Предупредительная информация об оперативной обстановке, связанной с совершением дистанционных краж и мошенничеств

Статистика:

За 6 месяцев 2024 года в Ханты-Мансийского автономного округа – Югры (далее – автономный округ) зарегистрировано 11 104 преступления, из них 3 494 (31,4%) дистанционные кражи (885) и мошенничества (2 609).

Справочно:

за 6 мес. 2014 года (10 лет назад) было зарегистрировано 762 мошенничества (6,3% от общего числа преступлений);

за 6 мес. 2020 года – 2 906 (27,5%);

за 6 мес. 2021 года – 2 790 (26,1%);

за 6 мес. 2022 года – 2 265 (21,5%);

за 6 мес. 2023 года – 3 078 (29,0%).

В среднем в сутки регистрируется 18-20 дистанционных краж и мошенничеств, в месяц почти 600 фактов (582,3).

Общий ущерб от данных преступлений 1,139 млрд рублей (за 6 мес. 2023 года – 658,7 млн руб., 6 мес. 2022 года – 295,2 млн руб.).

На Сургут (865), Нижневартовск (682) и Ханты-Мансийск (326) приходится более половины (53,6%) всех зарегистрированных в округе дистанционных краж и мошенничеств.

Сокращение числа дистанционных краж и мошенничеств не прогнозируется.

Для преступников данный способ обогащения становится все более привлекательным в силу разнообразия применяемых схем обмана граждан, высокой доходности, значительного уровня латентности и невысокого уровня раскрываемости данных преступлений.

Согласно исследованиям «Лаборатории Касперского» Российская Федерация на данный момент лидирует в мировом рейтинге по общему количеству инцидентов информационной безопасности.

У среднего российского пользователя риск стать жертвой киберпреступников и интернет-мошенников на данный момент находится на уровне 73-75%.

До коронавирусной пандемии показатель этого риска находился на уровне примерно 30-35%, но в течение последних 3-4 лет фиксируется существенный рост.

Цифровые технологии работают для Вас, но могут работать против Вас.

Портрет потерпевшего:

Дистанционным кражам и мошенничествам подвержены все категории населения вне прямой зависимости от возраста, пола, социального статуса, образования и т.д.

В результате совершения в 1 полугодии 2024 года 3,5 тысяч преступлений потерпевшими стали 426 пенсионеров (12,2%), в 249 случаях работники медицинской и образовательной сфер (7,2%).

Вместе с тем, это можно объяснить удельным весом данных категорий в общем числе жителей автономного округа.

Результаты опроса потерпевших свидетельствуют о том, что 99% из них знали о существующих угрозах стать жертвой мошенничества и были осведомлены об основных способах совершения данных преступлений.

Мошенники используют методы социальной инженерии, предварительно собирая о человеке необходимую информацию, в том числе в социальных сетях. В последующем преступники используют данные сведения чтобы втереться в доверие к потенциальной жертве и в последующем ею манипулировать.

В общении преступники обращаются как к слабостям человека (страх, алчность), так и к его достоинствам (вежливость, не позволяющая прекратить телефонный разговор; желание помочь попавшему в беду; готовность оказать содействие правоохранительным органам).

Часто в пользу мошенников срабатывает любопытство потерпевшего (а что будет, если я нажму на эту ссылку?), его лень (игнорирование рекомендации о замене пароля), самоуверенность (со мной-то ничего не случится) либо в совокупности – знаменитый русский «авось».

Схемы мошенничеств и краж:

24,5% – звонок сотрудника банка, Росфинмониторинга, сайта «Госуслуги», правоохранительных органов с информацией:

о подозрительных поступлениях и переводах денежных средств по счетам;

пресечение несанкционированного оформления кредита;

предложение помочь правоохранительным органам выявить мошенников в банковской организации путем оформления «встречного кредита» (зеркальная заявка) и перемещения средств на «защищенный» счет (ячейку);

17,7% – оплата или внесение предоплаты при совершении сделки по приобретению товаров на сайтах «Авито», «Юла», в социальной сети «ВКонтакте» и др., в том числе путем установки подозрительных приложений или переход по ссылкам на непроверенный или фишинговый ресурс с последующим вводом данных кредитных карт (счетов);

10,3% – инвестиции, приобретение криптовалюты, акций и др. (в данном случае часто виртуально показывается рост доходности, предлагаются бонусы за дополнительное вложение средств и привлечение других «инвесторов», при попытке вывести вложенные средства предлагается оплатить «страховку» и т.д.);

7% – кредитование в микрофинансовых организациях;

4,1% – оплата услуг (Бла-Бла-Кар, интим-услуг и т.д.);

3,8% – взлом аккаунтов социальных сетей и мессенджеров с последующим обращением за финансовой помощью;

1,1% – «родственник попал в беду».

«Новации» схем мошенничества:

мошенник представляется сотрудником оператора мобильной связи и предлагает продлить договор предоставления услуг связи (варианты – изменить тариф, вернуть «старый номер» и т.д.). Убедив потерпевшего сообщить код, поступивший в СМС-сообщении, мошенник получает доступ в его личный кабинет веб-банкинга либо на ресурс «Госуслуги», с последующим отключением абонента от данных ресурсов и хищением денежных средств или персональных данных;

предложение пройти флюорографию за счет медицинской страховки либо в дистанционном режиме продлить полис ОМС. Предложив выбрать клинику, для подтверждения записи предлагают сообщить поступивший код из СМС-сообщения;

мошенники, используя базу данных неиспользуемых номеров абонентов мобильной связи, проверяют наличие не отключенных кабинетов веб-банкинга, в последующем похищая денежные средства или используя эти кабинеты для дроппер-переводов;

использование чатов жильцов многоквартирных домов для «продажи» парковочных мест, излишков строительных материалов, бытовой техники, мебели по привлекательным ценам или предложение услуг по ремонту квартир. После получения предоплаты продавец исчезает из чата;

под видом налоговиков мошенники сообщают, что видят не учтенные при расчете налога суммы, поступавшие на банковский счет, и сообщают о необходимости пройти сверку налоговых платежей, якобы соответствующий документ уже был направлен налогоплательщику, предлагают ознакомиться. Документ, о котором говорят аферисты, не отображается в приложении «Мой налог» или в личном кабинете Федеральной налоговой службы. Тогда мошенники сообщают, что ресурс ФНС и портал «Госуслуги» рассинхронизировались, а для восстановления работы нужно назвать код из смс-сообщения;

от имени IT-компаний киберпреступники публикуют (как правило, в телеграм-канале) предложения о работе на удалёнке. Если пользователь отзывается на подобное предложение, лже-представитель компании начинает запрашивать у потенциального работника его персональные данные, после чего старается привязать к личному кабинету в онлайн-банке якобы телефонный номер корпоративной SIM-карты;

от псевдо-работников «Почты России» или же каких-то других почтовых служб поступает телефонный звонок с информацией о том, что человеку якобы поступила посылка из-за рубежа, за которую требуется перечислить таможенный сбор. В этом случае многие граждане сообщают

мошенникам, что они никакой посылки из-за рубежа не заказывали и не ждали. Тогда аферисты сообщают, что для отмены посылки и для того, чтобы не платить таможенный сбор, необходимо продиктовать код из СМС-сообщения, который придёт на телефонный номер абонента;

звонок пожилым людям от псевдо-работников Социального фонда России (СФР). Они сообщают, что размер текущей пенсии можно существенно увеличить, так как обнаружен неучтенный трудовой стаж. Поверивших в легенду приглашают «на консультацию» в Многофункциональный центр или отделение СФР для решения вопроса. Для записи на прием человек должен сообщить данные паспорта, СНИЛС, ИНН и озвучить код из СМС-сообщения;

мошенники используют детей для хищения денежных средств родителей. Пример: ребенок участвует в дистанционных онлайн играх. Ему поступает предложение приобрести время для продолжения игры, виртуальные предметы или способности героя и т.д. Не имея собственных средств, ребенок по указке мошенника сообщает данные банковских карточек родителей.

Мошенники чутко реагируют на происходящие в стране и мире события, учитывают сезонные факторы.

Аферисты связываются со школьниками, сдающими ЕГЭ, от имени наблюдателей пунктов проведения экзаменов через мессенджеры. В ходе разговора они запугивают подростков тем, что те якобы были замечены за списыванием во время написания работ, и предлагают им оплатить штраф, перейдя по ссылке.

Мошенники начали создавать в мессенджере «Telegram» специальные туристические чаты, которые представляют собой небольшие тематические сообщества по разным странам, курортам или даже отелям.

В таких чатах преступники представляются обычными туристами, которые якобы ищут попутчиков, или же гидами, которые приглашают на экскурсию в популярных туристических местах.

После этого схема обмана может быть разной. Например, злоумышленники могут потребовать внести предоплату за услугу, после чего пропадают с полученными денежными средствами. Или же предлагают зарегистрироваться на специальном сайте для поездки и ввести там свои персональные и платёжные данные.

Для продвижения мошеннических схем злоумышленники часто придумывают несуществующие государственные организации, обещающие гражданам социальные выплаты или другие услуги. Например, единый Компенсационный Центр Возврата Невыплаченных Денежных Средств (или ЕКЦ ВНДС), Департамент брокерских взысканий, Департамент арестованных счетов, Мосгосуслуги или Департамент поведенческого надзора, которые предлагают якобы найти себя в базе пострадавших от финансовых мошенников.

Информация о новых схемах мошенничества и принимаемых мерах по противодействию им размещается на телеграм-каналах «Лапша Медиа» (https://t.me/lapshamedia) и «Вестник Киберполиции России» (https://t.me/cyberpolice_rus).

О дропперах:

Дропперы или дропы — подставные лица, которые за вознаграждение предоставляют аферистам свои счета для транзита или обналичивания похищенных денег.

Часто мошенники выстраивают цепочки дропперов для запутывания следов движения похищенных денежных средств.

В большинстве случаев дропперов подыскивают в молодежной среде под предлогом дополнительного заработка (по некоторым оценкам, в России около 100 тыс. дропперов, из них 60% в возрасте от 14 до 24 лет).

Соглашаясь на «подработку», подростки и молодые люди часто не подозревают, что сами становятся соучастниками преступления.

Иногда дроппером можно оказаться практически случайно – например, если у вас украли учётную запись от электронного кошелька.

«Табу»:

сотрудники правоохранительных органов при расследовании преступлений не совершают процессуальных действий по телефону; предлагайте вызвать вас официальной повесткой для очного участия в расследовании; лучший вариант – просто повесить трубку;

сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные; лучший вариант – просто прекратите разговор;

«резервных счетов», «запасных или безопасных ячеек», «зеркальных кредитов» не существует – просто кладите трубку;

ни при каких обстоятельствах не сообщайте данные вашей банковской карты, а также секретный код на оборотной стороне карты;

не сообщайте пин-код третьим лицам;

сотрудники банка по телефону никогда не попросят пройти к банкомату;

никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно, мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте, действительно ли он просит о помощи;

в сети «Интернет» не переходите по ссылкам на неизвестные сайты;

не торопитесь, помните, что «бесплатный сыр только в мышеловке».

Самозапрет на выдачу кредитов:

С 1 марта 2025 года в России заработает Федеральный закон от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон «О

кредитных историях» и Федеральный закон «О потребительском кредите (займе)», по которому россияне смогут устанавливать самозапрет на выдачу кредитов. Разбираемся, как он будет действовать и в чем его минусы.

В чем суть самозапрета

Самозапрет — это ограничение, которое банк по заявлению клиента накладывает на операции, в том числе кредитование. Такая мера поможет обезопасить россиян от мошенников — снизить риск использования личных данных, включая копии паспортов, логины, пароли. Закон поможет тем, кто не хочет брать кредиты или боится, что за него это могут сделать другие люди. Но работать он начнет только с 1 марта 2025 года.

Как будет действовать запрет

Если вы захотите установить самозапрет, с 1 марта 2025 года это можно будет сделать через «Госуслуги» или МФЦ. Достаточно заполнить шаблон заявления и указать условия: например, вид кредитора (банк или микрофинансовая организация) или способ обращения за кредитом или займом (в офисе и дистанционно или только дистанционно). Отметка о том, что вы установили самозапрет, появится в вашей кредитной истории. Банки и МФО обязаны проверять ее. Если обнаружат отметку — обязаны в кредите отказать. А если все же выдадут его, то не смогут затем требовать от вас выплаты долга.

До 1 марта 2025 года самозапрет на выдачу кредитов можно устанавливать в самих банках или МФО. Для этого нужно прийти в офис и написать заявление о запрете онлайн-кредитования в конкретном финансовом учреждении. Практически все крупные банки предоставляют такую опцию, но каждый устанавливает свои условия и порядок оформления. Аналогичные запреты можно направить и в микрофинансовые организации.