Прокурор разъясняет. Как уберечь денежные средства на кредитных картах от мошенников

Развитие современных технологий оказывает влияние и на криминальную сферу. Если раньше на благосостояние граждан посягали лишь карманные и квартирные воры, то теперь с развитием онлайн-банкинга на охоту вышли такие «продвинутые» преступники, как фишеры, скиммеры и организаторы разнообразных мошеннических схем в Интернете.

Мошеннические операции с пластиковыми картами все более являются проблемой, как для владельцев кредиток, так и банковских работников.

Большая доля незаконных списаний происходит с помощью скимминга, т.е. считывания при помощи специального устройства данных с магнитной полосы карты. Применяются злоумышленниками и другие способы изъятия у невнимательных держателей карт размещенных на них денежных средств.

Одним из самых распространенных методов мошенничества является фишинг (от англ. fishing - рыбалка), когда мошенники получают доступ к конфиденциальным данным вкладчика от него самого. При этом злоумышленники используют несколько основных тактик.

Вариант первый – «звонок из банка» с просьбой о погашении задолженности по кредиту. Абонент предсказуемо отрицает наличие задолженности и кредита, тогда «представители банка» просят его уточнить данные своей карты - номер, PIN-код и дату выдачи, «чтобы больше не беспокоить по этому поводу». Если клиент сообщит все свои данные, мошенники без особого труда снимут средства с карты, изготовив ее фальшивый аналог.

Вариант второй - рассылка электронного письма, в котором от имени одного из крупных розничных банков сообщается о якобы последних новациях в его системе безопасности. Рассылка делается по широкому кругу адресов, и среди них, скорее всего, найдется какое-то количество клиентов интересующего их банка. Для отвода глаз запрашиваются некоторые сведения (вплоть до потребительских предпочтений), но самое главное - номер карты и PIN-код (еще могут поинтересоваться ответом на «контрольный вопрос»). К письму прикрепляется ссылка, якобы ведущая на сайт банка - эмитента карты. Но этот сайт - подделка, имитирующая логотип и дизайн сайта банка, которым пользуется выбранный мошенниками клиент. После заполнения этой анкеты данные клиента, а значит, и электронные средства, доступные на его карте, станут добычей мошенников.

Вариант третий - злоумышленники по электронной почте или на аккаунт (страничку) в соцсети присылают код, который рекомендуют вставить в строку браузера, либо ссылку, по которой они предлагают пройти. Но на

самом деле это фишинговая программа, скачивающая с вашего компьютера и пересылающая преступникам файлы cookies, которые отражают маршрут заходов выбранной ими жертвы в различные сервисы. В том числе, возможно, и пароль к личному кабинету в системе банка, которым пользуется этот гражданин.

Чтобы не стать жертвой фишинга, необходимо соблюдать элементарные правила. Прежде всего, нельзя допускать, чтобы данные вашей карты попадали к третьим лицам, тем более незнакомым. Банки и операторы платежных систем никогда не присылают писем и не звонят клиентам с просьбой предоставить им данные о счете, PIN-код или иные персональные данные - вся необходимая информация у банка и так имеется. Банк просит клиента лично заехать в офис или, если это vip-клиент, присылает к нему курьера. И еще - стоит взять себе за правило с ходу стирать пришедшие на ваш электронный адрес сообщения, содержащие непонятные вам коды.

Сами банки рекомендуют клиентам немедленно прекращать любую финансовую интернет-операцию, если возникли малейшие подозрения, что она проходит нештатно, и тут же обращаться к специалистам банка. Необходимо также как можно чаще проверять выписки со своего счета, для чего из соображений безопасности желательно подключить услугу sms-информирования о совершенных операциях.

Прокуратура Колосовского района