ГЕНДИРЕКТОР І ПЛУТНІ

Шахрай, вводячи в оману відповідального за здійснення платежів співробітника компанії, переконує його сплатити фальшивий рахунок або переказати гроші на рахунок, що належить шахраю.

ЩО ВІДБУВАЄТЬСЯ?

Шахрай телефонує чи пише листа, видаючи себе за генерального або фінансового директора.

З порядками в організації він чудово обізнаний.

Вимагає спішно провести платіж.

Каже щось на кшталт: «Це таємно», «Фірма Вам довіряє», «Я зараз не можу це зробити сам».

Часто гроші переказуються на інші рахунки, що відкриті за кордоном.

Працівник переказує гроші на рахунок, яким розпоряджається шахрай.

Додаткові вказівки можуть надходити від сторонньої особи або електронною поштою.

Посилається на надзвичайні обставини (податкову перевірку, злиття, поглинання).

Вимагає від працівника не дотримуватися чинного порядку узгодження.

ЯК РОЗПІЗНАТИ?

- Несподіваний лист чи дзвінок
- Звертання керівника вищої ланки, з яким ви зазвичай не маєте справи
- Вимога повної конфіденційності
- Тиск, наполегливе спонукання до швидких дій
- Незвичне розпорядження, що суперечить внутрішнім процедурам компанії
- Погрози або улесливість, обіцянки винагороди

ЯК ДІЯТИ?

КЕРІВНИКАМ

Знати про ризики, забезпечувати **належну поінформованість підлеглих.**

Спонукати підлеглих бути **особливо обачними під час здійснення платежів**.

Впровадити регламент, який регулює здійснення платежів в компанії.

Впровадити **порядок перевірки** платіжних доручень, отриманих електронною поштою.

Впровадити **процедури звітування** для протидії шахрайству.

Переглянути відомості на сайті компанії, **заборонити наводити зайві дані й закликати до обачності** в соцмережах.

Привести у відповідність до сучасних вимог технічні засоби безпеки.

Неодмінно заявляти про спроби шахрайства в Кіберполіцію, навіть у разі відсутності збитків.

СПІВРОБІТНИКАМ

Неухильно дотримуватись чинних регламентів безпеки платежів і закупівель. **Не оминати виконання жодної вимоги безпеки. Не поступатися тиску**.

Ретельно **перевіряти адресу електронної пошти**, якщо маєте справу з чутливою інформацією або грошовими переказами.

Радитися з обізнаними колегами щодо сумнівних платіжних доручень.

Не переходити за підозрілими гіперпосиланнями та **не відкривати сумнівних вкладень**, отриманих електронною поштою. Особливо пильнувати під час перевірки приватної пошти на службовому комп'ютері.

Не надавати зайвих відомостей, бути обачним у соцмережах.

Не розкривати чутливу інформацію про оргструктуру, безпеку та процедури компанії.

Неодмінно сповіщати про підозрілі електронні листи й телефонні дзвінки ІТ-службу вашої компанії.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | EMA

#CyberScams