Тысяча и один способ отъема денег у населения

Новые схемы нечестного отъема денег изобрели мошенники в 2020 году. Пандемия стимулировала у них творческий подход. Об этом на прошлой неделе шла речь на совместной пресс-конференции Банка России и УМВД по Ярославской области.

■ Ольга СКРОБИНА

Хищения в цифрах

Как сказал заместитель управляющего Ярославским отделением Банка России Евгений Ефремов, в России в прошлом году количество денежных операций, совершенных без согласия клиента, увеличилось на 34 процента по сравнению с 2019 годом, а объем денег, похищенных таким образом, увеличился на 52 процента. В Ярославской области тенденция схожая.

Средний размер такой транзакции – чуть больше 11 тысяч рублей. Но есть и рекордсмены. Так, в 2020 году ярославец перевел мошенникам порядка 6 миллионов рублей. В этом году пока рекордная транзакция – 3 миллиона рублей. Мошенники выманили у доверчивых граждан 9,8 миллиарда рублей, из них 8 миллиардов – у физических лиц.

– За 4 месяца этого года в Ярославской области количество преступлений с использованием информационно-телекоммуникационных технологий возросло на 46,8% по сравнению с аналогичным периодом прошлого года. Выросло количество хищений с использованием банковских карт, мобильной связи, сети Интернет. На 21,9% увеличилось количество мошенничеств, совершенных в отношении пожилых граждан, – сообщил заместитель начальника УМВД России по Ярославской области – начальник следственного управления полковник полиции Дмитрий Жигарев. – С начала этого года около 50 преступлений удалось предотвратить сотрудникам полиции просто потому, что они случайно оказались у банкомата в тот момент, когда паникующий человек пытался перевести деньги на «безопасный» счет.

Тренды и тенденции

Коронавирус внес свои коррективы и в банковские операции. В прошлом году был зафиксирован рост использования электронных средств платежей, увеличилась платежная активность населения в онлайне. Как сообщил Евгений Ефремов, рост таких транзакций к предэпидемическому году составил 23 процента.

В 2020-м как никогда ранее стали популярными покупки онлайн, многие практически отказались от офлайн-шопинга. Результат не заставил себя ждать. Следствием развития онлайн-торговли стали утечки персональных данных, которые, как известно, утекают в результате совершения торговых операций и оплат услуг в Интернете.

Зафиксирован рост мошенничеств, связанных с использованием дистанционного банковского обслуживания (ДБО). Объем хищений в ДБО вырос на 70,1% и составил порядка 3,8 млрд рублей.

– Если до 2020 года мошенники покушались большей частью на текущие финансовые операции, то в год эпидемии коронавируса под их прицел попали депозиты и кредитные средства. У людей отбирали даже то, чего у них нет, – деньги, оформленные в качестве кредитного займа, – рассказывает эксперт Ярославского отделения Банка России по кибербезопасности Андрей Коценко.

Популярные схемы

В прошлом году государство выплачивало пособия, оказывало меры соцподдержки, и этим тоже не преминули воспользоваться мошенники. Появились фишинговые сайты, где предлагалось оставить свои данные для выплаты пособий. Они-то и открывали доступ к банковским личным кабинетам.

Основные каналы связи мошенников и их жертв – телефон, электронная почта и мессенджеры.

Мошенники стали представляться не только службой безопасности банка, но и различными сотрудниками налоговых и социальных служб. Рассказывали, что государство назначило выплаты, но чтобы их получить, надо предоставить данные карты.

О популярных в 2020 году схемах мошенничества, связанных с получением различного рода выплат, и не только рассказал Андрей Коценко.

> ***«Чтобы как-то противодействовать мошенникам, Банк России выступил с законодательными инициативами. Одна из них дает возможность людям обратиться в банк с заявлением о добровольном ограничении на транзакции, совершаемые онлайн, и на денежные переводы. Но как эта норма будет работать, пока неизвестно – закон в стадии проработки.***

Первая схема – открытие депозита. Жертве звонит якобы сотрудник банка и рассказывает, что сейчас в связи с эпидемией коронавируса и прочими напастями предоставляются меры поддержки клиентам. Есть возможность открыть депозит по более высоким ставкам, и для этого даже не надо посещать банк, все можно сделать дистанционно. «Сотрудник» предлагает прямо сейчас, немедленно (ну а чего тянуть и раздумывать) открыть новый вклад под более выгодный процент и перевести туда деньги с вклада с менее выгодным процентом. Клиент соглашается, следует всем рекомендациям, и деньги с депозита исчезают.

Вторая схема – спасение средств. Эта ставшая уже привычной схема, при которой звонит «сотрудник службы безопасности» банка и говорит, что только что поступило заявление о закрытии вклада. «Сотрудник» обеспокоен, в чем же причина, хочет прояснить, чем же банк не угодил. Клиент уверяет – нет, никаких заявлений он не писал. «Сотрудник» сокрушается – это, стало быть, мошенники. Далее следует предложение перевести деньги с депозита на «безопасный счет». Клиент следует всем указаниям, и деньги исчезают безвозвратно.

Третья схема – кредитная карта. Клиенту поступает смс с непонятного телефонного номера о списании денег с кредитной карты и ее блокировке. Далее следует звонок от «сотрудника банка» с сообщением, что был несанкционированный доступ к кредитной карте. Клиент пугается. Но «сотрудник» предлагает ему «спасти» деньги с кредитки – всего-навсего пойти к банкомату, обналичить кредитную карту, а снятые деньги перевести на «безопасный счет».

Четвертый вариант – нужное приложение. Опять же звонит сотрудник «службы безопасности» с рассказом о попытке снять деньги. Клиент пугается – он же ничего не снимал. Далее следует предложение обезопасить телефон – ведь в нем есть доступ к безналичной оплате и ко всем банковским картам. Человеку предлагается установить безопасное программное обеспечение, достаточно всего лишь пройти по ссылке. Человек скачивает программное обеспечение, мошенники получают доступ к банковским приложениям и через них уводят деньги.

Пятый вариант – остановка операции. Начинается банально – со звонка «сотрудника службы безопасности» банка, который рассказывает о несанкционированном списании и о том, что карта заблокирована. Далее он выясняет все данные карты, просит назвать разовые пароли, которые приходят в смс. Здесь клиента держат в таком напряжении, чтобы он сам не входил в банковские приложения и не совершал там никаких действий. Мошенник, получив доступ к личному кабинету, переводит оттуда все деньги, успевает подать заявку на оформление кредита и даже вывести кредитные деньги.

Что делать?

Специалисты советуют: самый лучший способ обезопасить себя от мошенников – не вступать с ними в разговоры. Звонит «сотрудник банка», не стоит вести с ним беседу, нужно тут же нажать «отбой».

Если же клиент успел сообщить какие-то данные своей банковской карты или логины-пароли от личного кабинета, то перво-наперво надо позвонить в банк по номеру, указанному на карте, и заблокировать ее.

Следующий шаг – идти в банк. Там надо написать заявление о несанкционированном списании средств. Есть шансы приостановить операцию, вернуть средства. Так, в прошлом году банки вернули более 1,1 млрд рублей, или 11,3% от всего объема операций по переводу денежных средств, совершенных без согласия клиента. Но если клиент нарушил условия договора, предусматривающие необходимость сохранения конфиденциальности платежной информации, то в возврате средств откажут.

А уже после всего этого надо идти с заявлением о факте мошенничества в полицию. Увы, но как рассказал Дмитрий Жигарев, многие наши сограждане почему-то не хотят обращаться в правоохранительные органы с заявлением о том, что стали жертвой мошенников. Чаще всего причина банальна: люди стесняются, что поддались на уловки преступников. ■

> ***«К мошенничеству также относят ситуации, когда один человек забыл карту в банкомате, а другой ее нашел и воспользовался. Так, в этом году забытую карту нашел пенсионер, оплатил ею покупку бутылки водки и двух огурцов. Теперь дедушке на старости лет светит судимость.***