ПРОКУРАТУРА Г. НОВОСИБИРСКА РАЗЪЯСНЯЕТ

В последнее время участились случаи мошенничества в сети «Интернет». Наиболее распространенными способами являются следующие:

Способ №1. Фейковые СМС от банка. Злоумышленники присылают на номер жертвы СМС с текстом о том, что ее карта заблокирована. В конце сообщения указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит и попадает в руки злоумышленника, выполняя его просьбы и, сам того не замечая, передает свои конфиденциальные данные и деньги в чужие руки.

Способ №2. Словосочетание «служба безопасности» на многих действует как красная тряпка. Потенциальной жертве звонит якобы менеджер по работе с клиентами или другой подобный специалист и обращается по поводу заявки по кредиту, которую Вы якобы оформили на сайте. Как правило лжеменджеру удается выманить данные, которые позволят подключить мобильный банк жертвы, после чего он может и кредит оформить и сбережения украсть.

Способ №3. «Мы расследуем преступление». Звонит преступник, скомканно представляется служащим управления по борьбе с экономическими преступлениями и пр. Затем говорит, что они зафиксировали случай мошенничества с Вашей картой, счетами, кредитами, может начать запугивать. Смысл в том, чтобы подвести жертву к «сотрудничеству». Потерпевшему якобы надо пойти в банк, завершить оформление кредита, получить денежные средства и перевести их на «специальный защищенный счет».

Способ №4. «Вам только что звонили мошенники». Сначала потенциальной жертве звонит очевидный мошенник, которого легко проигнорировать, а затем с ней связывается сотрудник банка или полицейский и говорит, что зафиксировали звонок мошенника. В процессе лжесотрудник просит назвать данные карты или перевести деньги на спецсчета.

Способ №5. Поддельные ресурсы. Есть популярный сайт, где Вы можете быстро оформить онлайн-займы или инвестировать свои деньги, но злоумышленники могут зарегистрировать похожий домен и сделать точно такой же дизайн и личный кабинет. На первый взгляд ничего подозрительного. Вы вкладываете свои деньги, чтобы получать проценты, а как оказалось Вас обманули мошенники. Всегда проверяйте название домена.

Первое, что нужно сделать, если Вы стали жертвой мошенника, это сообщить о случившемся в ближайшее отделение полиции.