Как не стать жертвой киберпреступника

В Беларуси участились случаи телефонного мошенничества — вишинга. Мошенники звонят клиентам белорусских банков, представляются сотрудниками службы безопасности либо просто сотрудниками банка, под тем или иным предлогом просят предоставить данные о банковской платежной карточке, паспортные данные, коды, приходящие на телефонный номер, логины и пароли от системы дистанционного банковского обслуживания.

Злоумышленники также могут использовать программы-анонимайзеры. В таком случае при входящем звонке клиент банка будет видеть на своем телефоне номер банка, размещенный на официальном сайте. Вместе с тем мошенники могут подменить не телефонный номер целиком, а одну цифру в нем. Таким образом, клиенту сложнее визуально идентифицировать оригинальность номера банка. Для большей правдоподобности злоумышленники используют в качестве фона звонка шум работающего колл-центра банка.

Один из основных сценариев обмана выглядит следующим образом: при звонке злоумышленник представляется работником банка, сообщает, что в отношении счета клиента производятся мошеннические действия. По легенде, чтобы предотвратить несанкционированный перевод либо снятие денег в банкомате, клиенту нужно предоставить информацию о банковской платежной карточке либо другие данные.

Обращаем Ваше внимание, что при звонке клиенту банк всегда знает всю необходимую информацию. Сообщать кому-либо данные о банковской карточке, паспортные данные, коды категорически запрещено. Как только собеседники начинают узнавать подобную информацию, рекомендуем завершить звонок и перезвонить на номер банка, указанный на его официальном сайте.

Кроме того, акцентируем внимание, что мошенники выманивают деньги через взломанные страницы или страницы-клоны («фейковые страницы») в социальных сетях — якобы от имени друга приходит сообщение с просьбой дать данные банковской карточки для перевода денег. Злоумышленники также могут притворяться покупателями: под маской заинтересованности они обращаются к продавцу и говорят о намерении купить его товар в интернете. Продавцу предоставляют ссылку, перейдя по которой клиент вводит свои реквизиты, и тем самым передает их злоумышленнику. В дальнейшем мошенник использует их для денежных переводов.

Зафиксировано немало случаев, когда злоумышленники просят мобильный телефон под предлогом звонка, а затем устанавливают на него программное обеспечение для несанкционированных денежных переводов. Волна звонков телефонных мошенников продолжается. Отдел по раскрытию преступлений в сфере высоких технологий ОВД администрации Первомайского района г. Витебска рекомендует проявить бдительность, никому не передавать конфиденциальную информацию.