Информационен бюлетин за измамни схеми – Пренасочване на преводи

Както точно представлява?

Това явление е известно също като "мандатна измама" или "измамите с поглъщане на доставчици". В него се включва промяната на данните за сметките на доставчиците или клиентските сметки в комбинация с дебитни нареждания, манипулиране на дейностите с кредитни карти или промяна на данните за заплатите на служителите, особено когато се дължи бонус.

Предупредителни сигнали

• неочаквани искания за промяна или актуализиране на данните за плащане на редовен доставчик.
• независимо дали е по телефона, електронната поща или чрез писмо/факс, ако с фирмата Ви се свърже контрагент и внезапно Ви уведоми, че е променил платежните си детайли и иска да му плащате по друга сметка, винаги третирайте това като потенциален предупредителен сигнал.
• ако лицето по телефона е агресивно се опитва да ускори изпълнението на плащане.

Контакти

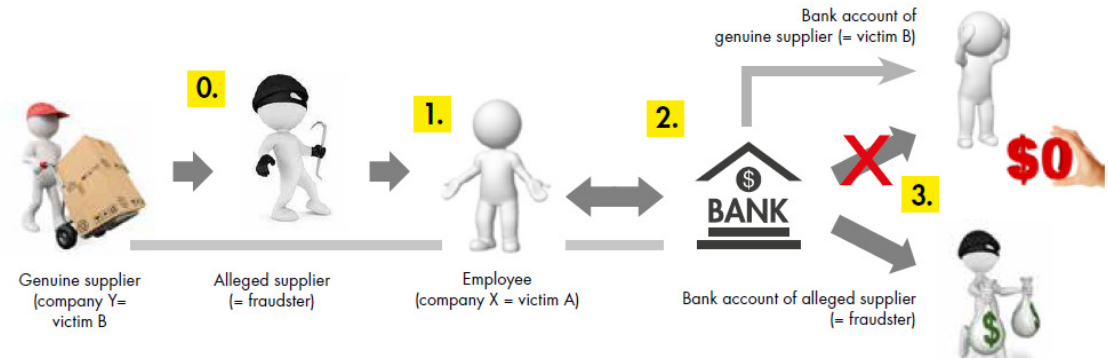
За въпроси/сигнали можете да се обръщате към обслужващия офис или Кол центъра на Райфайзенбанк (България) ЕАД.
имейл: call.center@raiffeisen.bg
телефон: 0700 10 000 (Vivacom); 17 21 (Mtel и Telenor)

Измамна схема

Кореспонденцията между двама бизнес партньори е пресечена (или „хакната“) и на платеца се изпращат фалшиви имейли, съдържащи оригинални фактури, които претендират, че са от съществуващ кредитор/доставчик, но платежните детайли са променени. Имейлът има за цел да уведоми получателя за новите (променени) данни относно банковата сметка, по която трябва да бъдат изпратени всички бъдещи плащания. В повечето случаи платецът разбира, че е бил измамен, след като е изпратил поне едно плащане в полза на измамната сметка, а първоначалният получател на средствата потвърди, че не е получил средства.

Основни елементи – как работи?

0. Редовни плащания от компания X към контрагент (напр. доставчик) компания Y.
1. Измамникът се свързва с компания X чрез телефон/ имейл/ писмо, като твърди, че е представител на компания Y (най-честият начин за контакт е имейл, като имейлите се изпращат от хакнат акаунт на истинския доставчик). Имейлът цели да уведоми компания X, че платежните детайли /сметка/ е променена и в повечето случаи има и прикачена инструкции за заплащане по текуща фактура.
2. Служител на компания X променя сметката в тяхната база.
3. От този момент всяко едно бъдещо плащане се изпраща към сметката на измамника.
4. В повечето случаи платецът осъзнава, че е попаднал в измамна схема след като контрагентът му се свърже с него и го информира, че не е получил дължимо плащане.



Внимание: Промяната на банковите сметки е необичаен процес и следователно всяко искане за актуализиране на платежните детайли от контрагент трябва да бъде третирано подозрително. Промените трябва да се разрешават само на висше ниво и след надлежна проверка.

Съвети как да се предпазите

• Отнасяйте към всяко уведомление за промяна на данните за банковата сметка на доставчика като високорискова дейност.
• Винаги проверявайте искането ПРЕДИ да извършите промяната или да извършите плащането. Не забравяйте да не използвате данните за контакт, предоставени в инструкцията, вместо това използвайте установените координати за връзка, за да потвърдите промяната. (Например, ако актуализацията е получена по електронна поща, потвърдете я по телефона или по факса, като използвате известен преди това номер).
• Преглеждайте движенията по сметките си ежедневно, за да идентифицирате бързо потенциалните измами.
• Никога не оставяйте фактури без надзор в офиса или на бюрото си.
• Когато е възможно, нека се установят поне два канала за контакт или две лица за контакт с доставчици, на които се извършват редовни плащания, така че всички фактури да могат да бъдат потвърдени с тях особено при съмнение.
• Инструктирайте служителите си, отговарящи за плащането на фактурите да правят проверка на документите за нередности и да проверяват техните притеснения относно компанията, която изисква плащане.