Информационные материалы для институтов об особенностях преступлений, совершенных с использованием ИТ-технологий и мерах по их профилактики.

В условиях цифровизации общественных отношений, проникновение ее во все сферы жизнедеятельности и использования сети «Интернет» без соблюдения элементарных правил безопасности трансформировалась структура преступности.

Уличные преступления ушли в прошлое, а правоохранительные органы столкнулись с новыми угрозами и вызовами криминального мира. Началась активная фаза развития мошенничества, вымогательства, совершаемых с использованием информационно-телекоммуникационных технологий. Мошенниками используются сведения, которые оставлены гражданами добровольно в сети «Интернет», это могут быть фото и видео изображения, переданные в ходе переписки в различных мессенджерах, или конфиденциальные данные, оставленные при посещении различных сайтов, данные банковских карт, введенные якобы для приобретения товара на фишинговых сайтах. Нельзя забывать и про использование злоумышленниками методов социальной инженерии, когда в ходе телефонных разговоров потерпевшие самостоятельно сообщают сведения, необходимые для управления их банковскими счетами или, доверясь мошенникам, вносят денежные средства на «безопасный» счет, устанавливают программы удаленного доступа к дистанционному банковскому обслуживанию.

За последние 5 лет количество таких преступлений увеличилось в 3 раза. В настоящее время это четверть всех криминальных деяний в России (26,5%), в регионах с высокой экономической активностью и кредитной платежностью населения, доля таких преступлений достигает 30 – 40% *(Москва, республики Северная Осетия – Алания, Крым, Московская область)*. Растет сумма причиняемого преступлениями ущерба. Согласно данным Банка России сумма похищенных денежных средств со счетов граждан только по операциям, совершенным без согласия клиента, в 2022 году выросла на 4, 29 % и составила 14,2 млрд рублей.

В среднем ущерб от таких преступлений в 2022 году по сравнению с 2021 годом вырос на 22 млрд рублей, продолжает расти в 2023 году.

Жертвами таких преступлений становятся все слои населения, от лиц преклонного возраста до несовершеннолетних граждан.

Кроме того, снижается и возраст мошенника, если в 2021 году такие преступления совершались в основном совершеннолетними лицами, то в настоящее время совершаются лицами, не достигшими возраста 18 лет.

В преступную схему все чаще вовлекаются лица, проходящие обучение в институтах, которые открывают на свое имя банковские счета, получают банковские карты, куда поступают похищенные денежные средства

потерпевших. Указанные лица, выполняя требования мошенников, обналичивают денежные средства, становясь соучастниками преступлений.

Кроме того, лица, оформившие на свое имя банковские карты, передают их мошенникам, которые используют их в преступных целях, оказывая таким образом пособничество в совершении преступлений.

Среди преступлений, совершаемых с использованием информационно-телекоммуникационных технологий самыми распространенными являются дистанционные хищения, которые происходят в условиях, исключающих личный контакт жертвы и мошенника. В результате реализации преступного умысла, потерпевший, находясь под воздействием обмана, переводит свои денежные средства на банковские счета мошенников.

Таким образом, цель у злоумышленников одна – завладеть денежными средствами, а сценарии обмана жертвы постоянно меняются.

Рассмотрим основные способы совершения преступлений с использованием информационно-телекоммуникационных технологий:

1. Звонки от якобы представителей правоохранительных органов, кредитно-финансовых организаций с сообщением о незаконных действиях с банковскими счетами (совершен перевод денежных средств с принадлежащего жертве счета, пытаются оформить кредит или уже оформили и пытаются обналичить денежные средства, получили доступ к управлению счетом потерпевшего и совершают по нему операцию, срочно необходимо снять все денежные средства и внести их на безопасный счет), также злоумышленники могут сообщать о незаконных операциях с недвижимостью, необходимости оперативного заключения договора купли-продажи.

При совершении таких звонков, потерпевшего называют полными анкетными данными, сообщают сведения о том в каком банке открыт счет. Однако, стоит помнить, что мы все пользуемся различными услугами, получение которых требует от нас регистрации в сети «Интернет», где мы оставляем свои анкетные данные, указываем места жительства, данные банковской карты, что также может быть использовано мошенниками.

В настоящее время граждане стали бдительнее, не поддаются на уловки мошенников и своевременно прерывают такие разговоры.

Указанные обстоятельства заставили злоумышленников при телефонном разговоре сначала говорить на отвлечённые темы, например, о состоянии геополитической обстановки в стране, правах и обязанностях правоохранительных органов и кредитных организаций, тем самым подыскивая подходы к предполагаемой жертве преступления. А уже после, войдя в доверие, получать конфиденциальные сведения для входа в личные кабинеты приложений дистанционного банковского обслуживания или заставлять жертву самостоятельно переводить денежные средства на принадлежащие мошенникам счета.

В настоящее время в условиях неспокойной геополитической обстановки для нарушения общественного порядка злоумышленники совершают звонки потерпевшим, сообщают о том, что специальные службы якобы проводят расследование и выявляют лиц из числа сотрудников банков, органов государственной власти, которыми совершаются преступления. Для пресечения преступной деятельности указанных лиц необходимо содействие. Под четкие указания лиц, совершающих преступления, жертва, считая, что принимает участие в поимке опасных преступников, изготавливает зажигательные смеси, использует их для причинения имущественного ущерба банкам, государству, что создает опасность гибели человека.

2. Звонки от якобы родственников потерпевшего с сообщением, что он попал в беду и ему срочно необходима финансовая поддержка.

Данная преступная схема появилась одной из первых, продолжает быть актуальной. Во время телефонного разговора жертву убеждают, что с ее близким человеком случилось непоправимое и срочно требуются денежные средства для решения проблемы.

Потерпевшему не дают положить телефонную трубку, постоянно держат на контакте, чтобы не дать позвонить близкому человеку и убедиться в его безопасности. Находясь под воздействием обмана, жертвы передают денежные средства злоумышленникам различными способами (перевод на банковские счета, карты, номера телефонов, передача наличных курьеру).

3. Широкое распространение получило незаконное использование персональных данных, личных фото, а также действий потерпевших при посещении различных сайтов в сети «Интернет».

Совершенствование высоких технологий и их применение в повседневной жизни очень удобно. Позволяет быстро получать информацию, приобретать товары. Сами по себе такие возможности и услуги при соблюдении мер предосторожности безопасны.

Однако, граждане, используя сеть «Интернет», не всегда проявляют бдительность. Зачастую не думают, что вводимые ими данные, в том числе персональные, сохраняются на том или и ином сайте, посещают запрещенные ресурсы, переходят по различным ссылкам, предназначенным для собирания информации о лицах. Порой неосмотрительно размещают в сети «Интернет» фото и видео изображения о частной жизни.

Перечисленные обстоятельства позволяют мошенникам использовать собранные данные в противоправных целях. Например, вымогать денежные средства под угрозами распространения сведений о личной жизни. Такие преступления стремительно развиваются.

4. Использование фишинговых сайтов, на которых размещаются сведения об оказании услуг по реализации авиа, ж/д –билетов, бронирование гостиниц, туристические путевки.

В данном случае гражданам, как правило, предлагаются более выгодные цены, условия проживания, туристические поездки по низким ценам. Сайты практически не отличимы от официальных компаний, предлагающих данные услуги. Разница может быть в одной букве или цифре. Однако, необходимо

помнить, что невозможно получить качественные услуги ниже рыночной стоимости, перед заключением каких-либо договоров и переводом денежных средств необходимо убедиться в реальности предоставляемых услуг, в том числе ознакомиться с отзывами о данном сайте.

Для хищения денежных средств мошенники также используют предложения по инвестированию денежных средств при проведении различных финансовых операций. Участникам данных проектов предлагается внесение денежных средств, приобретение акций для получения дохода. Предлагаются очень выгодные условия, высокий процент доходности от пользования денежными средствами потерпевшего. После получения денежных средств жертве могут предоставляться сведения об увеличении дохода, различные графики и схемы проведенных с их использованием финансовых операций, позволяющих сделать вывод о высокой доходности. Однако, данные сведения являются фикцией.

Как правило, о таких сайтах имеется множество отрицательных отзывов в сети «Интернет», которые не изучаются потерпевшими перед внесением денежных средств.

5. Мошенничество в социальных сетях через взлом аккаунта.

Жертва получает сообщение от своего знакомого с просьбой о предоставлении в долг денежных средств, не подозревает, что от его имени действует мошенник. При получении таких сообщений необходимо удостовериться, что с близкими людьми действительно произошли какие-то неприятности, например, позвонив по телефону, не стоит переводить денежные средства неизвестным лицам.

6. Хищение денежных средств под предлогом реализации товара, услуг, объявления о которых размещены на торговых площадках (Авито, Циан, Юля и другие).

Мошенники создают аккаунты на указанных торговых площадках, размещают на них сведения о реализуемых товарах, оказываемых услугах, фактически не намереваясь выполнять обязательства, желая получить денежные средства.

Перед приобретением товаров необходимо внимательно изучить сведения о продавце, дате его регистрации на торговой площадке, имеющиеся отзывы. Мошенники регистрируются незадолго до размещения своих объявлений. Кроме того, не нужно идти выполнять требования продавцов о необходимости полной оплаты товара до его получения, а в случаях когда потерпевшим размещен товар, то требования о необходимости перечислить какую-то сумму, которая в последствии вернется. Данные действия предпринимаются для получения сведений о реквизитах счетов жертвы.

Важно также понимать, что дистанционные мошенники используют разветвленные преступные цепочки. После получения доступа к банковским счетам потерпевших или когда жертва, находясь под воздействием обмана, готова передать мошеннику свои денежные средства, злоумышленникам необходимо в течение нескольких минут принять решение о том, на какие банковские счета перевести похищенные денежные средства, а также как их

обналичить. Для этого к участию в преступление привлекаются так называемые «дропы».

«Дропы», фактически, аналогичные промежуточные звенья для вывода похищенных средств. Это физические лица, которые оформляют на себя банковские карты, открывают счета, электронные кошельки. Но делают они это не для личного пользования. Реквизиты передают лицам, совершающим преступления (кураторам).

Полученные от «дропа» реквизиты банковских карт, счетов, электронных кошельков, мошенники называют потерпевшим, которые самостоятельно, действуя под влиянием обмана, переводят на них свои денежные средства.

В дальнейшем «дропы», действуя по указанию мошенников, «обналичивают» денежные средства с использованием различных банкоматов, осуществляют их дальнейший транзит.

Использование «дропов» необходимо мошеннику, чтобы самому «не засветиться» в совершении преступления, избежать наказания, скрыть сам факт киберпреступления и легализовать похищенные денежные средства, используя для их вывода цепочку проведенных операций, создавая сложность в установлении лиц, причастных к совершению преступлений.

Наличие такого инструмента для совершения преступлений приобрело огромные масштабы, из оборота изымается невероятное количество банковских карт, использовавшихся для вывода похищенных денежных средств. Бесконтрольное использование данного инструмента в преступной деятельности привело к функционированию в Российской Федерации «серого» рынка электронных средств платежа, позволяющих выводить огромные суммы денежных средств, похищенных у наших граждан.

Мошенники подробно инструктируют своих «подставных лиц», в том числе о том, какие показания должны быть даны в случае задержания сотрудниками полиции в целях избежание уголовной ответственности. На сегодняшний день мошенниками организованы банки данных «дропов», что позволяет осуществлять их бронирование при совершении преступления, использовать в определенную дату и время конкретного лица.

В настоящее время указанные лица привлекаются к уголовной ответственности, а также к ним имеется возможность предъявления потерпевшей стороной требования о возврате полученных на их счета денежных средств как неосновательного обогащения, поскольку какие-либо гражданско-правовые отношения между ними отсутствуют. При получении предложений об оформлении за денежное вознаграждение банковских карт или открытии счетов на свое имя и передача сведений по управлению счетами или карт другим лицам, необходимо отказаться от таких действий, не становиться соучастником преступления.

В заключении хотелось бы отметить, что обозначенные преступления возможны ввиду несоблюдения правил безопасного поведения, жертва сама предоставляет возможность совершения в отношении нее противоправных действий. В ходе разговора с мошенниками потерпевшие сами сообщают о

себе свои сведения, выполняют нелепые требования злоумышленников, такие как снятие со своего счета денежных средств и их внесение на «безопасные счета» мошенников. Сообщают свои конфиденциальные данные, позволяющие мошенникам получить удаленный доступ к управлению банковскими счетами.

Для того, чтобы не стать жертвой мошенников необходимо соблюдать пять правил безопасного поведения:

1. Не разговаривайте с незнакомыми людьми, положите трубку.
2. В случаях если звонят по телефону и представляются сотрудниками МВД России или других правоохранительных органов, банков, или ваш родственник попал в ДТП и т.д. прервите разговор, перезвоните на номера которые указаны на официальных сайтах той или иной организации и посоветуйтесь с родными.
3. Используйте приложения по блокировке спам-звонков или используйте эту опцию у операторов сотовой связи.
4. Не выкладывайте и не сохраняйте в сети интернет персональные данные.
5. Ни при каких обстоятельствах нельзя передавать посторонним лицам сведения о своих счетах и банковских картах, а также не совершать никаких действий со своими картами и вкладами, о которых просят незнакомые лица по телефону.

Будьте бдительны, проверяйте информацию. Мошенникам невыгодно, чтобы вы делали это, поэтому они могут говорить о «секретной информации» или о том, что вы должны принять решение прямо сейчас. Не поддавайтесь на провокации.

Следственный департамент МВД России