

РАХУНКИ Й ПЛУТНІ

ЩО ВІДБУВАЄТЬСЯ?

- До підприємства звертається нібито представник постачальника товарів/послуг або кредитора.
- Він може зателефонувати, написати листа або звернутися електронною поштою тощо.
- Шахрай наполягає на використанні нових банківських реквізитів (тобто даних одержувача платежу) в майбутніх рахунках-фактурах. Але новий банківський рахунок належить самому шахраю.



ЯК ДІЯТИ?

Довести до працівників інформацію про цей тип шахрайства та способи протидії.

Упровадити **регламент перевірки** автентичності платіжних вимог.

Перевіряти всі запити кредиторів, особливо ті, де вимагається в подальших рахунках змінити банківські реквізити.

Не брати контактні дані з листів, факсів, електронної пошти з вимогою змін. Користатися даними з **минулого листування**.

Домовитися **про відповідальних контактних осіб** з компаніями, яким ви регулярно платите.

КЕРІВНИКАМ



Наказати відповідальним за оплату рахунків **перевіряти їх усі на коректність**.

Перевірити дані, наведені на веб-сайті компанії, зокрема, про угоди й постачальників. Знеохотити підлеглих наводити зайві відомості про компанію в соцмережах.

Для платежів понад встановлений ліміт **впровадити порядок підтвердження** коректності номера рахунку й одержувача (наприклад, через особисту зустріч).

СПІВРОБІТНИКАМ



Не давати зайвої інформації в соцмережах про компанію, де працюєте.

По оплаті рахунку **повідомляти одержувача електронним листом**. Вказувати банк одержувача та, задля безпеки, чотири останні цифри номера його узгодженого рахунку.



Про спробу шахрайства неодмінно заявляйте у Кіберполіцію, навіть якщо ви не постраждали.