БСПБ

Уважаемые руководители и собственники бизнеса!

ВНИМАНИЕ!

Уведомляем вас о новой массовой схеме мошенничества, с которой уже столкнулись все банки и их клиенты. Просим ВНИМАТЕЛЬНО изучить данную информацию и довести ее до ваших сотрудников во избежание финансовых потерь от атаки мошенников

В последнее время хакеры атакуют различные ресурсы, в том числе бюджетных организаций и компаний.

Вследствие данных атак отдельные ресурсы взламываются, и мошенники получают информацию о сотрудниках организации. Это могут быть номера телефонов, адреса корпоративной почты и т.п.

Далее мошенники строят линию атаки, направленную на сотрудника организации, и используют полученную информацию для повышения доверия:

• в сети интернет находят фото руководителя организации, главврача, директора, ректора и т.п.

• звонят или пишут жертве в мессенджере от имени руководителя, используя его фото в качестве фотографии контакта

• в разговоре/переписке сотруднику сообщают о необходимости быть на связи, так как его разыскивает ФСБ, полиция, налоговая, ЦБ или иной гос. орган

• получив такой звонок якобы от руководителя, жертва уже подготовлена к следующему звонку от мошенников

• вместо звонка от руководителя организации или в дополнение к нему – жертве может быть направлено письмо на адрес корпоративной почты с официального адреса организации или от руководителя. В письме сообщается о проверке ФСБ, Следственного комитете и т.п., запрашиваются сведения о сотруднике и его личных доходах. Также в письме просят оставаться на связи, сохранять спокойствие и никому не сообщать о поступлении такого запроса

• далее поступает звонок или сообщение якобы от сотрудника ФСБ, следователя, налоговой, ЦБ или иного гос. органа

• в звонке жертве сообщают о расследовании утечки личных данных и конфиденциальной информации, могут убеждать человека, что на него пытаются взять кредит или вывести его деньги. Мошенники угрожают уголовной ответственностью за разглашение деталей проводимых мероприятий и запрещают говорить кому-либо о данной ситуации, включая родственников и тем более сотрудников Банка

• в конечном итоге человека так или иначе пытаются убедить взять кредит или снять все деньги и перевести их на некие «резервные» или «страховые» счета, «депозитные» ячейки, оформить «зеркальный кредит», провести процедуру «замены (обнуления) лицевого счета»

ЗАПОМНИТЕ – ЭТО МОШЕННИКИ!

Они хотят заставить Вас любыми способами вывести Ваши средства, чтобы завладеть ими

Что делать в этой ситуации?

- Не предпринимайте никаких действий под руководством звонящих, не раскрывайте информацию о себе
- Сразу же звоните в Банк и обращайтесь лично в отделение полиции

Помните!

- НИКТО, независимо от должности, НИКОГДА не может требовать от Вас совершать финансовые операции, оформлять кредиты, закрывать вклады
- Нельзя сообщать данные для входа в интернет-банк, коды из СМС
- Нельзя устанавливать на Ваш телефон никакие программы под руководством звонящих

Выполнение Вами рекомендаций Банка по безопасности, совместно с предпринимаемыми Банком мерами, поможет сохранить Ваши денежные средства.

С уважением,
Банк «Санкт-Петербург»