Аналитический обзор об актуальных способах совершения киберпреступлений

Стремительное развитие цифровых технологий, переход к безналичным расчетам, размещение в глобальной компьютерной сети Интернет персональных данных при достаточно низкой цифровой грамотности граждан, сопряженной с беспечным отношением к защите собственной информации, стали следствием увеличения количества регистрируемых киберпреступлений.

Злоумышленники активно используют в своей деятельности новейшие достижения науки и техники, применяют всевозможные компьютерные устройства и новые информационные технологии для совершения и сокрытия преступлений.

Структурный анализ совершенных в текущем году мошенничеств свидетельствует о явном преобладании таких способов завладения деньгами потерпевших, как:

1. Продажа несуществующего товара на различных Интернет-ресурсах. Часто жертвами мошенников становятся пользователи сети Интернет, желающие приобрести различные товары в социальной сети **Instagram.** Продавцы, как правило, просят произвести предоплату за товар, однако такие действия заканчиваются одним – граждане перечисляют предоплату, а в дальнейшем связь с продавцом теряется, не получив долгожданный товар.

Справочно: Для примера можно рассмотреть следующие мошеннические учетные записи: ***dsm_shop, kurtkaonline, belbuket_by, buyers__indi, bolshaya_elka и др****.*

2. Обман граждан под предлогом вложения средств в криптовалюту либо сделок с ней на несуществующих биржах и иного заработка в сети Интернет.

Справочно: Несуществующие инвестиционные проекты и мошеннические биржи – это обманные схемы, в которых инвесторам предлагается вложить средства в вымышленные или несуществующие бизнес-проекты, или финансовые инструменты с обещаниями высокой прибыли, которая на самом деле не может быть достигнута. К примеру, таких проектов можно привести «web.jintao-company.com», с помощью которого мошенники ввели в заблуждение жителя Молодечненского района и завладели 11 956 белорусских рублей.

3. Звонки мошенников в мессенджерах (Viber, Telegram, WhatsApp) под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, вынуждающих потерпевших под различными предлогами получать кредиты

и переводить денежные средства либо сбережения на подконтрольные злоумышленниками счета.

Основными способами совершения хищений имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса), являются:

1. Также звонки мошенников в мессенджерах под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, в ходе которых злоумышленники получают доступ к банковским реквизитам граждан.

Такой способ называется «Вишинг» – это один из методов мошенничества с использованием социальной инженерии (социальная инженерия – это совокупность способов психологического воздействия на поведение человека с целью получения выгоды), который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию, или побуждают, убеждают вероятную жертву к совершению определенных действий со своей банковской платежной картой

Он заключается в том, что злоумышленники, используя телефонную связь и, выдавая себя за сотрудников банка или правоохранительных органов, под различными предлогами вводят в заблуждение потерпевших, выясняя сведения о наличии банковских платежных карточках, их реквизитах, паспортных данных с целью последующего хищения денежных средств.

В большинстве случаев при совершении звонков мошенники используют интернет-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи.

При этом всем известные мессенджеры Viber, Telegram и WhatsApp имеют возможность использования виртуальных номеров.

К примеру, злоумышленники звонят жертве от имени банковского работника и сообщают, что необходимо осуществить какие-либо действия с банковской платежной карточкой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо проводит подозрительную оплату.

Для большей достоверности в качестве имени пользователя они указывают официальный номер банка либо его название, а для «аватарки» используют логотип или эмблему банковского учреждения.

При этом зачастую они уже владеют минимальной информацией о лицах, которым звонят (имя, отчество, дата рождения, последние цифры банковской карты и др.), что способствует повышению доверия к звонящему и производит на него определенное впечатление.

В дальнейшем преступник просит сообщить информацию о банковской карте – номер, срок действия, трехзначный код на ее обороте, содержание СМС-сообщения, которое в ходе разговора поступает на мобильный телефон, либо устанавливает мобильное приложение, позволяющее злоумышленнику получить удаленный доступ к мобильному телефону, в котором сегодня фактически у каждого имеется интернет-банкинг и, соответственно, доступ к банковскому счету.

2. Использование фишинговых Интернет-ресурсов.

Фишинг – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт с использованием поддельных интернет-ресурсов, контролируемых злоумышленниками, внешне схожих с настоящими (например, поддельные страницы услуги «Интернет-банкинг» различных банков).

К примеру, в прошлом году житель нашей области, при попытке совершить платёж за коммунальные услуги посредством системы Интернет-банкинга, воспользовался поисковой строкой сайта Google и перешёл, как оказалось, по ложной ссылке для оплаты. Злоумышленникам стали известны реквизиты банковской карты и в результате с его карт-счета было похищено почти 35 тысяч рублей.

Также в социальных сетях появилась реклама, обещающая «призы от Белагропромбанка». Переходя по ссылке, жертва попадает на поддельную банковскую страницу, на которой мошенники выманивают номера телефонов и иные личные данные, что дает им полный доступ к счетам обманутых и даже возможность оформления онлайн-кредитов.

Распространены кибермошенничества от имени «Белпочты».

Схема довольно проста – злоумышленники присылают потенциальной жертве сообщение через интернет-мессенджер. В нем сообщают о необходимости уточнения адреса доставки почтового отправления и предлагают перейти по ссылке в Интернете. Невнимательный человек, не проверив адрес, по которому ему предлагают перейти, попадает на фейковый сайт, стилизованный под официальный сайт «Белпочты». Там клиента просят ввести свой адрес, якобы для доставки некоего почтового отправления, и оплатить тариф за услугу «Белпочты» прямо на этой странице, введя реквизиты банковской карты.

Появились случаи мошенничеств, связанных с созданием фейкового аккаунта в мессенджерах от имени руководителя учреждения, где работает потенциальная жертва.

Злоумышленники осуществляют рассылку сообщений с указанием того, что в скором времени гражданину позвонит или напишет сотрудник вышестоящей инстанции (Министерства образования, МВД, КГБ, КГК, СК,

ОВД). Как правило, пугаясь, граждане говорят любую информацию, которую требует сотрудник. Далее просят установить удаленное программное обеспечение, позволяющее получить ему доступ к устройству, либо вести видеозапись с демонстрацией экрана мобильного телефона.

Преступления против компьютерной безопасности (глава 31 УК) в большинстве случаев возбуждаются по фактам по факту блокировки **учетной записи «iCloud» мобильных устройств «iphone»**.

Основные способы совершения вымогательств (ст. 208 Уголовного кодекса), можно разделить на две основные категории:

1) связаны с **угрозой распространения личной информации потерпевших, которые последние желали сохранить в тайне** как правило фотографий и видеозаписей интимного характера, которые, в большинстве случаев, потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером противоположного пола для знакомства.

2) связаны с **блокированием компьютерной информации** физических лиц. При этом в подавляющем большинстве случаев отмечается блокирование учетных записей Apple ID посредством ввода авторизационных данных, предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшим полноценно использовать свои мобильные устройства.

Основными факторами, способствующими совершению киберпреступлений, являются халатность, излишняя доверчивость граждан, мнимая возможность быстрого обогащения, получение крупных сумм денежных средств, а также недостаточное информирование населения о способах и методах применяемыми преступниками при совершении указанных преступлений.

Знание основных схем и способов обмана позволяет гражданам быть более внимательным и осторожным, что, в свою очередь, помогает предотвратить случаи совершения киберпреступлений.