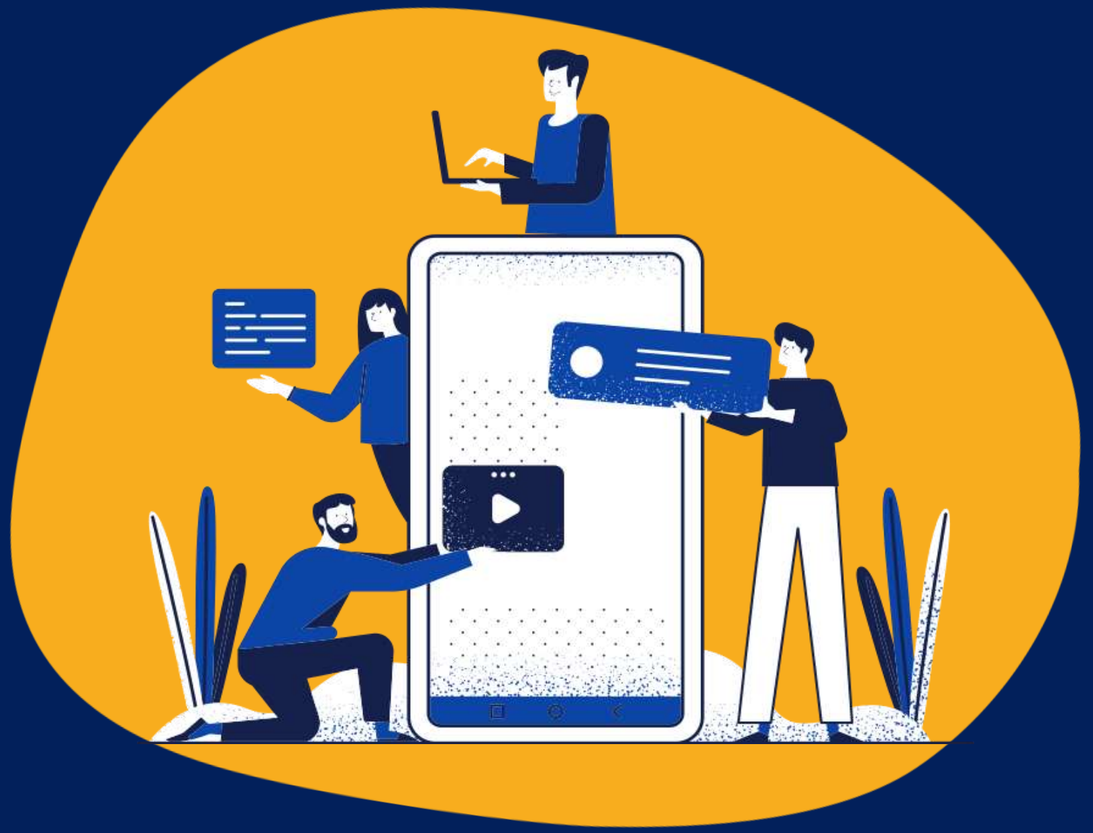
БІБЛІОТЕКА
СУМСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ

Цифрова безпека



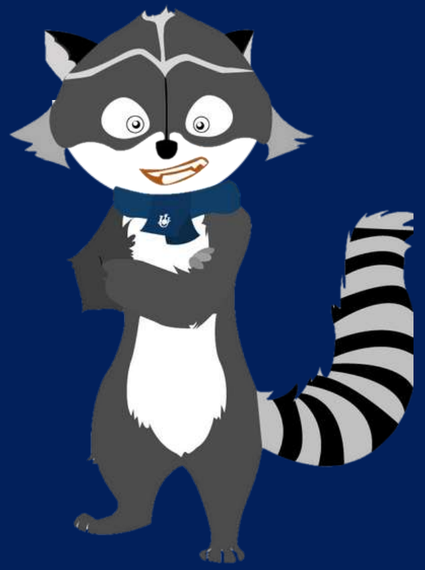
Практичні поради

ЗМІСТ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Створюй складні паролі

Налаштуй двофакторну аутентифікацію



Дотримуйся приватності

Відмовся від геолокації

Захищай свої пристрої

ЯК СТВОРИТИ НАДІЙНИЙ ПАРОЛЬ

- складай пароль мінімум з 8–14 символів
- застосовуй прописні та строчні букви
- додавай цифри та символи
- застосовуй різні букви та цифри
- використовуй парольну фразу

Ненадійні паролі зазвичай стають причиною хакерських атак.

ЯК ЗАХИСТИТИ ПАРОЛЬ

- не використовуй особисті дані для пароля
- раз на квартал змінюй паролі
- використовуй менеджери паролів
- застосовуй двоетапну перевірку
- не забувай виходити зі своїх акаунтів
- не залишай паролі в пам’яті браузера

МЕНЕДЖЕРИ ПАРОЛІВ

програмне забезпечення з розширеним функціоналом, що полегшує доступ до паролів, ліцензійних ключів, Wi-Fi для доступу до вебсайтів та додатків.
Менеджери паролів дозволяють створювати зашифровані архіви, щоб надійно зберігати файли та завантажувати їх у хмарне сховище.

ДЕ КЕРУВАТИ ПАРОЛЯМИ

у налаштуваннях *веббраузерів*, якщо використовуєш особистий пристрій, наприклад:

Google Chrome

Safari

Internet Explorer

Mozilla Firefox

Вбудовані менеджери паролів у браузерах не настільки потужні та корисні, як сторонні менеджери паролів.

ДЕ КЕРУВАТИ ПАРОЛЯМИ

у сторонніх менеджерах паролів, які генерують надійні паролі, запам’ятовують їх, і дозволяють входити до вебсайтів, наприклад:

LastPass **KeePass** **1Password**

На думку фахівців, *використання сторонніх менеджерів паролів є найбільш безпечним*.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ KEEPASS

безкоштовне програмне забезпечення з відкритим кодом, має основні можливості менеджерів паролів для персонального використання.

Як легко користуватися KeePass

ВИДИ ДВОХЕТАПНОЇ ПЕРЕВІРКИ

- *резервний метод* входу до акаунта за допомогою SMS або виклику на телефон
- через програмні застосунки аутентифікатори *Google Authenticator, Authy (iOS, Android), Microsoft Authenticator*
- *апаратний ключ безпеки*

ЯК НАЛАШТУВАТИ ДВОХЕТАПНУ ПЕРЕВІРКУ, НА ПРИКЛАДІ GOOGLE?

- перейди у свій *обліковий запис Google*
- натисни *Управління акаунтом Google*
- на лівій панелі навігації натисни *Безпека*
- у блоці *Вхід в акаунт Google* натисни *Двохетапна аутентифікація* ✓ та *Почати*
- виконай подальші вказівки на екрані

ЗАГРОЗИ НЕЗАХИЩЕНИХ МЕРЕЖ WI-FI ТА BLUETOOTH

- не підключайся автоматично до мереж Wi-Fi
- використовуй лише захищені паролем мережі
- вимикай Wi-Fi, Bluetooth, коли їх не використовуєш
- відкривай сайти лише з шифруванням HTTPS
- використовуй перевірені VPN-з’єднання

VPN-СЕРВІСИ: ПЕРЕВАГИ ТА ЗАГРОЗИ

- ✓ анонімність IP-адреси в мережі
- ✓ маскування місцезнаходження
- ✓ відсутність географічних обмежень в доступі
- ✓ захищене з'єднання з віддаленою мережею

- ✓ VPN-сервіси збирають дані про користувачів
- ✓ є ризик передачі даних до мереж загального користування
- ✓ небезпека несанкціонованого використання мікрофону та камери пристроїв

ПРАВИЛА БЕЗПЕКИ E-MAIL

- не зазначай свою адресу на сумнівних сайтах
- не розпаковуй вкладені в листи підозрілі архіви
- видаляй листи від підозрілих адресатів
- не відповідай на спам листи, налаштуй фільтр
- використовуй безпечне шифрування HTTPS
- не користуйся чужими пристроями для входу на електронну пошту

ФІШИНГ

електронні листи від шахраїв, метою яких є отримання доступу до особистої та конфіденційної інформації.

Сьогодні фішинг маскується під офіційні сервіси підтримки, листи відписки від розсилок, сайти або оголошення.

ЯК РОЗПІЗНАТИ ФІШИНГ

підозрілі посилання

https://bit.ly/security-check-gmail

помилки в тексті

Заради вашої безпеки та приватносьті, вам треба

неперсональні звернення

Шановний користувач!

ЯК РОЗПІЗНАТИ ФІШИНГ

заклик до термінової дії

У вас лише 24 години, інакше акаунт буде видалено назавжди!

фейкова назва відправника

фейкова назва відправника

ТЕРМІНОВО актуалізувати персональні дані...

https://bit.ly/3dfqXJY

ЯК УНИКНУТИ ФІШИНГУ

- перевіряй підозрілі URL-адреси та посилань
- будь уважним надаючи особисті дані
- остерігайся шахрайських листів
- перевіряй файли, перш ніж завантажувати
- остерігайся осіб, що видають себе за інших
- повідомляй про фішинг організації, від імені якої написали шахраї

http://surl.li/ckpv

БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ

- використовуй біометрію
- не залишай смартфон без нагляду
- не переходь за посиланнями з SMS
- завантажуй застосунки з офіційних маркетів додатків
- уважно читай користувацькі угоди застосунків
- регулярно оновлюй програмне забезпечення

ЗАХИСТ ФІНАНСОВОГО НОМЕРА

- зареєструй SIM-картку у мобільного оператора, тоді сторонні не зможуть перевипустити твій номер телефону
- встанови власний ПІН-код на SIM-картку
- у разі втрати смартфону заблокуй SIM-картку

ЧИСТИЙ СМАРТФОН — ТВОЯ БЕЗПЕКА

вимкни мобільний пристрій

протри поверхню:

- сухою тканиною з мікроволокна
- тканиною змоченою у мильному розчині
- серветками для дезінфекції

не вмикай телефон поки повністю не висохне

ЦИФРОВА БЕЗПЕКА У ТВОЇХ РУКАХ