

Телефонное мошенничество – один из самых распространенных видов преступной деятельности в наше время. Основной целью любого мошенничества является хищение денежных средств. Для хранения, использования и вывода похищенных денежных средств злоумышленники используют банковские карты, расчетные счета, электронные кошельки («Киви банк», «Яндекс.Деньги», «ВебМани», «Тинькофф-мобильный кошелек»), счета абонентских номеров, наличные переводы («Колибри», «Вестерн Юнион», «Золотая корона», «Форсаж»). Часто встречается такая схема мошеннических действий, при которой злоумышленник создает сайты в виде Интернет-магазинов и похищает деньги, «продавая воздух».

Мы часто встречались в своей повседневной жизни с абонентскими номерами, которые начинались на «8-800-...». Эти номера наиболее яркие представители SIP-телефонии, которая отличается от привычной сотовой связи тем, что она не требует наличия сотового аппарата или подключения к базовой станции, все звонки поступают на персональный компьютер или смартфон через специальное приложение. При этом для звонящего каких-либо видимых изменений не происходит, а для мошенника это похоже на входящий вызов в «Skype», «Viber», «WhatsApp». Отличительными особенностями SIP-телефонии являются:

- входящие звонки могут поступать на несколько компьютеров одновременно, при условии, что все они подключены к одному аккаунту (стандартная работа всех Call-центров, когда вам отвечает первый освободившийся специалист);

- на один аккаунт можно зарегистрировать бесконечное количество виртуальных номеров;

- виртуальные номера могут иметь любой вид, как привычный нам 8(800)-..., так и 8(499)-..., 8(475)-... и др., даже абонентские номера операторов сотовой связи. Поэтому если мошенником был использован абонентский номер, внешне похожий на стационарный (с указанием кода любого города), можете быть уверены – это виртуальный номер SIP-провайдера. Ни один мошенник не может быть настолько глуп, чтобы звонить с домашнего телефона.

Наиболее частые телефонные и интернет-мошенничества:

- мошенник размещает на сайтах объявлений (Авито, Юла, Циан и др.) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или оказание каких-либо услуг, за которые в последующем получает предоплату, тем самым похищая деньги;

- мошенник звонит по объявлению, размещенному на сайте (Авито, Юла, Циан и др.) и говорит, что желает приобрести товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код. Получив данные сведения, осуществляют перевод через онлайн сервисы или совершая покупки. Или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк, и в последующем похищая денежные средства;

- мошенник совершает в сети Интернет взлом страницы социальной сети (Вконтакте, Одноклассники, ДругВокруг и др.), в последующем пишет всем друзьям из списка сообщения с просьбой занять денежные средства под различными предлогами («заболел родственник», «срочно необходима материальная помощь для операции», «не хватает на срочную покупку» и т.д.), либо сообщение об оказании помощи в получении какой-либо денежной выплаты, компенсации, льготы, якобы предусмотренных законодательством («надбавка к пенсии для граждан старше 40 лет», «компенсация за кредит» и т.д.);

- мошенник создает Интернет сайтах по продаже товара различной тематики. Регистрируется несколько виртуальных номеров (8(800)-..., 8(499)-... и др.) у SIP-провайдера и указывает их на сайте в качестве контактов. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта;

- мошенник звонит в организацию и говорит, что желает воспользоваться ее услугами по заказу банкета, заказу крупной партии товара или прочих услуг. Далее он сообщает адрес, где бы он хотел встретиться с представителем компании и спрашивает его телефон. В последующем он связывается с представителем и просит последнего по пути пополнить счет абонентского номера (или банковской карты) на определенную сумму, которую он «отдаст при встрече»;

- мошенник осуществляет рассылку SMS-сообщений с текстом о списании денежных

средств или блокировке банковской карты. В данном сообщении указывает свой другой абонентский номер (иногда виртуальный (8(800)-..., 8(499)-... и др.), который может проинформировать о произошедшем. Жертва звонит по данному номеру, после чего мошенник просит либо сообщить контрольные данные банковской карты, либо просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк, и в последующем похищая денежные средства;

- на стационарный или абонентский номер гражданина звонит мошенник, который обращается под видом родственника («Привет, мама», «Привет, бабушка» и т.д.) и сообщает, что «попал в ДТП и сбил человека», «с кем-то подрался» и тому подобное, а после передает трубку якобы «сотруднику полиции», который за отдельную плату предлагает решить вопрос об отказе в возбуждении уголовного дела;

- на стационарный или абонентский номер гражданина звонит мошенник, который представляется сотрудником прокуратуры или правоохранительных органов и сообщает, что в настоящее время задержана группа мошенников, продававших некачественные БАДы, и что гражданину положена компенсация, но для ее получения необходимо оплатить государственную пошлину или налоговый сбор;

- на сотовый телефон с операционной системой «Android» с неизвестного номера приходят SMS-сообщения с текстом «Здравствуйте, я по Вашему объявлению. Не интересует обмен с доплатой? Ссылка www.avit.o.ru/FriZksk)», или SMS-сообщение с текстом: «Смотри как мы здорово получились на этой фотографии. Ссылка www.bit.ly/ZreizE1eaAa)». Жертва проходит по данной ссылке, загружая на свой телефон вирус, предоставляющий злоумышленнику доступ к SMS-командам. в дальнейшем мошенник похищает деньги путем направления сообщений на номер 900.

Не попадайте на уловки мошенников, которые пользуясь «эффектом неожиданности», требуют от жертвы выполнения всех действий: «пиши код сразу же», «назови кодовое слово», «не обращай за помощью к сотрудникам банка», «не говори родственникам». Не сообщайте никому контрольные данные по банковской карте и поступивший код доступа к вашим счетам. В случае получения на мобильные телефон, в социальной сети сомнительных сообщений о блокировке карт, предоставлении льгот, сомнительных телефонных звонках, проверяйте информацию у официальных источников, не поленитесь перезвонить родственникам для проверки достоверности полученной о них информации, не вносите оплату за товары и услуги, не будучи уверенным в продавце.

Будьте бдительны и осторожны, так вы убережете себя от мошенников!

Старший следователь следственного отделения отделения МВД России по Шенталинскому району майор юстиции Филиппова Ирина Витальевна