Криминал

Киберпреступность как национальное бедствие

За последние полтора года в стране в два раза увеличилось число IT-преступлений. По словам руководства Сбербанка, ситуация настолько сложная, что имеет все признаки национального бедствия. Ранее представители Сбербанка сообщали, что ежемесячно телефонные мошенники крадут со счетов россиян от трёх с половиной до пяти миллиардов рублей. Средний чек по мошеннической операции составляет примерно восемь тысяч рублей. Каждый десятый звонок любому абоненту в России – мошеннический, и в день таких звонков совершают около 100 тысяч.

Виктор Рамих

Фишинговые сайты

Редакция «Магнитогорского металла» постоянно публикует информацию УМВД о подобных преступлениях, рассказывая о способах обмана, предупреждая о новых жульнических сценариях. Однако легковерные граждане продолжают следовать указаниям лжесекьюрити банков и виртуальных следователей, переводят деньги на какие-то «безопасные» счета, в итоге теряя все сбережения. В очередной раз вынуждены обратиться к проблеме IT-мошенничества. Недавние случаи мошенничества в отношении магнитогорцев, потерявших внушительные суммы, заставляют вновь обратиться к злободневному вопросу. О новых схемах обмана, подробностях преступлений, поимке жуликов рассказали начальник отделения следственной части УМВД Магнитогорска подполковник юстиции Татьяна Шапкина и старший специалист группы по связям со СМИ Мария Морщакина.

Прежде чем говорить о жульнических ноу-хау, напомним старые схемы отъёма денег, с помощью которых преступники продолжают обогащаться. Подчеркнём, россияне каждый месяц лишаются до пяти миллиардов рублей.

– Люди попадают под психологическое воздействие преступников, – напоминает Татьяна Юрьевна избитую схему обмана. – Неизвестные, представившись сотрудниками силовых структур, сообщают о краже денег с банковского счёта абонента. Граждане верят, потому что используются подменные номера, похожие на номера следственных комитетов, МВД, и называют конфиденциальную информацию о банковских картах. Другой способ мошенничества связан с рассылками сообщений, например, что банк подарил 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 приводит к хищению средств.

Простому смертному не под силу определить фишинговый сайт, разобраться в подмене под силу только профессионалам. Сайт-клон отличался от оригинального всего лишь одной буквой. Бывает разница в одной запятой. Определить фишинговый сайт могут лишь специалисты, в Челябинской области это спецподразделение «К» ГУВД. В отделе имеется оборудование, позволяющее установить место регистрации сайта – за рубежом или на территории России.

Что касается денежных подарков, то «Коммерсантъ» сообщает о новой схеме мошенничества, связанной с акцией банков в рамках «школьных» выплат в размере десяти тысяч рублей на каждого ребёнка. Ряд банков пообещал увеличить сумму на тысячу рублей, если для получения денег будет использована их карта. Этим и воспользовались мошенники. Схема вполне классическая: пользователь регистрирует карту в программе мошеннического сайта, написав её номер и телефон, а затем вводит код из СМС. После этого обманщики получают доступ к онлайн-банку и списывают средства. Пока обнаружен только один подобный сайт – vtb-school.ru. Он был зарегистрирован 26 августа и на момент публикации уже не работал. По мнению экспертов, злоумышленники тестируют новую схему, и в случае её «успеха» количество таких сайтов может увеличиться.

– Один из способов обмана связан с рекламой, которая убеждает в возможности быстрого заработка на фондовых рынках, торгах, бирже, криптовалюте, – продолжает подполковник юстиции Шапкина. – Люди регистрируются в соцсетях, вводят личные данные, вкладывают деньги, играют, причём на большие суммы. Недавно допрашивала потерпевшую, сотрудницу учреждения бюджетной сферы с зарплатой 17 тысяч рублей, которая в различных банках города оформила кредиты на сумму, превышающую миллион.

– Другая магнитогорка объявление о высоких заработках нашла в соцсети, – уточнила Мария Морщакина. – Поверив рекламе, заполнила анкету на сайте, указала личную информацию. Ей позвонили якобы финансовые консультанты, уговорив вложить на «инвестиционные» счета по 30 тысяч рублей. Поначалу жулики перевели на её карту чуть больше тысячи рублей, якобы выигрыша, каждый раз убеждая увеличить вложения, тогда, мол, и доход возрастёт. Уверовав в свой успех, женщина вложила не только свои накопления, 400 тысяч рублей, но и оформила кредит на 600 тысяч. Прибыли она так и не дождалась, более того, лишилась денег. Сайт оказался заблокированным, телефонные номера отключены. Осознав, что стала жертвой обманщиков, изучила отзывы о сайте. Люди предупреждали, что это мошенническая платформа.

«Безопасный» счёт мошенников

– С недавнего времени в числе потерпевших стало больше молодёжи, – уточняет Татьяна Шапкина, – хотя на протяжении нескольких лет жертвами в основном становились люди пенсионного возраста. Во время допроса потерпевших выясняется, что об IT-преступлениях молодые люди слышали, знали, но самонадеянно считали, что их никогда не обманут. Совет: если поступил звонок якобы из банка или любой правоохранительной структуры во время цейтнота на работе, попросите перезвонить, либо внимательно выслушайте информацию. Мне тоже поступал подобный звонок. Человек говорил с явным акцентом. Россиян нередко атакуют преступники из стран СНГ. Чтобы не стать жертвой, вспомните информацию, которую не устают повторять правоохранители. Представители силовых структур могут позвонить по одной причине: пригасить в рабочий кабинет для личной беседы. Правоохранители никогда не обращаются за информацией дистанционно, по телефону, тем более с просьбой оказать содействие в поимке банковского вора, который, по их словам, опустошает ваши счета. Положите трубку, перезвоните в дежурную часть УМВД и убедитесь, что вы избежали печальной участи – не стали жертвой мошенников.

Ежемесячно телефонные мошенники крадут со счетов россиян от трёх с половиной до пяти миллиардов рублей

В последнее время преступники усовершенствуют схемы обмана, рассказывая байки о безопасных и опасных счетах. Звонят потенциальной жертве, сообщая, что с её счёта хотят украсть деньги, которые надо защитить – перевести на временный счёт. Затем на почту пользователя приходят поддельные письма из банков, в которых указывается, что средства находятся в безопасности. Если люди намерены обратится в банк, чтобы уточнить информацию о необходимости смены лицевого счёта и перевода денег на какой-то резервный счёт, пугают уголовным преследованием «за распространение информации, полученной в ходе выполнения регламентных работ». По такой схеме обманули нашу землячку.

– Подавшись на уговоры телефонного абонента, она снимает в банке полтора миллиона рублей, которые находятся якобы на опасном счёте, – продолжает Татьяна Шапкина. – Рассказывает мужу о добрых людях, оказавших помощь в спасении денег. Супруг отреагировал мудро, посчитав безопасным местом домашний сейф. Утром мошенники возобновили атаку. Женщина взяла деньги из сейфа и по указке неизвестных в терминале одного из сетевых магазинов стала переводить суммы якобы на безопасные банковские счета. Её не смутило, что в счёте непривычно маленькое число цифр. Это был номер телефона. Семейные накопления она потеряла.

Припоминаю случай, когда потерпевшая оформила онлайн-кредит на полтора миллиона рублей и в течение двух часов переводила деньги на указанные счета. Её друг не мог добиться объяснений и оттащить её от банкомата. Женщине заморочили голову уголовной ответственностью за разглашение банковской тайны. Конечно, стоит учесть психологическое давление, но можно было взглянуть на ситуацию трезво, дойти до банка, полиции? Поражаешься и негодуешь, насколько слепо люди верят словам неизвестного телефонного абонента. Подобные преступления трудно раскрываются даже по горячим следам. Кроме того, жертвы выполняют указания липовых следователей – до последнего молчат, пока не поймут, что попались в капкан мошенников. Подчёркиваю, нет опасных и безопасных счетов. Если деньги в опасности, банк сам блокирует и счета, и банковские карты.

Карточка с нулевым балансом

Сотрудники УМВД недавно задержали преступную группу из пяти человек. Они крали деньги, используя данные чужих банковских карт, которые люди оставляли в Интернете, допустим, подписываясь на приложения онлайн-кинотеатров. Сеть охватывала пять российских городов. Совет от подполковника юстиции Татьяны Шапкиной: «Для онлайн-покупок либо заведите карточку с нулевым балансом, на которой будет сумма, равная стоимости товара, либо не оставляйте реквизиты карты на сайтах подписок и всевозможных услуг».

Магнитогорские полицейские задержали ещё одну преступную группу. В соцсети «ВКонтакте» мошенники рассылали фишинговые сайты – клоны настоящих. Жулики заманивали акцией, которую якобы проводит банк – дарит клиентам деньги, и просили назвать секретные данные карт для перевода финансов.

– В числе преступников была и магнитогорка, – уточняет Татьяна Юрьевна. – Во время обыска у неё изъяли несколько дорогих часов, стоимость которых приближалась к миллиону рублей, несколько айфонов последних моделей за 100–150 тысяч рублей. Дама ни в чём себе не отказывала, швыряясь легко доставшимися деньгами. Да, справедливость восторжествовала, но не всегда можно обнаружить деньги и ценности, которые потрачены, например, на отдых в Швейцарии.

Ещё одна схема обмана связана с местами лишения свободы. Сидельцы просят людей помочь: назвать реквизиты банковских карт якобы для того, чтобы сделать один-два денежных перевода. За услугу обещают заплатить тысячу рублей. Добрые люди откликаются: подростки выдают секретные цифры родительских карт, на счетах которых вскоре не остаётся ни копейки.

В преступной цепочке есть деяния, которыми занимаются дропы – подставные лица, оформляющие на своё имя множество банковских карт с последующей передачей главарям группировок и обналичиванием средств. Люди соблазняются хотя и маленьким, не более тысячи рублей, но и лёгким заработком, не осознавая, что они, как соучастники преступников, также подпадают под уголовное преследование

– Мошенников, которые обналичивали и переводили деньги на указанные счета, установили и задержали в Иркутске сотрудники уголовного розыска Магнитогорска, – добавляет Мария Морщакина. – В группировке были распределены функции, соблюдалась иерархия, действия регламентировались негласными уставами. Подельники не знают друг друга, могут находиться в разных регионах страны, пользуются удалённой связью, что затрудняет раскрытие преступлений.

Мария Морщакина назвала цифры статистики IT-мошенничеств в Магнитке. С начала года зафиксировано 940 случаев, только за последние дни ущерб составил миллион 300 тысяч рублей.

Ирина Коротких