ИНФОРМАЦИЯ

о популярных сценариях мошенничества с использованием цифровых технологий и рекомендуемых инструментах защиты

Кибератаки на компании, факты **дистанционных хищений денежных средств** у граждан фиксируются все чаще, при этом криминальные схемы, в том числе по выводу незаконно полученных доходов, постоянно меняются. За последние пять лет количество противоправных деяний в указанной сфере в целом по России возросло в два раза и сейчас составляет треть от всех зарегистрированных преступлений. Больше половины из них относится к категории тяжких и особо тяжких. Основной массив приходится на кражи и мошенничества.

Происходят **утечки персональных данных**, которые используются для формирования так называемых «цифровых портретов» в противоправных целях. Отмечается рост киберхищений, связанных с применением метода социальной инженерии, когда граждане, как правило, пенсионного возраста, сами сообщают сведения о себе лицам, представляющимся сотрудниками государственных органов или банковского сектора. Самые распространенные способы неправомерного завладения денежными средствами сопряжены с созданием фальшивых сайтов, а также получением доступа к конфиденциальным данным пользователей.

В основном такая вариативность реализации преступных намерений исходит из-за рубежа, включая **кол-центры, находящиеся на территории Украины**. Кроме того, киевскими спецслужбами используются схемы запугивания жертв несуществующим уголовным преследованием либо долговой финансовой зависимостью. Это заканчивается совершением последними преступлений против общественной безопасности. Фигурантами по таким делам нередко становятся высокообразованные люди, которые сами призваны формировать законопослушное поведение.

Как показало собственное исследование группы компаний «Сбер», проведённое в 2023 году, на Украине действовало более тысячи мошеннических колл-центров, в которых задействовано порядка 100 тысяч человек. Примерно 300 таких колл-центров сосредоточены в Днепре – так называемой «столице» телефонного мошенничества. По данным банка, 92% звонков преступников направлены на Россию, а оставшиеся 8% получают жители других стран, преимущественно Польши, Германии и Казахстана. Доходы идут на личное обогащение и закупку вооружения против России.

Обнаруженная «Сбером» база данных показала, что 212 колл-центров (на тот момент) управлялись тремя головными центрами по модели франшизы, а инфраструктура для их деятельности сосредоточена в Нидерландах и Германии. Преступники используют профессиональные CRM-системы для управления звонками и фиксируют в них суммы украденного.

Средний колл-центр похищает 40 тысяч долларов в месяц, а совокупный ущерб от деятельности 212 колл-центров, работающих по франшизе, в 2023 году достиг 100 миллионов долларов. Типовой колл-центр совершает 70 тысяч звонков в день и насчитывает до 100 «операторов» в одну смену.

Мониторинг мошеннических схем и способов защиты от них

Чтобы не стать жертвой телефонного или интернет мошенничества необходимо своевременно отслеживать используемые злоумышленниками мошеннические схемы, а также предлагаемые специалистами банковского сектора, правоохранительных органов и юристов инструменты защиты своих сбережений.

Вашему вниманию предлагаются наиболее распространённые в 2022-2023 годах такие сценарии.

«Брачные мошенничества»

С использованием сети Интернет (преимущественно на сайтах знакомств) преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предлогами «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.). Переписка ведется главным образом студентами лингвистических ВУЗов.

Направленные жертвами деньги преступники получают на подставных лиц. После получения средств переписка под различными предлогами прекращается.

«Приобретение товаров и услуг посредством сети Интернет»

При покупке в интернет-магазинах, граждане часто невнимательны, чем и пользуются мошенники. Обычно схема мошенничества выглядит так: создаётся сайт-одностраничник, на котором выкладываются товары одного визуального признака.

Цена на товары обычно весьма привлекательная, ниже среднерыночной. Отсутствуют отзывы, минимален интерфейс, указаны скудные контактные данные. Чаще всего такие интернет-магазины работают по 100% предоплате. Переписка о приобретении товаров ведется с использованием электронных почтовых ящиков.

По договоренности с продавцом деньги перечисляются, как правило, за границу через «Western Union» на имена различных людей, после чего псевдо-продавец исчезает.

«Крик о помощи»

Один из самых циничных и распространённых способов хищения денежных средств.

В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Здесь важно прежде чем переводить свои деньги, проверить – имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

«Фишинг»

Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на «сайт-двойник» такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространенным является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

«Нигерийские письма»

Также один из самых распространённых видов мошенничества, когда жертва получает на свою почту письмо о том, что является счастливым обладателем многомиллионного наследства. Затем мошенники просят у получателя письма помощи в многомиллионных денежных операциях (получение наследства, перевод денег из одной страны в другую), обещая процент от сделки.

Если получатель согласится участвовать, то у него постепенно выманиваются деньги якобы на оплату сборов, взяток чиновникам и т.п.

«Брокерские конторы»

С начала текущего года в НЦБ Интерпола МВД России наблюдается значительный рост количества обращений граждан, пострадавших от действий брокерских контор.

В частности имеется информация о таких недобросовестных брокерских компаниях, как: «MXTrade» и «MMCIS».

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам – трейдерам.

Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

Важно! Помните, что инвестирование, предлагаемое на условиях брокерской компании, всегда является высоко рискованным даже при наличии безупречной репутации брокерской компании.

Способы защиты от мошенничества

Доля возврата средств банками клиентам, когда последние самостоятельно переводят деньги аферистам или открывают им доступ к своему счету.

Сейчас банки по закону «О национальной платежной системе» не обязаны возвращать деньги в этих случаях. Банк России вместе с участниками рынка и экспертами предлагает внести изменения в законодательство, чтобы люди могли рассчитывать на возврат средств даже тогда, когда их обманули с помощью социальной инженерии.

Банк России ведет базу о случаях и попытках перевода денежных средств без согласия клиентов. В ней аккумулируются данные из банков, в том числе содержатся сведения о дропперских счетах, которые злоумышленники используют для вывода и снятия похищенных средств.

Механизм возмещения гражданам похищенных злоумышленниками средств

Если банк-отправитель получил информацию из базы ФинЦЕРТа, но не учел ее в своих бизнес-процессах и совершил перевод на такой счет, то он будет обязан вернуть клиенту похищенную сумму, даже в случаях, когда хищение произошло с использованием методов социальной инженерии.

Кроме того, Банк России внедряет так называемый «период охлаждения», когда у гражданина будет время обдумать и оценить совершаемые действия. Банк-плательщик будет обязан на два дня приостанавливать зачисление денег на счет, информация о котором содержится в базе Банка России. Формально банк не нарушит права добросовестных граждан и законодательство, приостанавливая перевод, поскольку по закону перевод совершается в срок до трех рабочих дней

Кроме того, проверять операцию на признаки мошенничества должен и банк-получатель. Если он видит, что деньги перечисляют на счет, содержащийся в базе регулятора, то у банка должно быть право приостанавливать доступ владельца такого счета к дистанционному обслуживанию. То есть получатель подозрительного счета не сможет сразу же удаленно распорядиться деньгами, перевести их на любой другой счет, что обычно сразу делают мошенники. Чтобы разблокировать эту возможность, владельцу счета придется прийти в отделение банка с паспортом, на что вряд ли пойдут дропперы. В то же время будут соблюдены все гражданские права добросовестных банковских клиентов.

Банк России повышает требования к банковским полисам страхования от мошенников, чтобы в страховки были включены случаи возврата средств при атаках социальных инженеров. Речь о любых случаях, когда клиент добровольно переводит деньги мошенникам или раскрывает им банковские сведения, то есть при атаках телефонных мошенников, онлайн-мошенников. Все эти случаи должны включаться в страховое покрытие. При этом из покрытия планируется исключить случаи, по которым банки обязаны возмещать средства клиентам по закону «О национальной платежной системе». Это все случаи, когда мошенники похитили средства, используя какие-то технологические приемы, например, без непосредственного участия человека.

В октябре 2023 года вступил в силу закон об оперативном взаимодействии между Банком России и МВД. Сотрудники полиции получили доступ к базе ФинЦЕРТ, которая в свою очередь пополняется сведениями от МВД. Эти данные помогут банкам эффективнее вести борьбу с мошенническими списаниями средств с банковских карт, в том числе с использованием методов социальной инженерии. Раньше при рассмотрении дел о мошенничестве много времени уходило на запросы данных и переписку между правоохранительными органами и банками. Теперь обмен данными будет проходить оперативно».

«Валютные ограничения»

Последние два года мошенники запугивали своих потенциальных жертв не только несанкционированными переводами или оформлением кредитов, но и привязывались ко всем новостным поводам. Говорили об угрозе в связи с отключением от системы «Свифт», об уходе Visa и Mastercard, о дефиците валюты, об угрозе деньгам на вкладах, т.е. использовали все возможные информационные поводы.

Мошенники звонили потенциальным жертвам, представлялись работниками банков или обменных пунктов и сообщали, что евро и доллары вот-вот перестанут выдавать или изымут из обращения. Людям предлагали перевести деньги на некий «специальный счет», но для этого нужно было сказать по телефону банковские данные, с помощью которых мошенники потом переводили средства на свои счета.

Помните, что банки не запрашивают финансовую информацию клиентов по телефону, поэтому самое лучшее решение в этой ситуации – бросить трубку и найти всю информацию самостоятельно. У Банка России нет планов изымать сбережения ни в рублях, ни в валюте.

Обо всех валютных ограничениях можно узнать на сайте финансового маркетплейса Банки.ру, а если возникнут сомнения, то прежде чем совершать операцию, можно уточнить информацию на «горячей линии».

«Мобилизация»

Одновременно с нагнетанием истерии о возможной мобилизации распространялись две схемы мошенничества – поддельные документы и фишинг.

В первом случае в интернете даже появились сайты, которые маскируются под видом сервисов по изготовлению документов. Кроме того, тем, кого могли мобилизовать, писали в мессенджерах с похожими предложениями.

За медицинскую отсрочку или справку с «бронью» мошенники предлагали заплатить от 20 до 65 тыс. рублей. После оплаты поддельный документ могут не отправить вовсе, но даже если он придет, пользоваться такими справками уголовно наказуемо.

Кроме того, регистрировались случаи, когда мошенники приходили домой к потенциальным жертвам якобы с повесткой. Человеку предлагали за деньги не вручать ее, а иначе придется явиться в военкомат. Правда, массовой эта практика так и не стала.

В случае с фишингом собирались личные данные. Сразу после объявленной мобилизации в Интернете появилась якобы база данных граждан, которых государство планирует мобилизовать. На самом деле подобного списка в открытом доступе нет. Мошенники манипулируют страхом и выдают ложные данные за действительные, предлагая за деньги «исключение из списков мобилизованных».

Второй метод: дать ссылку на якобы полный список, а на сайте уже запросить личные данные и банковскую информацию у потенциальной жертвы. Переводить деньги и переходить по таким ссылкам не стоит.

«Мошенничество под видом государственных органов»

Это многоуровневые схемы звонков с участием якобы правоохранительных органов, Банка России и кредитных учреждений.

Чаще всего говорят о некоем безопасном счете в Центробанке, на который нужно срочно перевести средства, которым якобы грозит хищение. Кроме того, для убедительности присылают человеку в мессенджер или на электронную почту документы или удостоверения с логотипом и печатью Банка России. Также аферисты могут прислать скан-копию заявления о заявке на кредит якобы от лица жертвы с его ФИО и поддельной подписью. Со стороны все это выглядит очень правдоподобно. Критическое мышление у жертв при использовании таких приемов снижается.

Помните: Банк России не работает напрямую с физлицами. По своей инициативе его сотрудники не звонят гражданам, не рассылают им электронные письма и СМС-сообщения. Регулятор не обслуживает и не открывает счета физлиц.

В таких случаях необходимо сразу класть трубку, а также не называть свои личные и банковские данные вне зависимости от того, как представился человек по телефону.