Целевое интервью с начальником УУР ГУ МВД России по Алтайскому краю полковником полиции Э.О.Сороколетовым по профилактике дистанционных мошенничеств

Предупреждён – значит, вооружён: как не попасть в сети мошенников

Полицейские предупреждают: никому не передавайте свои пароли и коды!

В последнее время не только в Алтайском крае, но и в России, в целом, широкое распространение получили так называемые дистанционные мошенничества, совершаемые с использованием мобильной связи и сети Интернет. О профилактике подобных преступлений в сфере IT-технологий, защите своих персональных данных, о том, что нужно знать гражданам, чтобы не стать жертвой злоумышленников рассказывает Эдуард Сороколетов, начальник Управления уголовного розыска Главного управления МВД России по Алтайскому краю.

- Эдуард Олегович, какие виды дистанционного мошенничества в крае встречаются чаще всего?

- На сегодняшний день в крае распространены мошенничества, совершаемые с номеров 8800 и 495, которые граждане воспринимают как «горячие линии» банков. Злоумышленники сообщают, что являются сотрудниками службы безопасности банков, и что с вашего счета произошло несанкционированное списание денежных средств, либо говорят, что карта заблокирована. Просят назвать реквизиты карты, пароль CVC и коды доступа, пришедшие по СМС. Таким образом получают полный доступ к счёту и похищают деньги. Сотрудники полиции совместно с экспертами Центробанка постоянно напоминают о том, что ни коем случае нельзя подходить к банкомату и вообще выполнять какие-либо манипуляции с использованием информации о своих картах и счетах под диктовку неизвестных лиц по телефону.

Кроме этого, потребителей обманывают при сделках купли-продажи, которые заключаются через интернет. Злоумышленники выставляют объявления, потерпевшие перечисляют оплату или аванс за товар, объявления тут же исчезают, а телефоны «липовых» продавцов оказываются недоступны. Либо обратная история: потерпевшие размещают объявления, а им звонят мошенники, якобы, для того, чтобы перевести аванс. Люди сами сообщают коды и пароли доступа к счету и в результате лишаются средств.

Имеют место взломы страниц в социальных сетях, когда приходят письма от имени знакомых с просьбой занять деньги. Достоверность такого письма нужно обязательно перепроверить у знакомого или близкого человека, который входит в круг друзей вашего аккаунта и от имени которого пришло сообщение. Популярен такой вид мошенничества как предложение помощи для оформления кредита. В результате граждане сами передают данные своих документов, карт, счетов, и мошенники пользуются этими данными, чтобы похитить имеющиеся на счетах средства или оформить кредит на ничего не подозревающего гражданина, а полученные в кредит деньги опять же оказываются похищенными. Пожилым людям часто предлагают купить медицинские приборы либо БАДы, после чего в базе остаются их персональные данные и номера телефонов. Через некоторое время потерпевшим вновь звонят потенциальные мошенники и говорят, что вам положена компенсация за приобретенный некачественный товар либо БАД. Но за получение этой компенсации предлагают перечислить на чужие счета достаточно приличные суммы. В надежде получить бОльшее пожилые люди лишаются своих сбережений.

- Хотелось бы немного статистики: насколько активизировались мошенники? В чем сложность борьбы с дистанционными мошенничествами?

- Количество дистанционных мошенничеств неуклонно растет. В крае за полгода количество подобных преступлений возросло на 46, 7 % (с 560 до 1511 преступлений). Противоправные деяния совершаются с использованием большого количества сим-карт и телефонов. При этом мошенниками используются различные платежные системы. Они действуют с территории других регионов. Будучи хорошими психологами, мошенники в телефонной беседе под различными предлогами уговаривают людей перевести деньги с их банковских карт на счет некоего абонентского номера через те или иные платежные системы (экспресс-переводы, онлайн-сервисы) или же передать их лично в руки неустановленному лицу. К сожалению, основной причиной распространенности телефонного мошенничества по-прежнему остается доверчивость граждан. Чаще всего жертвами становятся женщины и люди пожилого возраста.

«горячую линию» банка. Обращаю особое внимание – никогда сотрудники банков инициативно не звонят клиентам. Код с обратной стороны карты (CVC) нельзя никому сообщать ни при каких условиях! В социальных сетях использовать более сложные, многоступенчатые пароли, чтобы страницу не взломали. При продаже-покупке через Интернет нужно внимательно изучать страницу продавца. Ни при каких обстоятельствах нельзя передавать посторонним лицам сведения о своих счетах и банковских картах, а также не совершать никаких действий со своими картами и вкладами, о которых просят незнакомые лица по телефону. При возникновении любых вопросов либо сомнений необходимо проконсультироваться непосредственно в отделении банка, позвонить на горячую линию кредитной организации, уточнить сведения по телефону доверия полиции, обратиться в ближайшую дежурную часть или даже к сотруднику полиции, которого вы увидели на улице. Будьте бдительны. Не отдавайте свои деньги мошенникам!