Приложение 1

В интернете активизировались финансовые мошенники

Охотников за чужими деньгами меньше не становится. Так, мегарегулятор стал инициатором блокировки более 400 нелегальных доменных имен. Организации, стоявшие за ними, занимались различными видами финансового мошенничества в интернете. Жулики маскировались под микрофинансовые организации, банки, форекс-дилеров, страховые компании. Однако никакого права работать в этой сфере они не имели: все легально действующие игроки на финансовом рынке обязаны иметь лицензию Банка России. Для потребителя подобная лицензия – это гарантия защиты его прав. «Проверить наличие лицензии не сложно, – поясняет управляющий Отделением по Владимирской области ГУ Банка России по ЦФО Надежда Калашникова. – достаточно зайти на сайт www.cbr.ru в раздел «Финансовые рынки», где представлен «Справочник участников финансового рынка»». На этом же сайте опубликованы постоянно обновляющиеся государственные реестры микрофинансовых организаций и кредитных потребительских кооперативов.

Ищите «белую метку»

Как же сегодня мошенники в интернете обманывают своих жертв? В основном, пользуясь невнимательностью граждан или их стремлением заработать легкие деньги. Одним из самых распространенных способов обмана можно считать махинации «черных» кредиторов. Эти жулики действуют разными методами. К примеру, организуют рассылку одобрений на «кредит» или звонят по телефону, рассчитывая, что хоть кто-то из адресатов действительно подавал подобную заявку. Откликнувшейся на предложение жертве предлагается заплатить «комиссию» за одобрение или рассмотрение заявки, причем, сделать перевод через крупный банк. Кстати, когда клиенты начинают жаловаться, что не получили кредит, самые циничные аферисты предлагают им… заплатить за рассмотрение «заявки» еще раз.

Впрочем, человек и сам может наткнуться на нелегальных кредиторов, когда ищет в интернете, где бы занять или куда под наибольший процент вложить деньги. В этом случае мошенники расставляют ловушку следующим образом: создают сайт, как две капли воды похожий на интернет-представительство известной финансовой компании. Человек без колебаний заполняет заявку на кредит, порой раскрывая данные своей банковской карты, – а в конце онлайн-цепочки остается и без заемных, и без собственных денег.

Иногда финансовые организации, которые лишились лицензии, продолжают через интернет предлагать «заем до зарплаты». Такая деятельность также незаконна. «Чтобы клиенту было проще опознать мошенников, Банк России применяет схему, разработанную вместе с Яндексом. В результатах поиска микрофинансовые организации обозначаются специальным знаком «Реестр ЦБ РФ»», – рассказывает Надежда Калашникова.

Выявляет Банк России также случаи, когда финансовые мошенники сумели обмануть не отдельных граждан, а целые предприятия. К примеру, организации с автопарком аферисты сумели продать поддельные полисы каско.

В компании с пирамидами

В интернете прочно обосновались финансовые пирамиды – компании, выплачивающие деньги вкладчикам из средств вновь пришедших клиентов. Мониторинг

Международной конфедерации обществ потребителей (КонфОП) показал, что подобные компании занимают верхние позиции в топ-30 поисковых запросов в интернете по вложениям средств. Организаторы мониторинга изучили выдачу поисковых систем «Яндекс» и Google по запросу «вложить деньги выгодно» с настройками, обеспечивающими объективность выборки, и затем провели анализ сайтов небанковских организаций, предлагающих вложение средств. Среди наиболее характерных признаков 25 выбранных организаций – обещания супердоходности, рассказы об «уникальных продуктах» и неправомерное использование символов государственной власти.

Мошенники могут называть себя инвестиционными фондами, прикрываться известными названиями и убеждать, что деньги вкладываются в «высокодоходные проекты». Например, представленные в мониторинге КонфОП компании обещали клиентам различный уровень доходности – от умеренной в 10–12% (за инвестиции в солнечную энергетику в Испании) до практически неосуществимой в 550% («игра» в ценные бумаги). Половина из рассмотренных компаний решили не указывать на сайте свои реквизиты, но при этом разместили различные «свидетельства» и «сертификаты» (в том числе иностранного происхождения), призванные доказать их надежность и состоятельность.

Как отмечают в Банке России, перенос деятельности финансовых пирамид в интернет – это тенденция последнего времени. Сейчас на долю интернет-проектов приходится четверть выявленных пирамид, 46% приходится на фирмы с признаками фиктивности, 29% – это пирамиды, маскирующиеся под микрофинансовые организации и кредитно-потребительские кооперативы.

Спешить медленно

Собственно, для выявления мошенников Банк России использует систему автоматизированного мониторинга интернета. Во Владимирской области зафиксированы факты хищений денежных средств с карточных счетов клиентов в размерах до 3 тыс. рублей. Преступления стали возможны в связи с использованием клиентами идентичных и упрощенных пин-кодов и паролей в одной из онлайн-систем. Также мошенники пользуются тем, что многие люди не соблюдают правила информационной безопасности при установке мобильных приложений. Зафиксированы случаи, когда на смартфон внедряется вредоносное программное обеспечение, позволяющее осуществлять удаленный доступ на короткий номер, с которого клиент обычно управляет счетом. Вредная программа без ведома клиента может распоряжаться его финансами, несанкционированно проводя отправку и получение SMS-сообщений, которые затем автоматически удаляются из памяти телефона.

«Если вы получили SMS-сообщение, письмо или звонок от предполагаемых мошенников – напишите обращение в Банк России в интернет-приемной на сайте www.cbr.ru. Если пострадали от действий жуликов – обратитесь в правоохранительные органы», – поясняет управляющий Отделением по Владимирской области ГУ Банка России по ЦФО Надежда Калашникова. А еще лучше – не попадать в подобные неприятные ситуации. Для этого нужно обязательно проверять лицензию финансовой организации, не верить излишне щедрым обещаниям и не спешить с принятием решений, связанных с деньгами. И, конечно, периодически обновлять программное обеспечение на смартфоне и компьютере.