Схемы хищения средств мошенники находят в соцсетях

Мошенники, которые крадут средства граждан с банковских карт, сконцентрировались на представителях среднего класса в возрасте 25–40 лет. Эти клиенты в основном предпочитают не обращаться в полицию, а делиться подробностями происшедшей неприятности в соцсетях. Злоумышленники отслеживают такие жалобы, выбирают наиболее удачные схемы хищения, дорабатывают их и активно применяют на практике.

О том, что активные пользователи социальных сетей, готовые всем рассказывать о каждом шаге, в последнее время стали невольными помощниками кибермошенников, рассказал заместитель главы главного управления безопасности и защиты информации Банка России Артем Сычев. По его словам, в 2017 году злоумышленники, использующие «социальную инженерию» для хищения средств с банковских карт, все чаще обращали свое внимание на людей в возрасте от 25 до 40 лет, относящихся к среднему классу.

«Данная выборка не случайна. Какое логичное действие человека, которого ограбили? Обратиться в полицию и в банк, чтобы сообщить о хищении, – рассуждает Артем Сычев. – Однако данная категория жертв злоумышленников предпочитает сообщать о хищениях в социальных сетях – «ВКонтакте» или Facebook, причем в подробностях расписывая все детали». Таким образом, мошенники фактически получают готовую инструкцию и применяют ее на практике, добавляет он.

Экспертам по информационной безопасности известно о подобной проблеме. Они считают бездумную активность в соцсетях крайне опасной. «Существуют совершенно легальные SMM-технологии, которые по тегам или же ключевым словам позволяют искать в сетях нужную информацию, их активно используют многие компании, например, для отслеживания упоминаний бренда, – рассказывает руководитель экспертного центра безопасности Positive Technologies Алексей Новиков. – При этом есть совсем недорогие программные решения, которые злоумышленники дорабатывают под свои цели».

По словам директора по маркетингу компании Solar Security Валентина Крохина, мошеннические схемы, полученные из соцсетей, потом публикуются в специальных

сообществах мошенников, дорабатываются и тиражируются. По словам Артема Сычева, почти каждое сообщение в соцсетях об успешной атаке в 2017 году сначала давало резкий всплеск аналогичных хищений, а потом модификацию атаки.

Речь идет о довольно простых, но многообразных схемах, рассчитанных в первую очередь на доверчивость граждан. «Например, злоумышленники звонят под видом сотрудника кредитной организации или МФО потенциальной жертве с сообщением, что ей одобрен кредит в режиме онлайн и теперь нужны лишь реквизиты карты для зачисления денег, – рассказывает господин Сычев. – Вариаций множество, и они постоянно модифицируются, в том числе с учетом данных из соцсетей».

Собранные данные злоумышленники чаще всего используют для хищений с использованием электронных средств платежа (в онлайн). Согласно статистике ЦБ, в 2017 году было совершено 317,1 тысячи хищений с использованием электронных средств платежа на сумму 961 млн рублей, среди которых более 90 % связаны с побуждением владельца карты к совершению операции путем обмана или злоупотребления доверием. Доля несанкционированных операций с картами, о которых пострадавшие не сообщили в правоохранительные органы, – 97 %. И это лишь статистика по инцидентам, о которых клиенты сообщили в банк.

Эксперты отмечают, что проблему излишней откровенности пользователей соцсетей, которая множит атаки, необходимо решать. В частности, до граждан необходимо донести риски публичного раскрытия определенной информации. «Когда речь идет о хищении нескольких сотен рублей, то для многих нет смысла обращаться в полицию: деньги не вернуть, однако поделиться хочется, – отмечает Алексей Новиков. – Но важно помнить о последствиях и делать это как минимум в личной переписке». Способствовать решению проблемы, по его мнению, могло бы введение упрощенной процедуры информирования полиции о подобных «копеечных» инцидентах, чтобы сложность процедуры не отпугивала пострадавших. По словам Валентина Крохина, самый действенный способ борьбы с этим явлением – применение сервисов мониторинга и анализа социальных сетей теми же правоохранительными органами и самими банками для выявления в них жалоб с описанием схем хищений для предотвращения повторной реализации их на практике.

(www.kommersant.ru)