ИЗМАМИ С КОМПРОМЕТИРАНИ БИЗНЕС ИМЕЙЛИ/ИМЕЙЛИ, ПРИВИДНО ИЗПРАТЕНИ ОТ РЪКОВОДИТЕЛ В КОМПАНИЯ

Тази измама възниква, когато служител, упълномощен да извършва плащания, е подмамен да плати фалшива фактура или да направи неразрешен превод от сметката на компанията.

КАК РАБОТИ ИЗМАМАТА?

Измамникът се обажда или изпраща имейл, представяйки се за високопоставено лице в компанията (например, главен изпълнителен директор или финансов директор).

Измамниците имат добри познания за компанията.

Те изискват спешно плащане.

Те използват думи като "Поверителност", "Компанията ти има доверие", "В момента не съм на разположение".

Искането е често за международни плащания към банки извън Европа.

Служителят прехвърля средства към сметка, контролирана от измамника.

Инструкции как да се процедира може да се дадат по-късно, от трето лице или по електронна поща.

От служителя се изисква да не спазва стандартните процедури за одобрение.

Те споменават деликатна ситуация (например, данъчен контрол, сливане, придобиване).

КАКВИ СА ПРИЗНАЦИТЕ?

- Неочакван имейл/телефонно обаждане
- Пряк контакт от високопоставен служител, с когото обичайно не комуникирате
- Искане за абсолютна поверителност
- Натиск и чувство за неотложност
- Необичайна молба в противоречие с вътрешните процедури и правила
- Заплахи или необичайно ласкателство/обещания за възнаграждение

КАКВО МОЖЕТЕ НА НАПРАВИТЕ?

АКО СТЕ КОМПАНИЯ

Бъдете наясно с рисковете и се уверете, че **служителите също са информирани и внимателни.**

Насърчавайте служителите си **да обръщат повишено внимание на исканията за плащане.**

Въведете вътрешни протоколи при плащания.

Въведете процедура за верификация на заявките за плащане, получени по имейл.

Създайте **отчетни процедури** за управление на измамите.

Прегледайте информацията, публикувана на уебсайта на фирмата ви, **ограничавайте информацията и проявявайте предпазливост** по отношение на социалните мрежи.

Повишавайте и актуализирайте редовно техническата сигурност.

Винаги се свързвайте с полицията в случай на опити за измама, дори и да не сте станали жертва.

АКО СТЕ СЛУЖИТЕЛ

Прилагайте стриктно въведените процедури за сигурност за плащания и доставки. **Не пропускайте стъпки и не се поддавайте на натиск.**

Винаги **внимателно проверявайте имейл адресите**, когато работите с чувствителна информация/парични преводи.

В случай, че се съмнявате за нареждане за плащане, **консултирайте се с компетентен колега.**

Никога не отваряйте подозрителни линкове или прикачени файлове, получени по имейл. Бъдете особено внимателни, когато проверявате личния си имейл от служебен компютър.

Ограничавайте информацията и проявявайте предпазливост по отношение на социалните мрежи.

Избягвайте да споделяте информация относно йерархията, сигурността и процедурите в компанията.

Ако получите подозрителен имейл или телефонно обаждане, винаги уведомявайте ИТ отдела на компанията.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Асоциация на банките в България

#CyberScams