НОТАРІАЛЬНА ПАЛАТА УКРАЇНИ
NOTARY CHAMBER OF UKRAINE

вул. Хрещатик, 6, оф. 5а,
м. Київ, 01001, Україна
6 Khreshchatyk street, office 5a,
Kyiv, 01001, Ukraine

Комісія з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності

Шановні нотаріуси!

Комісія з питань інформатизації, цифрової трансформації та запобігання кіберзлочинності пропонує вам до ознайомлення інформаційний лист-рекомендації з метою підвищення рівня кібербезпеки, цифрової компетентності, грамотності та дотримання основ кібергігієни серед нотаріусів. Це дозволить забезпечити захист конфіденційної інформації, безперебійну діяльність і стійкість до сучасних кіберзагроз.

Основні кроки для користувача, щоб мінімізувати ризики кібератаки на комп'ютер

Сьогодні нотаріуси працюють з великою кількістю конфіденційної інформації, персональними даними, що робить їх особливо вразливими до **кібератак**.

Кібератака — це спроба зловмисників отримати несанкціонований доступ до комп'ютера користувача, його даних або отримати доступ до інформаційних систем, баз даних, реєстрів, сервісів тощо, до яких має санкціонований доступ користувач. Щоб захистити свої робочі комп'ютери та мінімізувати ризики отримання зловмисником віддаленого доступу чи втрати даних, пропонуємо наступні рекомендації.

Що таке кібергігієна і чому вона важлива?

Кібергігієна — це набір правил і практик для безпечного користування комп'ютерами та мережею. Дотримуючись кібергігієни, ви:

- Захищаєте особисті та робочі дані від несанкціонованого доступу.
- Знижуєте ризик вірусних атак і витоків інформації.
- Забезпечуєте надійну та стабільну роботу вашої техніки.

1. Використовуйте сервіси електронної пошти з функціями захисту від загроз.
Обирайте **поштові сервіси**, які мають вбудовані інструменти для перевірки електронних листів. Такі сервіси автоматично:

- Виявляють **спам** (небажані листи рекламного характеру);
- Блокують **фішингові посилання** (шахрайські посилання, що імітують справжні сайти для крадіжки ваших паролів);
- Перевіряють вкладені файли на наявність **шкідливого програмного забезпечення** (вірусів, троянів, програм вимагачів).

Порада: Gmail, Outlook, Proton та інші популярні сервіси вже мають вбудований захист, але завжди перевіряйте, чи ці функції увімкнені.

2. Вчіться розпізнавати фішингові повідомлення.
Фішинг — це оманливе ніформаційне повідомлення, завдяки якому зловмисники намагаються виманити ваші паролі або іншу чутливу інформацію, змусити вас вчинити негайну дію (яка призведе до завантаження та виконання шкідливого файлу) через підроблені листи електронної пошти.
Як розпізнати фішинг:

- Лист може містити граматичні, орфографічні чи стилістичні **помилки** в тексті або ж виглядати підозріло, непрофесійно;
- В тексті повідомлення вас просять **терміново змінити пароль, ввести пароль** або натиснути на посилання або ж завантажити файл;
- Адреса відправника схожа на офіційну, але має **незначні зміни** (наприклад, замість example.com пишуть examp1e.com).

Порада: Ніколи не натискайте на підозрілі посилання та не відкривайте підозрілі вкладення-файли. Перевірити посилання, або ж підозрілий файл можна за посиланням virustotal.com

3. Використовуйте сучасну операційну систему з автоматичними оновленнями.
Сучасні **операційні системи** (наприклад, Windows 11, macOS) регулярно випускають **оновлення**, що закривають уразливості, які можуть використовувати хакери.

- Увімкніть **автоматичне встановлення оновлень**, щоб не пропустити критичні виправлення;
- Уникайте використання «старих» систем, таких як **Windows 7, Windows 8,** які більше не підтримуються і не отримують оновлень.

Порада: Перевірте, чи актуальна у вас версія операційної системи, чи активна функція оновлень у налаштуваннях вашої системи. За необхідності оновіть операційну систему, встановіть оновлення.

4. Використовуйте антивірусний захист з автоматичним оновленням.
Антивірусний та антишпигунський захист допомагає виявляти та знешкоджувати шкідливе програмне забезпечення. Основні вимоги до антивіруса:

- Він має **автоматично оновлюватися** для захисту від нових загроз;
- Включати функцію **постійного моніторингу** активності на комп'ютері.

Порада: Використовуйте надійні антивірусні програми, наприклад Windows Defender, Bitdefender, ESET, AVG.

5. Працюйте на комп'ютері під обліковим записом "Користувач", а не "Адміністратор".
У більшості випадків користувачі працюють під роллю **Адміністратора**, що відкриває доступ до всіх налаштувань системи. Це небезпечно, адже вірус або шкідливе програмне забезпечення, у разі його запуску під роллю «Адміністратор» може отримати усі адміністративні права.

- Створіть окремий **обліковий запис "Користувач"** для щоденної роботи;
- Роль **Адміністратора** використовуйте лише для встановлення програм або зміни налаштувань.

Пояснення: Робота під обмеженими правами мінімізує ризики внесення шкідливих змін до системи.

6. Обов'язково використовуйте надійний пароль для користувача операційної системи. Захистіть доступ до вашого комп'ютера паролем, що відповідає **основним вимогам безпеки**:

- Обов'язкова встановіть пароль користувача для входу в операційну систему на комп'ютері;
- Пароль має складатися мінімум із **8 символів** (великі та малі літери, цифри, спеціальні символи);
- Уникайте очевидних паролів (дата народження, ім'я, "12345");
- Не використовуйте **один і той самий пароль** для різних облікових записів.

Порада: Додатково увімкніть **двофакторну аутентифікацію (2FA)**, де це можливо, щоб підвищити рівень захисту.

7. Політика замкненого екрана — це важливий елемент забезпечення інформаційної безпеки в діяльності. Коли ви залишаєте своє робоче місце, заблокуйте екран свого комп'ютера (або ж налаштуйте автоматичне блокування), щоб запобігти несанкціонованому доступу до інформації. Ця політика мінімізує ризики витоку даних, зменшує ймовірність випадкового доступу сторонніх осіб до важливої інформації та сприяє підтриманню загального порядку на робочих місцях.

Захист робочого комп'ютера від кібератак — це обов'язок кожного нотаріуса. Виконуючи базові правила безпеки, ви мінімізуєте ризики і захищаєте як свої дані, так і осіб які звертаються до вас. **Безпека в цифровому світі залежить від ваших дій та обізнаності.**

03.02.2025

З повагою,
Голова комісії **Наталія КОЗАЄВА**