Объем средств, который хакеры похитили с банковских карт россиян с помощью социальной инженерии – иначе говоря, классического обмана – в прошлом году составил 650 млн рублей. По сравнению с предыдущим годом этот показатель упал на 15%, поскольку россияне изучили наиболее популярные схемы мошенничества и научились не реагировать на них. Это следует из расчетов, которые для «Известий» провела компания Zecurion, специализирующаяся на безопасности банковского обслуживания. Впрочем, в нынешнем году, по ее прогнозам, объем хищений увеличится до 750 млн рублей. По словам экспертов, кибермошенники совершенствуют свои схемы. Например, они начали представляться сотрудниками налоговой и под предлогом необходимости погашения долга получают необходимые данные.

Кибермошенники, использующие методы социальной инженерии для хищений, как правило, звонят гражданам, представляясь сотрудниками банков, и просят сообщить данные карт (номер, CVV, PIN-коды и пр.). Также хакеры программируют интерактивные голосовые системы (IVR) для звонков гражданам. Или высылают на электронную почту клиентов банков письма со ссылками и файлами, ориентированными на их интересы. Открывая эти вложения, клиенты запускают вирус.

Одна из схем ориентирована на людей, продающих автомобили на различных интернет-ресурсах. В ней потенциальный покупатель предлагает сразу внести задаток за автомобиль на банковскую карту клиента. При этом «покупатель» просит продавца сообщить полученный на телефон код авторизации, назвав который, владелец не увидит ни задатка, ни своих денег.

По данным Zecurion, которая проанализировала информацию более сотни банков, в 2015 году объем хищений с банковских карт россиян составил 765 млн рублей. В прошлом году показатель снизился на 15% до 650 млн – граждане стали более опытными и уже не поддаются на прямолинейные ходы мошенников. Впрочем, по итогам этого года вновь ожидается увеличение объема хищений – до 750 млн рублей. Мошенники ввели новую схему обмана. Они звонят потенциальным жертвам, представляются сотрудниками Федеральной налоговой службы и под предлогом необходимости погашения задолженности выведывают необходимые данные. Иногда мошенники используют роботизированные обзвоны.

Руководитель направления противодействия мошенничеству Центра информационной

безопасности компании «Инфосистемы джет» Алексей Сизов уверен, что новая мошенническая схема будет актуальна еще минимум месяц. – Количество успешных атак будет зависеть от того, насколько подготовленными будут звонки от имени налоговой, будут ли их проводить по реальным должникам, – пояснил эксперт. – Обычно срок «жизни» мошеннической схемы – месяц или чуть больше, финансовая грамотность россиян растет, продвинутых клиентов банков все больше.

По прогнозам Алексея Сизова, злоумышленники будут изобретать новые схемы обмана потребителей.

– Нарушители используют как приманку новые сервисы дистанционной оплаты – например, Avito, а также появляющиеся платежные госуслуги – налоги, пошлины, – рассказал Алексей Сизов. – Обычных граждан чуть проще обмануть, представляясь именно сотрудниками госорганов.

Еще раз напоминаем: никому не сообщайте данные своих карт (номер, CVV, PIN-коды, одноразовые пароли от операций и пр.). Вы будете сами виноваты в том, что потеряли деньги, ведь данные сообщили именно вы. Банк не возместит потерянный ущерб. Обычно сотрудники банков спрашивают только ФИО и последние 4 цифры номера карты для проверки клиента. И то – когда клиент сам позвонил в банк.

2) Если вы сообщили данные карты и поняли, что вас обманули, звоните в банк и блокируйте «пластик». Возможно, средства удастся спасти, если вы окажетесь оперативнее мошенников.

(www.iz.ru)