Кібербезпека LNZ Group

Коротка пам’ятка з головними правилами. Повна версія з поясненнями — у директиві з кібербезпеки на сайті SEOWORK. Від вас не вимагають стати спеціалістом: не поспішати, перевіряти незвичні запити іншим каналом і одразу повідомляти, якщо щось пішло не так.

П’ять правил, що закривають більшість ризиків

- Один пароль — один сервіс. Витік в одному місці не має відкривати решту.
- MFA скрізь. Пошта, VPN, хмара, фінанси, CRM. Без другого фактора пароля недостатньо.
- Не поспішати під тиском. «Терміново», «штраф», «оплатіть сьогодні» — сигнал небезпеки.
- Робочі файли — тільки в робочих системах. Не на особисту пошту й не в приватну хмару.
- Знати, кому повідомити. Контакт IT — заздалегідь, а не в момент інциденту.

Паролі та MFA

- Довжина від 14 символів; фраза з кількох слів краща за короткий складний набір.
- Менеджер паролів замість файлу «паролі.xlsx».
- Другий фактор — додаток-аутентифікатор або ключ; SMS лише за відсутності іншого.
- Ніхто — ні IT, ні керівництво, ні банк — ніколи не просить ваш пароль чи код із MFA.
- Запит на підтвердження входу, якого ви не ініціювали: відхилити, зафіксувати час, повідомити IT.

Фішинг — на що дивитись

- Домен відправника: підміна однієї літери — класика (rn замість m).
- Посилання: наведіть курсор і подивіться реальну адресу, тоді дійте.
- QR-код перевіряйте так само, як посилання — камера не показує адресу заздалегідь.
- Голос керівника по телефону вже підробляють. Незвичне прохання про оплату — передзвоніть на відомий номер.
- Зміна реквізитів чи IBAN — тільки після підтвердження іншим каналом.

Правило подвійної верифікації платежів: будь-яка зміна реквізитів або несподіване прохання про оплату підтверджується дзвінком на раніше відомий номер, а не на той, що в листі.

Кібербезпека LNZ Group

Що робити, якщо клікнув

- 1. Від’єднайте пристрій від мережі (Wi-Fi або кабель).
- 2. Нічого не «лікуйте» самостійно й не вводьте паролі на цьому пристрої.
- 3. Не вимикайте і не перезавантажуйте пристрій без вказівки IT.
- 4. Не видаляйте підозрілий лист чи файл — вони потрібні для розслідування.
- 5. Одразу повідомте IT. Паролі змінюйте з іншого, чистого пристрою.

Робочі дані та пристрої

- Не завантажуйте договори, персональні й фінансові дані, паролі та внутрішнє листування у ChatGPT та інші непогоджені ШІ-сервіси.
- Не підключайте знайдені, особисті чи непогоджені USB-флешки й диски.
- Не встановлюйте програми та розширення браузера без погодження IT.
- Про втрату телефона, ноутбука чи носія повідомляйте негайно — навіть якщо він під паролем.

Куди повідомляти

Пошта IT та безпеки: vsmotritel@lnz.com.ua
Онлайн-форма: seowork.in.ua/forma-inczendentu/

У повідомленні коротко: що сталося, коли, на якому пристрої, які дані ви могли ввести. За повідомлення про інцидент не карають — карає замовчування.