Информация о преступлениях, совершаемых с использованием информационно-телекоммуникационные технологии

К сожалению, киберпреступность сегодня остается одной из самых динамично развивающихся и прибыльных отраслей преступного бизнеса. Широкое использование интернет-сервисов и упрощение алгоритма банковских транзакций привело к тому, что злоумышленники активно применяют информационно-телекоммуникационные технологии (*далее - ИТТ*) и социальную инженерию для хищения сбережений граждан.

Анализ структуры преступности в России и её динамики показывает, что на фоне сокращения общего числа грабежей, краж автомобилей, квартирных краж, разбойных нападений, фактов умышленного уничтожения имущества (поджогов) выросло число хищений, совершенных с использованием ИТТ.

Рост числа зарегистрированных преступлений также обусловлен особенностями криминальной деятельности в данной сфере: активно развивающимся применением ИТТ, переходом многих финансовых операций в сферу интернет-услуг, виктимным поведением потерпевших, постоянным возникновением новых способов совершения противоправных деяний, имеющимися возможностями для обеспечения анонимности преступников, а также необходимостью совершенствования механизмов противодействия им. Жертвами становятся как частные, так и юридические лица.

Разберем самые распространенные виды дистанционного мошенничества:

ФИШИНГ

Злоумышленники создают интернет-страницу, которая очень похожа на известный вам ресурс, например, госуслуги или сайт банка. Отличие минимально - это может быть другое доменное имя (замена интернет-адреса на «.com», «.net» вместо «.ru»), замена буквы или лишний знак. Невнимательный пользователь, доверяя «проверенному» сайту, вбивает свои личные данные, логины и пароли или даже сообщает банковскую и финансовую информацию.

ЧЁРНЫЕ БРОКЕРЫ

Мошенники предлагают современный и безопасный способ заработка - поторговать на бирже или вложить денежные средства в инвестиции. Вам выделят персонального консультанта, пообещают научить и обеспечить всей информацией. Нет денег - возьми кредит, ведь уже через пару месяцев ты станешь российским «волком с Уоллстрит». Чтобы жертва ничего не заподозрила, с ней даже могут заключить договор и завести личный кабинет на сайте с логином и паролем, провести «Вебинар».

Так, в феврале жительница Радужного таким образом потеряла 1 400 000,00 рублей.

САЙТЫ ОБЪЯВЛЕНИЙ

Схемы обмана через ресурсы купли-продажи или доставки различные. Мошенники цепляют жертву на крючок заманчивым предложением и низкой ценой. Дальше клиента могут вывести на всё тот же фишинговый сайт, где он проведет оплату и потеряет деньги. Но схема может быть и гораздо проще - мошенники под благовидным предлогом попросят сделать предоплату и исчезнут.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Одной из самых распространенных форм хищений все также остается телефонное мошенничество, при этом аферисты действуют по давно отработанной схеме, используя лишь разные поводы для звонка. Не редко они выдают себя за сотрудников банка: сообщают абоненту о сбое в базе данных, блокировке карты, сомнительном переводе с его счетов, начислении бонусов или предлагают подключение к специальной программе привилегий, убеждают передать им конфиденциальную информацию или самостоятельно перевести финансы. Злоумышленники выдают себя за сотрудников правоохранительных органов, Пенсионного Фонда, используя современные технологии подмены данных, имитируют звонки с номеров, которые закреплены за службами.

Также злоумышленники представляются представителями мобильного оператора и сообщают, что абоненту необходимо продлить срок договора на обслуживание телефонного номера или переоформления действия SIM-карты.

Так, псевдо-оператор поясняет, что сейчас на сотовый телефон абоненту будут приходить коды, которые он должен сообщить.

Такая ситуация случилась недавно в регионе. Пенсионерке города Сургута позвонил неизвестный и представился менеджером одной из сотовых компаний, под предлогом планового переоформления пользовательского договора на сотовую связь, убедил югорчанку сообщить коды из смс-сообщений, после чего зайдя в приложение банка ПАО «ВТБ» потерпевшая обнаружила, что на ее имя оформили кредитование на сумму 800 000,00 рублей. Аналогичные случаи зафиксированы в Нефтеюганском и Октябрьском районе.

Следует помнить, что никто, включая представителей кредитных организаций, правоохранительных органов, не в праве требовать от гражданина предоставлять по телефону следующую информацию:

- персональные сведения (серию и номер паспорта, адрес регистрации, имя и фамилию владельца карты);

- реквизиты и срок действия карты, паролей или коды из смс-сообщений для подтверждения финансовых операций или их отмены;

- логин, ПИН-код, CVV- код банковских карт.

Сотрудники банка никогда не предлагают:

- установить программу удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);

- перейти по ссылке из смс-сообщения;

- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;

- под их руководством перевести для сохранности денежные средства на «защищенный счет»; зайти в онлайн-кабинет по ссылке из смс-сообщения или электронного письма.

Аферист может представиться родственником или знакомым и сообщить, что задержан сотрудниками полиции за то или иное преступление, например, хранение наркотиков, нанесение тяжких телесных повреждений, совершение дорожно-транспортного происшествия и даже убийства. Затем диалог продолжает якобы сотрудник полиции и предлагает за денежное вознаграждение прекратить уголовное преследование. Мошенники запугивают собеседника, не дают ему опомниться, ведут с ним непрерывный разговор вплоть до получения денег. В таком случае следует сбросить вызов и самому связаться с родственником или знакомым.

НОВЫЕ СХЕМЫ

Правоохранительные органы всё чаще фиксируют новые случаи дистанционных хищений, когда преступники используют «актуальную новостную повестку».

Теперь звонки от «представителей банков» поступают в связи с тем, что Россию отключают от международных платёжных систем, якобы вводится запрет на полное снятие наличных с банковских счетов или даже блокировка банковских операций. Также клиенту могут предложить взять кредит по низкой ставке, пока она не поднялась. Ещё одна, ставшая в последнее время популярной у мошенников схема: предложить клиенту банка повышенный кешбэк. Цель все та же: получить доступ к конфиденциальной информации, обмануть, убедить перевести деньги на подставной счёт.

Мошенники быстро ориентируются в происходящих социальных процессах и находят новые формы спекуляций.

Также возросло количество мошенничеств, совершенных с помощью известного сервиса поиска попутчиков «Бла Бла Кар». Жители округа переходят по ссылкам, которые присылают «водители» и переводят деньги в надежде забронировать поездку. Однако, денежные средства уходят на счета аферистов.

Так, 33-летняя жительница Сургута хотела добраться с помощью данного сервиса до окружной столицы. Для бронирования поездки девушка перешла по ссылке, отправленной водителем, ввела реквизиты своей банковской карты и код из СМС-сообщения. В результате мошенник пополнил свой кошелек на 4480. Но этого аферисту показалось мало, и тогда он отправил заявительнице еще одну ссылку, но уже якобы на возврат денежных средств. Девушка вновь поверила мошеннику и по той же схеме лишилась еще 6000 рублей.

А жительница Радужного собиралась забронировать поездку из г. Сочи в г. Саки. Несостоявшаяся поездка обошлась заявительнице в 12000 рублей. Аферисты убедили женщину перейти по ссылке для оплаты комиссии за проезд.

Отдел МВД России по городу Радужному совместно с администрацией города Радужный обращается к гражданам с просьбой проявлять бдительность, не поддаваться психологическому воздействию со стороны преступников, не сообщать неизвестным лицам

персональные данные, никому не передавать конфиденциальную информацию о своих счетах и банковских картах.

Просим провести беседу со старшими родственниками. Не поддавайтесь каким-либо выгодным предложениям участия в лотереях, в инвестиционных программах. Если вам звонят и начинают разговор о финансах, ваших банковских счетах - это однозначно мошенники. Будьте бдительны, берегите себя и своих близких!