Телефонные мошенники, или как сохранить свои деньги.

В Беларуси участились случаи противоправных деяний, связанных с хищениями денежных средств с использованием телефонных звонков — вишинга.

Злоумышленники звонят клиентам белорусских банков, представляются сотрудниками банковских учреждений, после чего под разными предлогами убеждают сообщить данные о платежных реквизитах банковской платежной карточки, паспортные данные, коды, приходящие на абонентский номер, логины и пароли от системы дистанционного банковского обслуживания. Для противоправной деятельности зачастую используется специализированное программное обеспечение. В таком случае при входящем звонке клиент банка будет видеть на своем телефоне номер банка, размещенный на официальном сайте. Для убедительности злоумышленники используют в качестве фона звонка шум работающего колл-центра банка.

Основная схема противоправных деяний выглядит следующим образом: при звонке злоумышленник представляется работником банка, сообщает, что в отношении счета клиента производятся мошеннические действия. Далее, для предотвращения якобы несанкционированного перевода либо хищения денег, клиенту нужно предоставить информацию о банковской платежной карточке либо другие данные.

В ряде случаев злоумышленник звонит держателю карточки и сообщает о том, что на его имя якобы оформлен кредит. Для его отмены также нужна уточняющая информация.

Обращаем Ваше внимание, что при звонке клиенту банк всегда знает всю необходимую информацию о его счете. Сообщать третьим лицам данные о реквизитах банковской платежной карты, паспортные данные, коды поступающие в сообщениях банка запрещено в соответствии с договором банковского обслуживания. В случае поступления подобных звонков, рекомендуем завершить общение и перезвонить на номер банка, указанный на его официальном сайте с целью выяснения всех обстоятельств.

Акцентируем внимание, что злоумышленники выманивают деньги через «взломанные» страницы или страницы-клоны («фейковые страницы») в социальных сетях. В данных случаях, якобы от имени друга приходит сообщение с просьбой дать данные банковской карточки для перевода денег.

Злоумышленники также могут действовать в роли покупателей: под предлогом заинтересованности они обращаются к продавцу и сообщают о намерении купить его товар в интернете. Продавцу

предоставляют ссылку, перейдя по которой он вводит свои реквизиты банковской платежной карты, которые в последствии становятся известными злоумышленнику. Последний, использует их для хищения денежных средств со счета жертвы.

Зафиксировано немало случаев, когда злоумышленники просят мобильный телефон под предлогом звонка, после чего устанавливают на него программное обеспечение для несанкционированных денежных переводов.

Волна звонков телефонных мошенников продолжается. Отдел по раскрытию преступлений в сфере высоких технологий рекомендует проявить бдительность, никому не передавать конфиденциальную информацию.

ОРПСВТ КМ УВД Гомельского облисполкома