Кібербезпека в роботі з державними інформаційними ресурсами

Навіщо це важливо?

Кіберфронт України

Кібербезпека завжди була вразливим місцем через брак кадрів та халатність. З початком повномасштабного вторгнення **загроза багаторазово загострилась.** З 2014 року ворожі хакерські угрупування готували "сплячі" закладки в державних та комунальних установах.

24 лютого 2022 року відбулася активація цих закладок та початок масованих атак на критичну інфраструктуру, банківські системи, провайдерів та мобільних операторів.

Проте Україна тримає кіберфронт завдяки злагодженій роботі CERT-UA, СБУ, кіберполіції та НБУ.

Закон України
від 27.03.2025 № 4336-IX

Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури

Розуміння основ

Ключові Поняття

Кібербезпека

Захищеність життєво важливих інтересів людини, суспільства та держави у кіберпросторі.

Кіберзахист

Комплекс організаційних, правових та технічних заходів для запобігання кібератакам, ліквідації їх наслідків та відновлення систем.

Кіберінцидент

Будь-яка подія (ненавмисна чи потенційна атака), що загрожує безпеці систем та інформаційних ресурсів.

Найнебезпечніша атака

Кібершпигунство та Витік Даних

Головна мета ворога: викрадення інформації з державних та комунальних установ. Атакують спонсоровані РФ угрупування (наприклад, UAC-0050, UAC-0006).

Як це працює?

- На пошту (часто бухгалтеру) приходить лист із темою "Платіжне доручення", "Помилковий платіж" або "Повідомлення від ДПС".
- Лист містить погрози (блокування рахунків), щоб змусити діяти швидко.
- Жертва відкриває шкідливе вкладення (PDF, архів) або переходить за посиланням.

Результат

Зловмисники отримують доступ до ПК, фінансової та службової інформації, що може мати руйнівні наслідки для держави.

Будьте пильні

Інші Поширені Загрози

1

📢 Інформаційно-психологічні операції (ІПСО) та Спам

Масові розсилки небажаних повідомлень для компрометації влади та впливу на емоційний стан громадян, поширення дезінформації.

2

🧳 Шкідливе програмне забезпечення (ШПЗ)

Безумовний лідер серед кіберінцидентів. Потрапляє в систему через завантажені файли, архіви, неліцензійне ПЗ.

3

🎧 Фішинг

Маскування під надійні джерела (банки, держустанови) для викрадення логінів та паролів через підроблені сайти.

4

🔒 Компрометація облікового запису

Несанкціонований доступ до вашої пошти, соцмереж, месенджерів.

Ваша перша лінія оборони

Фундаментальні Правила Захисту

✅ Ліцензійне ПЗ

Використовуйте тільки ліцензійні/легалізовані ОС та програми.

🔄 Оновлення

Своєчасно та систематично оновлюйте все програмне забезпечення.

🛡️ Антивірус

Встановіть антивірус з евристичним аналізом та увімкніть брандмауер.

💾 Резервне копіювання

Регулярно створюйте копії важливої інформації на зовнішні носії (SSD, HDD).

🚫 Сторонні носії

Не підключайте неперевірені флешки та диски.

Ваш перший замок

Сила Надійного Пароля

Ключові вимоги:

- **Довжина:** не менше 8 символів (ідеально 12-16).
- **Складність:** літери (великі та малі), цифри, спеціальні символи (!, @, #, $).
- **Унікальність:** різні паролі для різних акаунтів.

Безпека:

- ❌ Не використовуйте особисту інформацію (дати народження, імена).
- ❌ Не записуйте на стікерах чи в нотатках браузера.
- ✅ Регулярно змінюйте (кожні 3-6 місяців).
- ✅ Використовуйте менеджери паролів (наприклад, **KeePass**).
- ❓ Перевіряйте пошту на витоки через сервіс **Have I Been Pwned**.

https://haveibeenpwned.com/

Додатковий рівень захисту

Багатофакторна Автентифікація (БФА)

Що це? Додатковий рівень захисту, який вимагає підтвердження входу, крім пароля. Навіть якщо ваш пароль вкрали, зловмисник не зможе увійти у ваш акаунт.

Найбезпечніші способи:

- Спеціальні застосунки (**Google Authenticator, Microsoft Authenticator, Authy**).
- Електронний ключ (токен).

Менш безпечний спосіб: SMS-коди (можуть бути перехоплені).

Де вмикати?

Скрізь, де можливо: пошта, месенджери, соцмережі, банківські додатки, державні онлайн-сервіси. Це суттєво підвищує вашу кібербезпеку.

Підключення без ризиків

Безпека Wi-Fi Мереж

🚫 Публічний Wi-Fi (кафе, аеропорти)

- **Ніколи** не вводьте логіни, паролі, дані банківських карток.
- Використовуйте мобільний інтернет або VPN-сервіс.
- Вимкніть автоматичне підключення до відкритих мереж.

🏠 Домашній Wi-Fi

- Використовуйте сучасний протокол шифрування (**WPA3 або WPA2**).
- Встановіть надійний та унікальний пароль на саму мережу та на вхід в налаштування роутера.
- Регулярно оновлюйте прошивку роутера.

Чому це Важливо?

У сучасному світі електронна пошта є основним інструментом комунікації. Однак разом із зручностями вона несе і значні ризики. Фішинг, шкідливе програмне забезпечення та викрадення даних стають все більш витонченими. Розуміння основ кібербезпеки допоможе вам захистити себе та дані вашої організації.

Захист даних

Зберігайте ваші особисті та корпоративні дані в безпеці.

Запобігання шахрайству

Розпізнавайте та уникайте фішингових атак та інших видів кібершахрайства.

Боротьба зі шкідливим ПЗ

Запобігайте зараженню комп'ютерів та мереж вірусами та шкідливим програмним забезпеченням.

Золоті Правила Роботи з E-mail

Дотримання цих простих правил значно підвищить вашу кібербезпеку.

Невідомий відправник?

Не відкривайте вкладення та не переходьте за посиланнями. Це може бути спроба фішингу або розповсюдження шкідливого ПЗ.

Знайомий, але підозрілий лист?

Зателефонуйте та уточніть, чи справді людина надсилала вам цей файл. Шахраї часто підробляють адреси відправників.

Перевіряйте розширення файлів

Будьте обережні з архівами (.zip, .rar) та документами з макросами (.docm, .xlsm). Ці типи файлів часто використовуються для приховування вірусів.

Вимкніть автозавантаження

Вимкніть автоматичне завантаження файлів у налаштуваннях браузера. Це дасть вам додатковий контроль над тим, що зберігається на вашому комп'ютері.

Як Розпізнати Небезпечні Посилання?

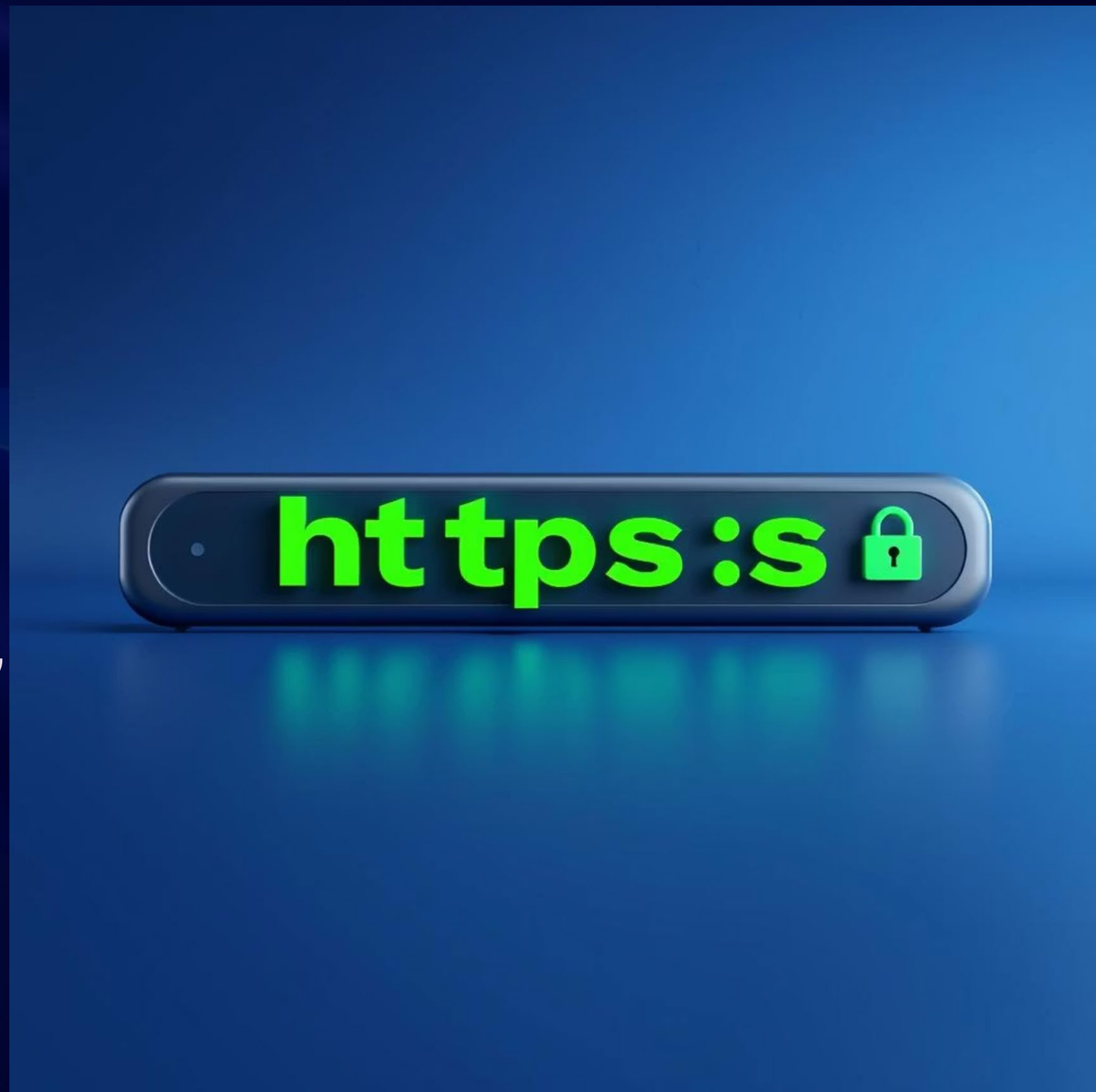
Фішингові посилання є одним із найпоширеніших методів викрадення даних. Навчіться їх розпізнавати, щоб уникнути пастки.

- **Скорочені посилання (Bitly, Cuttly)**

  Не переходьте, не перевіривши. Використовуйте сервіси типу Unshorten.It https://unshorten.it/ для перегляду повного посилання.

- **HTTPS**

  При введенні будь-яких даних переконайтесь, що адреса сайту починається з https:// і є значок замка. Це означає захищене з'єднання.



QR-коди: Джерело Ризику?

QR-коди стали повсякденним явищем, але вони також можуть бути інструментом для шахраїв.

Скануйте QR-коди **лише з надійних джерел**. Шахраї можуть замінити оригінальні QR-коди на підроблені, які ведуть на фішингові сайти або завантажують шкідливе програмне забезпечення. Завжди перевіряйте, чи немає ознак втручання.

Перед скануванням

Переконайтеся, що QR-код виглядає справжнім, не наклеєний поверх іншого.

Після сканування

Завжди перевіряйте посилання, на яке веде QR-код, перед тим як переходити за ним.

Увага на Домен!

Шахраї часто створюють домени, які дуже схожі на справжні, щоб обдурити користувачів.

1

Правильний домен

Наприклад: `privat24.ua`

2

Фішинговий домен

Може виглядати так: `prrivat24.ua` або `privat24.com.ua`

Завжди уважно перевіряйте кожну літеру в доменному імені. Навіть одна змінена буква може вказувати на шахрайство.

> **Ніколи не вводьте особисті дані** (логіни, паролі, номери карт) на сайтах, у достовірності яких ви сумніваєтесь.

Практичний Інструмент: VirusTotal

VirusTotal – це безкоштовний онлайн-сервіс
для перевірки файлів та посилань на наявність вірусів та шкідливого програмного забезпечення.

Як користуватися?

01

Зайдіть на сайт

Перейдіть на VirusTotal.com
https://www.virustotal.com/ в своєму браузері.

02

Завантажте або вставте

Виберіть "File" для завантаження підозрілого файлу або "URL" для введення посилання.

03

Отримайте звіт

Сервіс просканує файл/посилання за допомогою понад 50 антивірусів і надасть детальний звіт.

Важливе Застереження щодо VirusTotal

Хоча VirusTotal є потужним інструментом, важливо пам'ятати про його обмеження та правила безпечного використання.

Не завантажуйте конфіденційні дані!

Завантажуючи файл на VirusTotal, ви надаєте доступ до нього третій стороні. **Ніколи не завантажуйте документи, що містять конфіденційну або особисту інформацію** (наприклад, фінансові звіти, особисті фото, паролі тощо). Використовуйте сервіс лише для перевірки файлів, які не містять приватної інформації.

Організаційні заходи та відповідальність

Дозволене ПЗ

В державних системах можна використовувати лише програмне забезпечення, яке пройшло відповідну перевірку та відсутнє у переліку забороненого.

Відповідальність

Власники та розпорядники державних систем зобов'язані забезпечувати їх кіберзахист та негайно повідомляти про будь-які інциденти кібербезпеки.

Спеціальні підрозділи

В органах державної влади створюються профільні підрозділи з кіберзахисту, діяльність яких координує Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ).

Навчання та CERT-UA

ДССЗЗІ регулярно проводить навчання для фахівців з кібербезпеки. Всі інциденти необхідно негайно повідомляти Національній команді реагування на кіберінциденти (CERT-UA).

Принцип мінімальних привілеїв та безпека даних

Суть принципу

Кожен користувач, програма або система повинні мати доступ лише до тієї інформації та ресурсів, які абсолютно необхідні для виконання їхніх безпосередніх функцій, і нічого більше.

Як реалізується

- **Авторизовані системи:** Державні інформаційні ресурси обробляються виключно в системах, що пройшли перевірку та мають сертифікат відповідності.
- **Комплекс ТЗІ:** Застосування Комплексу технічного захисту інформації є обов'язковим для обробки інформації, що становить державну таємницю.
- **Державна експертиза ПЗ:** Програмне забезпечення, що використовується для роботи з державною таємницею, проходить обов'язкову державну експертизу.
- **Заборона розміщення:** Забороняється розміщення систем або їх резервних копій на окупованих територіях або на території держави-агресора.

Соціальні мережі як джерело інформації (OSINT)

Ваш цифровий слід – це вся інформація, яку ви свідомо або несвідомо залишаєте у відкритому доступі в інтернеті. Зловмисники та розвідувальні служби активно використовують ці дані для отримання цінної інформації.

Нікнейми та професійна діяльність

Часто однакові нікнейми використовуються в різних соціальних мережах, що дозволяє створювати єдиний профіль. LinkedIn надає вичерпну інформацію про професійну діяльність та зв'язки.

Коло знайомств та локації

Facebook розкриває коло вашого спілкування, місця, які ви відвідуєте, та ваші вподобання. Instagram демонструє подорожі, геолокації та стиль життя.

Публікації та "червоні прапори"

Ваші публікації, лайки, коментарі, список друзів та родичів – все це джерела цінної інформації.

Інформаційна бульбашка: Як "виринути"?

Стан інформаційної ізоляції, коли алгоритми показують вам лише те, що відповідає вашим поглядам.

Небезпека інформаційної бульбашки

- Створює ілюзію, що ваша точка зору є домінуючою.
- Обмежує доступ до альтернативних думок та розширення світогляду.
- Робить вас вразливими до маніпуляцій та інформаційно-психологічних операцій (ІПСО).

Як "виринути" з бульбашки?

- **Розширюйте пошук:** Переглядайте не тільки першу сторінку результатів.
- **Підписуйтесь на опонентів:** Читайте в соцмережах людей та організації, з чиєю позицією ви не згодні.
- **Анонімність:** Використовуйте режим "інкогніто", VPN, різні браузери та пошукові системи (наприклад, DuckDuckGo).
- **Очищення даних:** Регулярно чистіть історію пошуку, cookie та видаляйте старі, невикористовувані акаунти.

Пам'ятайте про свою відповідальність

Ключові Висновки

Кібербезпека – це не одноразовий захід

Це постійний процес адаптації та захисту в динамічному кіберпросторі.

Найслабша ланка – людина

Ваша пильність та обережність є вирішальними для захисту систем.

Дотримання правил кібергігієни є критично важливим

Для захисту державних інформаційних ресурсів та національної безпеки.

Будьте пильними, обережними та постійно навчайтесь

Ваш внесок у кіберзахист є безцінним для України.

ДЯКУЮ ЗА УВАГУ!

Залишайтесь Захищеними!

ПИТАННЯ?