо. Не вводьте ці посилання до браузера та не скануйте QR-коди вашим смартфоном, якщо ви не впевнені у їх вмісті та походженні.**
- **Використовуйте VirusTotal для перевірки підозрілих посилань так само, як для сканування файлів.**

12. Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб.

Сьогодні найактуальнішим засобом розсилання шкідливого програмного забезпечення є електронна пошта. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів та не відкривати файли навіть з безпечними розширеннями.

Не переходьте за невідомими посиланнями та не завантажуйте файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) та навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки. Звертайте увагу на ім'я електронної пошти: навіть якщо воно здається легітимним, усе одно потрібно перевірити (у телефонному режимі або в будь-який інший спосіб), чи дійсно ця особа відправляла вам повідомлення з вкладенням.

Іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більш ніж 50 антивірусами. Це набагато ефективніше, ніж сканування файлів антивірусом в автономному режимі, але враховуйте той факт, що завантажуючи файли на VirusTotal, ви надаєте доступ до нього третій стороні. Звертаємо вашу увагу на те, що, навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим.

Тричі подумайте перед відкриттям вкладень.

Будьте пильні
та залишайтесь
у безпеці!

ВИКОРИСТАНІ ДЖЕРЕЛА

- ✓ **Доценко С.О. Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання: Навч.-метод. посіб. / С.О. Доценко, В.В. Ворожбіт-Горбатюк, Т.М. Собченко. – Харків: Ранок, 2021.**
- ✓ https://academyranok.com.ua/course/elektronni-czyfrovi-osvitni-resursy/
- ✓ https://naurok.com.ua/kiberbezpeka-v-interneti-prezentaciya-293880.html
- ✓ https://naurok.com.ua/prezentaciya-ya-za-bezpechniy-internet-295387.html
- ✓ chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.datagroup.ua/storage/editor/files/cybersecurity-ua.pdf

ДЯКУЮ ЗА УВАГУ !