

Правила безпеки в інтернеті: ТОП-10

Правило 1: Не відкривайте вкладених файлів від невідомих відправників та не переходьте за підозрілими посиланнями

- **Подумайте, чи це повідомлення точно мало бути надіслане вам:** наприклад, чи справді ви замовляли якусь послугу або посилку;
- **Перевірте адресу відправника** — несправжню можна розпізнати, якщо уважно до неї придивитися;
- Сама назва додатку теж може багато сказати: наприклад, documents.js взагалі не є офісним файлом, хоч на перший погляд так може здаватися;
- **Наведіть мишку на посилання, проте не натискайте!** Тоді відобразиться адреса, а ви перевірите, на який сайт насправді вказує посилання.
- **Обережно переходьте за посиланнями в SMS-повідомленні.** Шахраї використовують ім'я банку для надіслання фіктивних SMS, щоб «виманити» у вас дані паролів або платіжної картки. Дізнайтеся **більше про SMS-фішинг.**

Правило 2: Перевіряйте адресу веб-сайтів, на які ви заходите, а також їхні сертифікати

- Уважно **перевіряйте вебсайти**, на яких ви перебуваєте: якщо вони будуть вам підозрілі - не вказуйте там жодних своїх даних;
- У разі необхідності введення автентифікаційних даних **переконайтеся, що з'єднання зашифроване.** На це вказує адреса, яка починається з **https://** та іконка закритого замка; також перевірте сертифікат веб-сайту (достатньо натиснути на замок);
- **Перевіряйте сайт**, використовуючи ресурс «Чорний список» від Асоціації ЄМА на наявність шахрайських сайтів в списку або сервіс кіберполіції «STOP FRAUD».

Правило 3: Часто оновлюйте пристрої та програмне забезпечення (системне та прикладне)

- **Не погоджуйтесь на встановлення на пристрої програм**, які походять з невідомих джерел;
- Не відключайте механізми захисту від виробника на своєму пристрої;
- **Не виконуйте дії, про які просить невідомий відправник в SMS-повідомленні/електронному повідомленні** (наприклад, натискання на посилання, які скеровують безпосередньо на сторінку входу в інтернет-сервіс банку);
- **Не вказуйте номер клієнта і пароль під час використання мобільного додатку** (за винятком процесу активації додатку);
- **Не встановлюйте жодних сертифікатів або додаткових програм для обслуговування.**

Правило 4: Створюйте складні паролі, які стороннім особам буде важко відгадати

- Пароль повинен містити не менше 8 символів, **складатися з великих і малих літер, цифр та спеціальних символів**;
- Не використовуйте паролі, які **можна знайти в словнику української мови або словниках іноземних мов** — злочинці мають програми, які можуть за кілька секунд зламати такі «словникові» паролі;
- Замість того, щоб записати, наприклад, пароль **Kredobank1234** — краще це зробити так: **Kred0b@nk1357>** його легко запам'ятати, але набагато складніше зламати;
- Часто змінюйте свій пароль;
- **Використовуйте генератори складних паролів** (включені в деякі програми менеджерів паролів або доступні online).

Правило 5: Не використовуйте однаковий пароль для різних облікових записів та не записуйте пароль на картках і в файлах на комп'ютері

- Створюйте **складний пароль** так, щоб ви могли його легко запам'ятати і ніде не записувати;
- Використовуйте спеціалізоване програмне забезпечення — менеджер паролів, наприклад KeePass.

Правило 6: Не вказуйте/не надсилайте свій логін і пароль іншим особам

- Ніколи **не давайте свій логін і пароль** до пристрою іншим особам;
- Жоден **працівник банку не має права просити вас** про дані для входу. Такі питання від осіб, що представляються як працівники банку, завжди повинні викликати підозри;
- Будьте особливо обережні, **коли вказуєте свої приватні дані в мережі Інтернет**.

Правило 7: Не входьте через загальнодоступну, незахищену мережу WI-FI в мобільний банкінг та інтернет-банкінг

- Використання відкритих та незахищених **WI-FI мереж є великою загрозою**;
- **Не підключайтесь до відкритих WI-FI мереж**, якщо хочете скористатися банкінгом.

Правило 8: Не використовуйте інтернет-банкінг на загальнодоступних пристроях

- Загальнодоступні пристрої **можуть мати вірус** або на них може бути встановлене **зловмисне програмне забезпечення**;
- Загальнодоступні пристрої краще використовувати для читання новин, порталів тощо.

Правило 9: Використовуйте всюди, де це можливо, функцію мультифакторної аутентифікації

- **Зберігайте в таємниці код доступу з SMS або мобільного додатку.**

Правило 10: Не підключайте зовнішні носії даних до свого пристрою, якщо ви в них не впевнені

- Зовнішні пристрої такі, як **USB, ліхтарики тощо, можуть містити зловмисне програмне забезпечення**, яке встановлюється на пристрої без вашого відома, і буде, наприклад, викрадати ваші дані;
- Якщо ви невпевнені, що це за пристрій і чи це безпечно, то краще його не підключайте;
- **Кіберзлочинці можуть навмисно залишати «заражену» флешку з написом, наприклад, «фото» для того, щоб ви хоча б із цікавості підключили її до вашого пристрою.**
Корисна інформація!

Департамент кіберполіції Національної поліції України має свій телеграм канал. У ньому ви можете переглянути усі актуальні новини про викриття правопорушень та махінацій в інтернеті, а також отримати рекомендації, як не потрапити на «гачок» аферистів у мережі. Підписуйтеся: <https://t.me/CyberpolUA>