**Профилактика преступлений, связанных с неправомерным завладением реквизитами пластиковых банковских карт и хищением средств с карт-счетов граждан, а также в сфере высоких технологий**

Глобальная всемирная сеть Интернет все чаще используется в преступных целях. Расширяющиеся технические возможности компьютеров, их программного обеспечения, активно развивающиеся сети сотовой связи, возможности хранилищ электронной информации, совершенствующиеся навыки пользователей, а также возрастающие их материальные возможности способствуют созданию новых способов, средств и объектов преступных киберпосягательств.

В связи с динамичным и масштабным ростом киберугроз и киберпреступлений, причиняемого ими ущерба юридическим и физическим лицам, такие угрозы и преступления представляют серьезную проблему для общества, а борьба с ними является актуальной и стратегически важной задачей для правоохранительных органов, особенно в части, касающейся реализации мер, направленных на эффективное противодействие росту киберпреступлений, своевременное установление лиц, совершивших преступные деяния, получение доказательств, подтверждающих совершение преступления.

На протяжении последних лет на территории Гродненской области наблюдается тенденция существенного роста преступности в сфере высоких технологий.

Основная часть таких противоправных деяний связана с несанкционированным доступом к личным страницам граждан в социальных сетях, последующим получением от их имени реквизитов банковских пластиковых карт иных лиц и хищением с карт-счетов граждан денежных средств (статьи 349 и 212 УК).

Регистрируемые преступления в сфере высоких технологий обладают определенной спецификой, при этом отчетливо видна тенденция серийного распространения однотипных преступлений, подходы к документированию и раскрытию которых также идентичны.

Например, еще два-три года назад к таким преступлениям можно было отнести факты перенаправления пользователей на сайты в сети Интернет, содержащие информацию от имени МВД о блокировке компьютера за просмотр материалов порнографического содержания и требованием уплаты «штрафа», которые квалифицировались по ст.351 (компьютерный саботаж) и 209 (мошенничество) УК. До этого аналогичные факты мошенничества были сопряжены с установкой на компьютеры вредоносного программного обеспечения, так называемых «винлокеров». Такие случаи в настоящее время носят уже единичный характер.

Анализ уголовных дел показывает, что в последнее время более широкое распространение получили преступления, совершение которых связано с использованием социальных сетей, в том числе сопряженных с несанкционированным доступом к аккаунтам пользователей такой сети.

Значительно увеличилось количество обращений в правоохранительные органы пользователей социальных сетей, с которыми злоумышленники вступили в переписку и последние под воздействием обмана, добровольно предоставили сведения о своей банковской платежной карте, либо перечислили деньги на указанные номера мобильных телефонов. Также заявителями выступают владельцы взломанных аккаунтов социальных сетей, от имени которых производилась переписка.

Существенно возросло количество хищений денежных средств с использованием полученных в ходе переписки либо звонков гражданам от имени сотрудников банков реквизитов банковских платежных карточек и иной конфиденциальной информации, позволяющей получить доступ к управлению карт-счетом.

В любом случае, традиционно сами потерпевшие предоставляли эту информацию злоумышленникам, которые входили к ним в доверие или обманывали различными способами.

Нередко жертвами киберпреступлений становятся различные предприятия и организации.

Причинами и условиями, способствующими совершению преступлений, явились наличие несложного пароля к электронному почтовому ящику и его несменяемость, излишняя доверчивость и неосмотрительность.

Имеющиеся возможности оперативного взаимодействия с правоохранительными органами иностранных государств, а также механизмы получения международной правовой помощи по уголовным делам не позволяют в полной мере обеспечить принцип неотвратимости наказания. Следует констатировать, что из-за специфики киберпреступлений, их раскрытие и расследование на современном этапе остается сложной задачей. Большая часть таких преступлений в настоящее время остается не раскрытыми.

При таких обстоятельствах на первый план выходит проведение качественной работы всеми заинтересованными субъектами по профилактике наиболее распространенных видов преступлений против информационной безопасности, повышению общей компьютерной и финансовой грамотности работников предприятий области и населения в целом, доведению гражданам информации о вероятных способах совершения в отношении них киберпреступлений, а также выявлению фактов несовершенства применяемых банковскими учреждениями Республики Беларусь финансовых инструментов, а также иных причин и условий, способствующих совершению хищений путем использования компьютерной техники.

Необходимо отметить, что в соответствии с Концепцией информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению, максимально полно и оперативно.

Такое реагирование предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба).

**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!