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 нотаріуса, 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 вашого комп’ютера, даних або отримати доступ до Єдиних та державних реєстрів. Щоб захистити свої робочі комп’ютери та мінімізувати ризики отримання зловмисником віддаленого доступу чи втрати даних, пропонуємо дотримуватися наступних рекомендацій:

---

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).

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

---

2. Вчіться розпізнавати фішингові повідомлення.
Фішинг — це обман, коли зловмисники намагаються виманити ваші паролі або інші дані, смусити вас вчинити дію (яка призведе до завантаження та виконання шкідливого файлу) через підроблені листи. Як розпізнати фішинг:

- Лист може мати **помилки** в тексті або виглядає підозріло непрофесійно.

- Вас просять **терміново ввести пароль** або натиснути на посилання або скачати файл.
- Адреса відправника виглядає схоже 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.

---

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.

- Вмикайте **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 з 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 зловмисне ПЗ може отримати ті ж права, що і Адміністратор (тобто усі 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**:

- Мінімум **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 акаунтів.

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

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.

Висновок:
Захист комп’ютера від кібератак — це обов’язок кожного нотаріуса. Виконуючи базові правила безпеки, ви мінімізуєте ризики і захищаєте як свої дані, так і дані ваших клієнтів.

Пам’ятайте: **безпека в цифровому світі залежить від ваших дій та обізнаності.**

19.12.2024

З повагою,
Голова комісії **Наталія КОЗАЄВА**