Натиснули на фішингове посилання? Не втрачайте час

План першочергових дій після підозрілої активності

Не кожен перехід за посиланням означає зараження комп’ютера. Але введення пароля, запуск невідомої програми або передача особистого ключа КЕП можуть мати серйозні наслідки.

Насамперед: негайно повідомте IT-фахівця або відповідального за кібербезпеку. Не приховуйте інцидент.

Ситуація 1. Ви перейшли за підозрілим посиланням

- [ ] Припиніть взаємодію з підозрілою сторінкою.
- [ ] Не вводьте паролі, коди підтвердження та інші дані.
- [ ] Нічого не завантажуйте та не запускайте.
- [ ] Повідомте відповідального фахівця й передайте адресу сторінки для перевірки.

Важливо: сам перехід не завжди призводить до компрометації, але може потребувати перевірки.

Ситуація 2. Ви ввели пароль або код підтвердження

- [ ] Негайно повідомте IT-фахівця.
- [ ] З іншого перевіреного пристрою змініть скомпрометований пароль.
- [ ] Завершіть активні сеанси та перевірте підключені пристрої.
- [ ] Перевірте налаштування багатофакторної автентифікації.
- [ ] Якщо це корпоративна пошта, перевірте правила автоматичного пересилання повідомлень і дозволи сторонніх застосунків.
- [ ] Перевірте інші системи, де міг використовуватися той самий пароль.

Ситуація 3. Ви відкрили підозрілий файл або запустили програму

- [ ] Негайно повідомте IT-фахівця.
- [ ] Ізолюйте пристрій від мережі відповідно до інструкцій фахівця.
- [ ] Не продовжуйте роботу з банкінгом, КЕП та корпоративними обліковими записами на цьому пристрої.
- [ ] Не видаляйте самостійно файли та не намагайтеся приховати сліди інциденту.
- [ ] Передайте пристрій для перевірки. Не відновлюйте звичайну роботу до дозволу відповідального фахівця.

Ситуація 4. Ви передали файл особистого ключа КЕП або підозрюєте його викрадення

- [ ] Негайно припиніть використання відповідного ключа.

- [ ] Зверніться до свого кваліфікованого надавача електронних довірчих послуг для блокування або скасування сертифіката.
- [ ] Повідомте керівника та відповідального за кібербезпеку.
- [ ] Перевірте доступні відомості про документи й операції, які могли бути підписані без вашого відома.
- [ ] Організуйте отримання нового ключа та перегляд захисту середовища підписання.

Пам’ятайте: просто змінити пароль може бути недостатньо, якщо сам файл ключа вже скопійовано.

Ситуація 5. Ви оплатили підозрілий рахунок або виявили підміну реквізитів

- [ ] Негайно зателефонуйте до банку за офіційним номером.
- [ ] Повідомте про підозру на шахрайство та попросіть перевірити можливість зупинки або повернення платежу.
- [ ] Перевірте, чи не було інших несанкціонованих операцій.
- [ ] Повідомте керівництво й фінансовий підрозділ.
- [ ] Збережіть рахунок, листування, банківські реквізити й час операцій.
- [ ] Зв’яжіться зі справжнім контрагентом через перевірений канал.

Що потрібно зробити після будь-якого підтвердженого інциденту

- [ ] Збережіть докази: повідомлення, вкладення, знімки екрана, час подій та доступні журнали.
- [ ] Перевірте, чи не отримали зловмисники доступ до інших систем.
- [ ] Попередьте контрагентів, якщо від вашого імені могли надсилатися шахрайські повідомлення.
- [ ] За необхідності повідомте CERT-UA або Кіберполіцію.
- [ ] Перед відновленням звичайної роботи переконайтеся, що причина компрометації усунена.

Контакти, які варто заповнити заздалегідь

Відповідальний за кібербезпеку:

Телефон IT-фахівця:

Контакт банку:

Надавач послуг КЕП:

Контакт керівника:

Найголовніше

Швидкість повідомлення про інцидент має значення.

Не потрібно самостійно з’ясовувати всі обставини, перш ніж звернутися по допомогу. Вчасне реагування може обмежити наслідки атаки.