УВАЖАЕМЫЕ РОДИТЕЛИ И УЧАЩИЕСЯ!

Управлением Следственного комитета Республики Беларусь по Гродненской области проанализированы причины и условия, способствовавшие совершению 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.

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 Республики Беларусь).

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 Республики Беларусь. 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.

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.

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).

В период январь – май 2020 года на территории Гродненской области совершено 7 преступлений несовершеннолетними. Все противоправные деяния связаны с использованием банковских карт потерпевших, получения незаконного доступа к их данными в мобильном либо интернет-банкинге.

Статья 209. Мошенничество

Мошенничество – умышленное противоправное безвозмездное завладение чужим имуществом либо правом на имущество с корыстной целью путем обмана либо злоупотреблением доверием. Отличительной особенностью мошенничества является то, что мошенник завладевает имуществом потерпевшего, используя заблуждение лица, которое его передает либо не препятствует изъятию.

1. Завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием (мошенничество) -
наказываются общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.
2. Мошенничество, совершенное повторно либо группой лиц, -
наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до четырех лет, или лишением свободы на тот же срок.
3. Мошенничество, совершенное в крупном размере, -
наказывается лишением свободы на срок от двух до семи лет со штрафом или без штрафа.
4. Мошенничество, совершенное организованной группой либо в особо крупном размере, -
наказывается лишением свободы на срок от трех до десяти лет со штрафом.

Статья 212. Хищение путем использования компьютерной техники

1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации –
наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.
2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации, –
наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.
3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, –
наказываются лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.
4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, –
наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

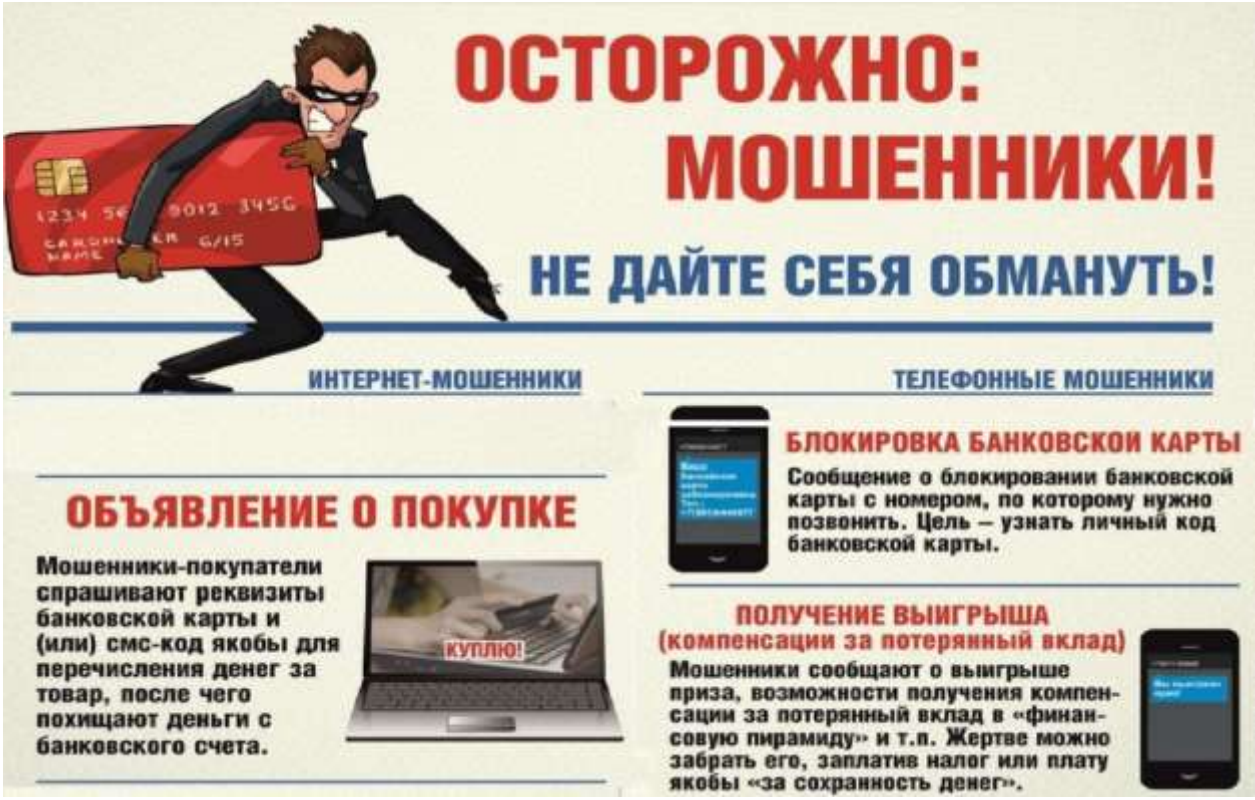
Статья 349. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, -
наказывается штрафом или арестом.
2. Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, -
наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, -
наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 351. Компьютерный саботаж

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) -
наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.
2. Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, -
наказывается лишением свободы на срок от трех до десяти лет.



НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!!!