Материал подготовлен управлением

Следственного комитета

Республики Беларусь по Гродненской области

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.

Так, если в 2018 году следственными подразделениями Гродненской области возбуждено 666 уголовных дел в сфере высоких технологий, из которых 382 дела о хищениях, совершенных путем использования компьютерной техники, то уже в 2019 году их количество выросло практически вдвое до 1 311 (802). По итогам 4 месяцев текущего года возбуждено 334 (205) уголовных дела, что свидетельствует о продолжаемой динамике роста такого рода преступлений.

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.

Например, следственным управлением УСК в марте текущего года окончено предварительное следствие по уголовному делу по обвинению Л. в совершении преступлений, предусмотренных ч.ч.1, 4 ст.209, ч. 4 ст. 212 УК.

Расследованием установлено, что Л., действуя с единым умыслом на систематическое безвозмездное завладение денежными средствами ЗАО «Альфа-Банк» в особо крупном размере в рамках банковского продукта «Кредит-онлайн», введя в заблуждение более 90 жителей г.Гродно и Гродненского района, под предлогом оказания ему помощи в обналичивании денежных средств с использованием карт-счетов и абонентских номеров сотовой связи последних, а также мобильного приложения «InSync.by», завладел денежными средствами ЗАО «Альфа-банк» на общую сумму 419 850 рублей.

Кроме того, следствием достоверно установлено, что по всем соответствующим эпизодам обвинения Л. заявки на получение кредитов-онлайн в ЗАО «Альфа-Банк» были оформлены и поданы исключительно обвиняемым от имени держателей банковских платежных карт, без их ведома и согласия. После зачисления кредитных денежных средств на карт-счета клиентов банка, на мобильный номер потерпевших поступало sms-сообщение уведомительного характера о зачислении определённой суммы денежных средств, при этом сведений о том, что зачисление денег связано именно с оформленным кредитом-онлайн в указанном сообщении не содержалось, что позволяло держателям БПК быть в полной мере уверенными в том, что именно Л. осуществил перевод данных денежных средств.

Еще одним способом завладения денежными средствами держателей банковских карт является информирование последних посредством сети Интернет о выигрыше крупной суммы денежных средств. В ходе переписки злоумышленники, под предлогом перечисления выигрыша на банковскую карту, предлагают пройти процедуру регистрации на сайте, где держатель банковской карты указывает фамилию, имя и отчество, а также мобильный телефон. Затем запрашиваются реквизиты банковской карты, на которую якобы будет перечисляться выигрыш. После ввода реквизитов банковской карты на мобильный телефон, указанный в анкете, приходит смс-сообщение с кодом подтверждения, при вводе которого с банковской карты автоматически списывается не фиксированная сумма денежных средств. После их списания на сайте появляется сообщение о том, что в системе неполадки и держателю банковской карты предлагается пройти повторно процедуру регистрации и ввода реквизитов банковской карты. В ходе каждой такой процедуры регистрации и ввода реквизитов банковской карты с банковской карты заявителя списываются денежные средства.

Например, Щучинским РОСК 05.02.2020 по ч.2 ст.212 УК возбуждено уголовное дело по факту умышленного завладения неустановленным лицом с целью хищения денежных средств реквизитами банковской карты, эмитированной ОАО «АСБ Беларусбанк» на имя С., после чего, путем совершения 12 несанкционированных транзакций, похитило со счета указанной выше банковской карты денежные средства на общую сумму 7 851 российский рубль, что на день совершения преступления составило 326 белорусских рублей.

Согласно сведениям, представленным ОАО «АСБ Беларусбанк», установлено, что принадлежащие С. денежные средства перечислены на неустановленный счет АО «Тинькофф Банк» (Российская Федерация).

Нередко жертвами киберпреступлений становятся различные предприятия и организации.

Ярким примером отсутствия предусмотрительности и должной бдительности со стороны ответственных должностных лиц является уголовное дело, возбужденное Волковысским РОСК по факту несанкционированного доступа к компьютерной информации ГСУП «Подороск».

Входе предварительного следствия установлено, что неустановленное лицо, имея доступ к компьютерной информационной системе, 19.07.2019, нарушив систему защиты, осуществило несанкционированный доступ к компьютерной информации, а именно – к финансовым счетам ГСУП «Подороск», администрация которого расположена в аг. Подороск Волковысского района, что повлекло выход из строя компьютерного оборудования.

В ходе предварительного следствия проведена компьютерно-техническая экспертиза, по результатам которой установлено, что на жёстком диске системного блока персонального компьютера имеются файлы, определяемые антивирусными программными средствами как вредоносные. Помимо того, на представленном на исследование жёстком диске обнаружены сведения о посещении сайтов сети «Интернет» при помощи программ-браузеров. В

частности, установлено, что за весь период эксплуатации исследуемого системного блока персонального компьютера при помощи программ-браузеров неоднократно его пользователями осуществлялось посещение различного рода интернет-ресурсов (сайтов), информационное содержание которых не связано с деятельностью предприятия ГСУП «Подороск». Так, пользователем данного персонального компьютера утром 19.07.2019 (в день заражения компьютера вредоносным программным обеспечением) осуществлялось посещение сайта «ok.ru» - социальная сеть, что свидетельствует о его использовании во вне рабочих целях.

При таких обстоятельствах, учитывая, что использование служебного компьютера, при помощи которого осуществляется ведение учёта и организация экономической деятельности предприятия, во вне служебных целях, повышает риск его заражения вредоносным программным обеспечением, следствие пришло к выводу, что одним из условий совершения вышеуказанного преступления явилось несоблюдение работниками предприятия ГСУП «Подороск» правил пользования служебным компьютерным оборудованием.

Показательным является пример возбужденного в феврале текущего года по ч.2 ст.349 и ч.4 ст.209 УК уголовного дела по фактам несанкционированного доступа к электронному почтовому ящику ОАО «Строитель» (г.Ошмяны) и хищения денежных средств указанного общества на сумму более 40 000 евро.

Предварительным следствием установлено, что неустановленное лицо, с использованием сети Интернет, осуществило в январе 2020 года несанкционированный доступ к электронному почтовому ящику ОАО «Строитель» и ознакомилось с содержащейся в нем перепиской, в том числе с партнером-поставщиком оборудования из Швеции «BCC AB». Неустановленное лицо с целью хищения денежных средств от имени компании «BCC AB» на указанный электронный ящик направило письмо об изменении банковских реквизитов,с предоставлением реквизитов подложного и подконтрольного неустановленному лицу банковского счета в Швеции. 13.02.2020ОАО «Строитель» на указанный счет перечислило сумму в размере более 40 000 евро, которыми данное лицо завладело.

Причинами и условиями, способствующими совершению преступлений, явились наличие несложного пароля к электронному почтовому ящику и его несменяемость, излишняя доверчивость и неосмотрительность бухгалтера предприятия, не убедившегося в личности лица, выдаваемого себя за представителя шведского партнера, и не проверившего информацию об изменении реквизитов банковского счета.

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).

Информируя об изложенном и в целях принятия повышения эффективности деятельности всех субъектов профилактики, прошу нацелить уполномоченные государственные органы на проведение ими на системной основе профилактических мероприятий по противодействию киберпреступности, основанных на популяризации среди населения, прежде всего молодежи, нетерпимости к асоциальному поведению в информационном пространстве, а также на разъяснительной работе в средствах массовой информации и сети Интернет.

Необходимо усилить контроль за соблюдением на предприятиях области установленного порядка расчетов за приобретаемые товары, услуги и т.п., что в полной мере относиться и к объектам торговли, операторам сотовой связи, интернет-провайдерам.

Помимо изложенного прошу поддержать нашу инициативу о необходимости внесении изменений в банковское законодательство и уже на сегодняшний день ориентировать руководителей банковских учреждений, расположенных на территории области, на внедрение практики СМС-информирования клиентов о наиболее распространённых способах компрометации реквизитов банковских пластиковых карт, их причинах, а также на вручение держателям вновь эмитированных банковских пластиковых карт соответствующих памяток.

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 защитыденежных 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!