Материал к теме: «О возможных схемах работы мошенников и рекомендации по выявлению злоумышленников»

По информации Следственного комитета Республики Беларусь: в последнее время правоохранительными органами фиксируется рост количества преступлений, связанных с хищениями денежных средств граждан с использованием компьютерной техники. О ряде популярных способов, которыми пользуются в эти дни преступники, сообщалось не раз различными средствами массовой информации, правоохранительными органами и банками. За 10 месяцев этого года зарегистрировано 7,7 тыс. преступлений в сфере высоких технологий. Это в 2,2 раза больше, чем за аналогичный период прошлого года. Больше всего таких преступлений зарегистрировано в Минске – 1959, **в Гродненской области - 524.** Со счетов пострадавших с января по октябрь 2019 года всего было похищено 6,1 миллиона рублей, из этой суммы 64,9% было возвращено владельцам.

Недавно сотни белорусов стали жертвами так называемого вишинга - телефонного мошенничества, связанного с выманиванием у держателей банковских карт конфиденциальной информации. По фактам вишинга за ноябрь зарегистрировано около 400 преступлений.

Национальный банк Республики Беларусь информирует:

Информация о возможных схемах работы мошенников и рекомендации по выявлению злоумышленников

В настоящее время наиболее **распространенными методами социальной инженерии** у злоумышленников являются:

- метод выманивания реквизитов банковских платежных карточек с использованием взломанных аккаунтов друзей в социальных сетях, когда от имени друга просят сообщить реквизиты карточки либо совершить определенные действия по переводу денежных средств посредством систем дистанционного банковского обслуживания;
- метод с”лже-покупателем“, когда злоумышленник под видом покупателя связывается с клиентом банка – продавцом (который разместил объявление о продаже товара в интернете) и под предлогом внесения залога перед покупкой товара предоставляет продавцу ссылку на мошеннический сайт (визуально похожий на официальный сайт банка) для получения денежного перевода;
- вишинг – вид мошенничества, заключающийся в том, что злоумышленник, используя телефонную коммуникацию и играя определенную роль (например, сотрудника банка), под разными предлогами узнает у держателя карточки конфиденциальную информацию (реквизиты карточки, номер паспорта, личный идентификационный номер,

другие аутентификационные данные, в том числе логины, пароли, СМС-коды) или стимулирует к совершению определенных действий со счетом или карточкой;

- метод с использованием смартфона – под предлогом совершения звонка злоумышленник просит смартфон, незаметно устанавливает не нем программное обеспечение (регистрируется в межбанковской системе идентификации, получает доступ для совершения операций в системе расчетов с использованием электронных денег и т.п.) посредством которого осуществляет переводы денежных средств (электронных денег).

Обращаем внимание, что для защиты денежных средств клиентов у банка есть вся необходимая информация. Банк не должен спрашивать у вас ни реквизиты карточки, ни паспортные данные.

Поэтому **НИКОГДА НИКОМУ НЕ СООБЩАЙТЕ:**

- информацию, размещенную на вашей банковской платежной карточке (на обеих сторонах): номер, дату, код;
- коды, которые банк направляет вам в виде СМС, коды на отдельной карте, выданной в банке, логин и пароль, иные цифровые или буквенные коды;
- паспортные данные: номер паспорта, личный номер и т.д.

В случае поступления подобных звонков**НЕМЕДЛЕННО**завершите разговор, обратитесь в контакт-центр банка, выпустившего карточку (по номеру с официального сайта банка или указанному на вашей карточке), расскажите о ситуации и далее следуйте рекомендациям сотрудника банка.

НИКОМУ НЕ ДАВАЙТЕ в руки свой мобильный телефон и предупредите об этом ваших близких, особенно детей и лиц пожилого возраста!