Очистят кошелек
Покупать дорогие фильтры для воды вынуждают мошенники

НЕИЗВЕСТНЫЕ люди просят впустить их в квартиру, под видом специалистов проводят некие «анализы» воды из крана, а потом заявляют о ее недопустимом качестве. Исправить ситуацию предлагается с помощью дорогостоящих очистителей для воды. Чаще всего жертвами таких продавцов становятся пожилые люди, поэтому важно знать, что представители госструктур не занимаются подбором и продажей бытовых фильтров.

Карточные шулеры

Как защитить свой банковский счет от киберпреступников

БЕЗОПАСНОСТЬ

Ульяна Вылегжанина, СЗФО

В прошлом году несколько тысяч владельцев банковских карт в регионах СЗФО лишились своих денег. Продвинутые жулики изобретают все новые способы краж с помощью виртуального пространства, SMS-сообщений и телефонных звонков, но сохраняют в арсенале и старые трюки. Корреспондент «Российской газеты» выяснила, как уберечься от высокотехнологичных финансовых преступлений и что делать, если вы все-таки стали жертвой киберпреступников.

РИА НОВОСТИ

Специалисты не устают напоминать, что коды от банковских карт необходимо хранить отдельно и не передавать даже работникам банка.

Не говорите никому

В Калининграде участились случаи мошенничества с использованием мобильных банковских сервисов. Об этом сообщает отдел «К» регионального УМВД, где раскрывают преступления в сфере высоких технологий. Только за одну неделю в полицию обратились десять человек. Все они размещали информацию о продаже того или иного товара на популярном сайте бесплатных объявлений.

Жулики звонили, представлялись покупателями и узнавали номера банковских карт жертв — якобы для того, чтобы перечислить предоплату. Зачастую мошенники говорили очень быстро, перескакивая с одного на другое, чтобы сбить продавцов с толку. В результате некоторые калининградцы сообщали неизвестным собеседникам код, необходимый для подтверждения операций в мобильном банковском сервисе. Беспрепятственно войдя в систему, мошенники переводили деньги с карт потерпевших на свои счета.

— Я продавала через Интернет стиральную машину за десять тысяч рублей, — рассказывает 30-летняя жительница Калининграда Татьяна. — Мне позвонил мужчина, сказал, что его очень заинтересовало объявление. Но вот незадача, живет он в Советске и забрать товар сможет только через три дня. А чтобы я за это время никому машинку не продала, он готов сразу перевести мне на карту всю сумму. Я согласилась, назвала номер карты. Мужчина перезванивает, просит назвать пароль для входа в систему «Банк онлайн» — мол, без этого он не сможет перевести деньги. Стоит пояснить, что этот человек очень быстро тараторил, несколько раз у него терялась связь, он снова перезванивал. Словом, мы с ним общались весь день, и у меня уже голова кругом шла. Еще маленький сын, ему два года, в это время капризничал. В общем, умом-то я понимала, что коды и пароли никому давать нельзя. А тут замоталась — и пароль сказала. Хорошо еще, что на карте было лишь 150 рублей. Мне пришла SMS, что операция на сумму десять тысяч рублей не прошла. Я и поняла, что он не мне предоплату хотел перевести, а с моего счета деньги снять.

Сотрудники отдела «К» призывают граждан к бдительности и внимательности. И напоминают, что пароли и коды, которые используются для подтверждения операций с денежными средствами и авторизации мобильных банковских сервисов, нельзя сообщать никому и ни под каким предлогом, даже сотрудникам банка.

Дорогие скидки

Мошеннический трюк с предоплатой работает и в обратном направлении. В Мурманской области больше 200 человек пострадали в прошлом году при попытке купить в Интернете дешевые товары. Жулики предлагают доверчивым пользователям Всемирной сети авиабилеты, мебель, одежду, бытовую технику и многое другое буквально за копейки. В погоне за «скидками» жители Заполярья переводили преступникам необходимые суммы, после чего контактные телефоны «продавцов» оказывались вне зоны действия сети.

Как пояснили в отделе «К» УМВД по Мурманской области, сайты, предлагающие заманчивые скидки, как правило, регистрируются за рубежом. Кроме того, мошенники используют хитрые схемы укрытия IP-адресов и многоступенчатую регистрацию.

— Такие преступления раскрываются тяжело, однако у нас есть и положительные примеры, — делится информацией начальник отдела «К» Вадим Гаврилюк. — Так, в этом году мы задержали неработающую жительницу Мурманской области, которая ранее уже привлекалась к уголовной ответственности за мошенничество. Продавая через социальные сети бытовую технику, она требовала предоплату. Возбуждено уголовное дело, по которому проходит больше 20 потерпевших.

По словам Гаврилюка, самый лучший способ обезопасить себя от мошенников — внимательно изучать все данные о регистрации сайтов и фирм, предлагающих баснословные скидки. Пользователи Интернета легко могут проверить, официальный это сайт или поддельный, введя в любой поисковик почтовый адрес компании. Порой солидные с виду фирмы указывают местом своей регистрации сарай или гараж. Или заявленных улиц вообще не существует.

Иногда дельцы снимают деньги с банковских счетов, просто запомнив номер карты, подпись ее владельца и специальные коды. Как правило, такие мошенники работают в сфере обслуживания.

— В текущем году несколько жителей Мурманской области пострадали от действий организованной группы, — продолжает начальник мурманского отдела «К». — Члены ОПГ, работая барменами в кафе и ресторанах, при расчете запоминали информацию о банковских картах. В дальнейшем они снимали денежные средства через интернет-кошельки. Сейчас уголовное дело находится в суде. За аналогичное преступление в Никеле преступная группа уже осуждена. Мы настойчиво рекомендуем жителям Заполярья никому и никогда не передавать свою банковскую карту в руки. При расчете за оказанную услугу вставляйте в переносной терминал карточку сами, после введения PIN-кода сразу же забирайте, и ни в коем случае не оставляйте ее официантам.

> Тяжелее всего раскрываются преступления, связанные с хищением денег с банковских карт с помощью вредоносных программ и вирусов

Ваша карта бита

Тяжелее всего раскрываются преступления, связанные с хищением денег с банковских карт с помощью вредоносного программного обеспечения, продолжает тему начальник отдела дознания мурманского УМВД Денис Колесников. В прошлом году в Заполярье возбудили порядка 800 таких уголовных дел. Раскрыть удалось больше 200 преступлений.

С одной стороны, затруднения связаны с тем, что деньги с помощью мобильных вирусов воруют киберпреступники из других субъектов РФ. С другой стороны, порой жертвы в течение долгого времени не знают, что их счет оказался в распоряжении мошенников. Вирус проникает в программное обеспечение мобильного устройства, и при несанкционированных операциях блокирует SMS-оповещения «мобильного банка».

Впрочем, даже если преступников привлекают к ответственности, возместить ущерб потерпевшим удается не всегда.

— Несмотря на меры, которые предпринимает полиция, мошенники успевают потратить добытые преступным путем деньги на собственные развлечения и предметы роскоши, — продолжает Денис Колесников. — Если от действий преступника пострадало несколько граждан, а общая сумма присвоенных денежных средств составляет несколько миллионов рублей, то процент возмещения ущерба каждому потерпевшему может быть достаточно низким.

Самый эффективный способ защитить свой банковский счет — это установить антивирусную программу на мобильное устройство, при этом базы данных антивируса должны постоянно обновляться. Как считают полицейские, лучше заплатить один раз за покупку актуальной антивирусной программы, чем постоянно рисковать деньгами.

ПРЯМАЯ РЕЧЬ

Олег Ефимов, калининградский юрист, специалист по направлениям «Защита прав потребителя», «Банки и кредиты»:

— В российском законодательстве строго определены случаи, в которых банк обязан вернуть деньги, похищенные с карты клиента. Речь идет о ситуациях, когда утрата произошла не по вине клиента — из-за недостаточной защищенности банковских сервисов, банкоматов, несовершенства клиент-банка и так далее.

Если же к утрате денежных средств привели действия самого владельца карты, банк имеет право не возвращать их. К примеру, распространено мошенничество, при котором злоумышленники создают фишинговую (поддельную) страницу банковского сайта. Человек вводит на подставном сайте данные своей карты. Злоумышленники перезванивают ему, представляются сотрудниками банка, узнают пароль, который приходит на телефон, и переводят все деньги на сторонние счета.

В этой ситуации клиент, по сути, собственноручно отдал деньги мошенникам. Во-первых, не проверил название страницы в адресной строке, что нужно делать обязательно, заходя в интернет-банк. Во-вторых, сообщил постороннему человеку пароль. И банк не будет нести ответственность за эти ошибки. Также нельзя потребовать у финансового учреждения деньги, если карта потеряна или украдена, а владелец не заблокировал счет. И таких примеров много.

Если же у вас списали деньги с карты, и вы уверены, что никак не способствовали мошенникам, в первую очередь необходимо позвонить на горячую линию банка. Затем в течение суток следует прийти в офис банка с заявлением о списании и требованием вернуть денежные средства. Полезно иметь при этом какие-то доказательства, что вы не могли совершить операцию. К примеру, что вы в момент списания денег были за границей, в другом регионе или в другой части города. Хорошо, если ваши слова подтвердят несколько свидетелей. Если банк откажется возвращать деньги, можно обратиться с иском в гражданский суд.

Параллельно необходимо как можно скорее написать заявление в полицию. Есть некоторые шансы, что мошенников найдут, и они к тому моменту не успеют потратить ваши деньги.