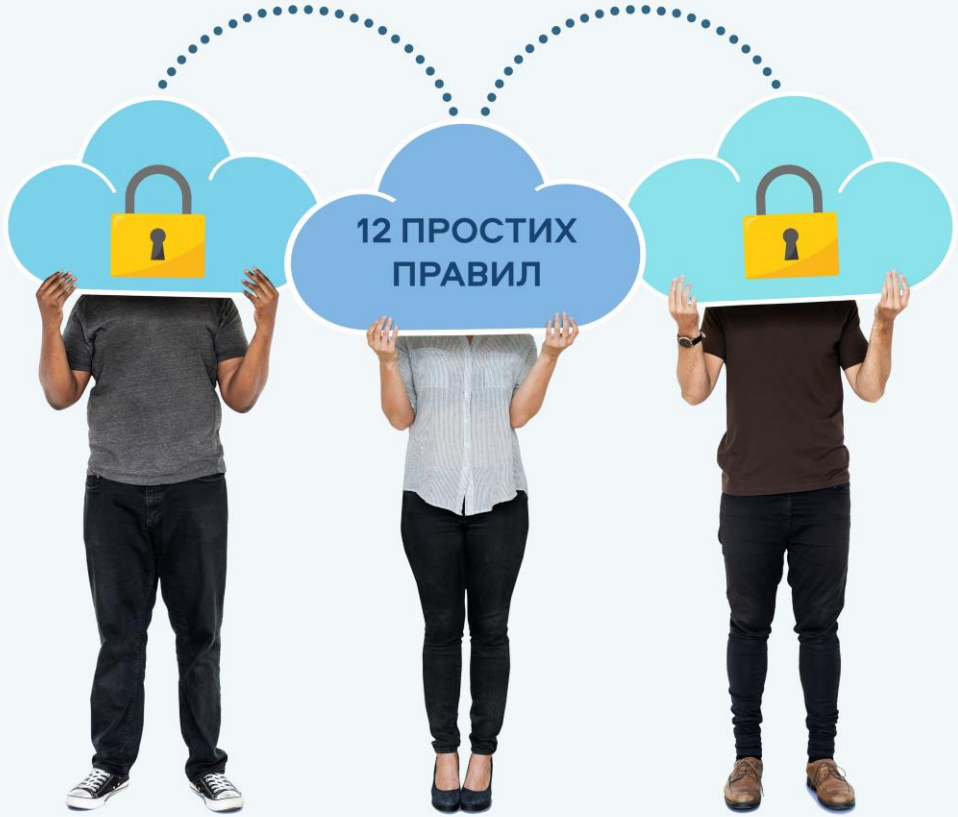
Основні правила кібергігієни

від CERT-UA



Дізнайтесь, як не стати жертвою кібершахрайства

За аналізом тенденцій останніх років, 2019-й стане одним з найбільш складних для спеціалістів з кібербезпеки. Тотальна цифровізація усіх процесів щодня робить потенційними жертвами кібершахраїв все більшу кількість користувачів мережі.

Інтернет-банкінг, соціальні мережі, e-mail розсилки — усе це є інструментом для кібератак, тому важливо знати, на що звертати увагу та як реагувати на загрози.

Ми, як відповідальний оператор зв'язку, бажаємо вам завжди залишатись у безпеці та пропонуємо переглянути 12 простих правил кібергігієни від CERT-UA (Computer Emergency Response Team of Ukraine).

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!