Криминал

Предновогодние сценарии кибермошенников

Преступники всё чаще используют новую схему обмана – «холодные» звонки чат-ботов

С начала года в Магнитогорске зарегистрировано более 1140 случаев мошенничества, ущерб от которых превысил 50 миллионов рублей. В масштабах страны потерпевшими стали десятки тысяч сограждан, а обманщики обогатились на 45 миллиардов рублей.

Евгений Рухмалёв

Один из способов совершения киберпреступлений – звонки с телефонов, начинающихся с 495, 497. Чаще всего абоненты этих номеров излагают потенциальным жертвам очередную схему обмана. Несмотря на предупреждения во всех СМИ, развенчивающие сказку о безопасных счетах, находится немало простаков, продолжающих верить, что с ними действительно говорят представители банков. Они послушно переводят деньги на указанные счета и теряют накопления. По такой схеме в прошлом месяце обманули магнитогорца 1978 года рождения. Позвонивший представился сотрудником службы безопасности банка и огорошил сообщением, что на магнитогорца оформлен кредит на 600 тысяч рублей. Клиенту банка необходимо либо подтвердить оформление кредита, либо уменьшить сумму. Через личный кабинет мужчина уменьшил сумму до 320 тысяч рублей, и, следуя совету лжесекьюрити, обналичил деньги и перевёл на «безопасный» счёт. Через месяц получил смс-сообщение о списании денежных средств, как первом платеже по кредиту, и только тогда осознал, что его обманули.

В последнее время преступники всё чаще представляются сотрудниками силовых структур, призывая граждан оказать содействие в задержании мошенников. Понятно, о «спецоперации» просят не говорить даже близким. Граждане верят, поскольку звонки поступают с подменных номеров, похожих на номера следственных комитетов, МВД, и называют конфиденциальную информацию о банковских картах. Если люди намереваются обратиться в банк и уточнить информацию о смене лицевого счёта или переводе денег на резервный счёт, то лжеправоохранители пугают уголовным преследованием «за распространение информации, полученной в ходе выполнения регламентных работ». Чтобы избежать неприятностей, следует зарубить на носу, что представители силовых структур могут позвонить по одной причине: пригасить в рабочий кабинет для личной беседы. Они никогда не обращаются за информацией дистанционно, по телефону, тем более с просьбой оказать содействие в поимке банковского вора, который якобы опустошает ваши счета. Положите трубку, перезвоните в дежурную часть УМВД и порадуйтесь, что не стали жертвой мошенников.

«Холодный» обзвон

На днях и на мой гаджет поступил звонок. Требовательная незнакомка спросила, проводила ли я транзакции по карте? Её напористость должна была рассеять последние сомнения: она – сотрудник банка. Не дожидаясь ответа, женщина застрочила, как из пулемёта, жонглируя экономическими терминами. Мои попытки вставить хоть словечко, игнорировались. Поступила мудро: осознавая, что это новая уловка мошенников, сбросила звонок. Повторного вызова не последовало. Это новая схема обмана – «холодные» звонки чат-ботов. Есть несколько вариантов информации. Например, робот сообщает абоненту: «Смена номера, привязанного к счёту, произошла успешно. Если вы не подавали заявку, нажмите «1» или дождитесь ответа оператора». Тех, кто сразу сбрасывает звонок, мошенники отсеивают. Жулики ищут человека, проявившего хоть минимальный интерес. Тогда его сразу переведут на лжеоператора, а дальше в действие вступают приёмы социальной инженерии – «атаки» на человека»: это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию.

«Российская газета» рассказала о новых, более изощренных и многоходовых схемах обмана. Мошенники стали пугать людей информацией, мол, ваша квартира пропала из базы Росреестра, кто-то пытается ею завладеть, или ваша машина исчезла из базы ГИБДД. Чтобы не потерять движимое и недвижимое имущество, людям предлагают срочно его продать. За машиной буквально через 30–40 минут приезжают перекупщики, вынуждая совершать сделку по заниженной цене.

Все чаще люди попадаются на заманчивые предложения поиграть на бирже. Положив 15–20 тысяч на виртуальный счёт, они через пару дней получают проценты – от трёх до четырёх тысяч рублей. Окрылённые идеей быстрого и сверхвысокого дохода, люди верят в успех, увеличивают взносы, влезают в кредиты, распродают имущество, но биржевые маклеры, обобрав наивных, заметают следы. Так, месяц назад неизвестные, выдав себя за финансовых консультантов, убедили магнитогорца «выгодно» вложить деньги в криптовалюту. Мужчину подкупило то, что первоначально он получил хоть и небольшую, но прибыль. «Консультанты» уговорили пожилого человека оформить кредит на 400 тысяч рублей и вложить деньги в криптовалюту. В общей сложности пенсионер перевёл более 550 тысяч, но деньги со счетов вывести не смог. Осознав, что стал жертвой обманщиков, обратился в полицию.

Несколько месяцев назад 47-летний мужчина также пытался обогатиться на криптовалюте. Занял около 200 тысяч рублей и купил виртуальные деньги. Обещанной прибыли так и не дождался, а вот денег лишился. Подобные преступления бьют чёрные рекорды. В стране зафиксирована самая крупная сумма, похищенная «финансовыми консультантами» – 12 миллионов рублей.

Фишинговые сайты

В сентябре в статье «Магнитогорского металла» «Киберпреступность как национальное бедствие» начальник отделения следственной части УМВД Магнитогорска подполковник юстиции Татьяна Шапкина, предостерегая горожан, рассказала, что в сезон распродаж и праздников на гаджеты приходят различные письма со ссылками на неизвестные сайты: «Традиционный вариант обмана – звонок с «выгодным» предложением: новогодняя акция, бесплатное обслуживание карты, понижение кредитных ставок. Для подключения к услуге надо назвать код из sms. Например, сообщается, что банк дарит клиенту на день рождения деньги, для получения которых надо перейти по ссылке на сайт банка. Сайт фишинговый, поддельный. Но люди вводят секретные данные, даже пароли от личного кабинета, что заканчивается хищением средств».

Обычному человеку не всегда под силу определить фишинговый, липовый сайт. Адрес сайта-клона может отличаться от оригинального всего лишь одной буквой. Бывает разница в одной запятой. Определить поддельный сайт могут лишь специалисты. В Челябинской области это спецподразделение «К» ГУВД.

В преддверии Нового года жертвой мошенников стала 48-летняя горожанка. В социальных сетях она нашла объявление о поставках импортных вещей. Отзывы были обнадёживающими. Женщина выбрала верхнюю одежду. Поставщики требовали 100-процентной оплаты и получили от заказчицы более 12 тысяч рублей. Женщине даже прислали код, свидетельствующий о движении товара, и заверили, что посылка придёт через 10 дней. Но товар она так и не получила. Горожанка отправила сообщение в группу, но её заблокировали. Лишь тогда женщина поняла, что стала очередной жертвой киберпреступников.

Подобная неприятность случилась с молодым человеком, который поднаторел в интернет-покупках. В соцсетях он прочёл объявление о продаже автомобильных шин и, не сомневаясь, выполнил просьбу продавца: отослал 36 тысяч рублей. Виртуальный визави заверил, что скоро покупатель получит товар. Но доставка задерживалась, а в соцсетях ни объявления, ни следов продавца не осталось. Понимая, что его обманули, потерпевший обратился в полицию.

Многоступенчатый обман

Эксперты зафиксировали, что мошенники стали разрабатывать сложные многоступенчатые схемы обмана. Звонят в течение нескольких дней, представляясь сотрудниками разных ведомств, охотясь не столько за паролями из sms или cvv-кодами, сколько за легковерными людьми. Массированная словесная атака продолжается до «победного» конца: на счету потерпевшего ни копейки плюс миллионные кредитные обязательства. Дистанционное банковское обслуживание и возможность кредитования по упрощенной схеме увеличивает количество обманутых людей.

По такой схеме преступники «работали» с 49-летней горожанкой. Несколько дней ей поступали звонки якобы от сотрудников различных банков, представителей силовых структур. Женщину даже уговорили проверить телефонный номер на принадлежность к конкретной организации. Магнитогорку напугали сообщением, что с её счетами происходят подозрительные операции, пресечь которые можно лишь одним способом: оформить кредит и перевести деньги на «безопасный» счёт. Она последовала совету, но банки отказывали в кредитах. Мошенники убедили женщину занять деньги у друзей и знакомых и оформить кредиты на членов семьи. Советы горожанка выполнила, лишив семью суммы, превышающей 420 тысяч рублей.

Летом 2021 года мошенники несколько месяцев звонили пенсионерке, используя приёмы социальной инженерии. В результате пожилая женщина продала квартиру и перевела миллионы преступникам.

По данным Центробанка, в третьем квартале года в России было совершено около 250 тысяч операций без согласия клиентов на сумму 3,2 миллиарда рублей. По сравнению с аналогичным периодом прошлого года объём похищенного вырос на 18 процентов. По количеству мошеннических операций лидируют платежи в Интернете, по суммам – переводы через систему дистанционного банковского обслуживания.

Чтобы не попасться на удочку мошенников во время новогодних распродаж, Центробанк и полиция рекомендуют пользоваться только известными сайтами, завести отдельную банковскую карту, можно виртуальную, и переводить на неё деньги непосредственно перед платежом. Кроме того, необходимо своевременно обновлять антивирусную защиту на компьютере, ноутбуке, мобильном телефоне. Во время сёрфинга в Интернете она подскажет, что ресурс, на который собираетесь выйти, опасен. Также советуют использовать официальные мобильные приложения магазинов и торговых площадок, что позволит защититься от попадания на ресурс злоумышленников.

Ирина Коротких