7 перевірок перед тим, як відкрити лист

Новий тендер, рахунок від постачальника, документ на підпис чи повідомлення від керівника? Перш ніж переходити за посиланням, відкривати вкладення або виконувати прохання, перевірте сім речей.

☐ **1. Чи очікували ви це повідомлення?**

Ви справді брали участь у цій закупівлі, очікували рахунок або домовлялися про отримання документа? Неочікуване повідомлення - привід для додаткової перевірки.

☐ **2. Чи справжня адреса відправника?**

Перевірте повну адресу електронної пошти та домен. Шахраї можуть замінити одну літеру, додати дефіс або використати схожу назву.

☐ **3. Чи не змушують вас поспішати?**

«Терміново!», «До 17:00», «Ваш акаунт буде заблоковано», «Пропозицію потрібно подати негайно» - такі формулювання можуть використовуватися для психологічного тиску.

☐ **4. Чи безпечне посилання?**

Перевірте справжню адресу сайту, а не лише текст посилання. Якщо повідомлення стосується закупівлі на SmartTender, самостійно відкрийте офіційний сайт smarttender.biz і знайдіть відповідну процедуру.

☐ **5. Чи немає підозрілих вкладень?**

Будьте особливо уважні до неочікуваних архівів із паролями, подвійних розширень файлів, виконуваних програм і документів, які вимагають увімкнути макроси. Не запускайте невідомі файли.

☐ **6. Чи не просять вас передати конфіденційні дані?**

Пароль, одноразовий код, файл особистого ключа КЕП або доступ до комп’ютера не можна передавати стороннім особам через листування чи месенджери.

☐ **7. Чи не просять змінити звичайний порядок роботи?**

Новий IBAN, термінова оплата без погодження, повідомлення від «директора» з незнайомого акаунта або прохання нікому не розповідати про платіж - підстави зупинитися й перевірити запит.

ГОЛОВНЕ ПРАВИЛО

Не впевнені — не переходьте, не завантажуйте, не оплачуйте.

Зв’яжіться з відправником через інший, заздалегідь перевірений канал: номер телефону з договору, офіційний сайт або внутрішній корпоративний контакт.