Телефонное мошенничество.
Как не стать жертвой обмана?

Мошенничества, совершаемые с использованием мобильной и проводной связи

1) сотовый и проводной телефон используется как средство передачи голосовой информации:
- «ваш сын попал в аварию...»,
- «мама/папа у меня проблемы...»
- «это из банка/соцзащиты и пр...»,

2) сотовый телефон используется для передачи СМС с ложной информацией:
- «мама, кинь мне на этот номер денег, потом все объясню»,
- «ваша карта заблокирована подробности по тел..»,
- «с вашего счета списано 5000 рублей, подробности по тел...».

3) сотовый телефон и ваше объявление в сети Интернет (сайт Avito и другие подобные сайты) используется мошенником для получения от вас данных карты и привязки карты к мобильному телефону мошенника:
- «я по вашему объявлению на авито (о продаже, о сдаче в аренду), сообщите мне данные с вашей карты и код на обратной стороне я вам отправлю деньги...»;
- «я хочу отправить деньги вам на карту за товар на авито, предоплату за аренду, у вас карта привязана к мобильному банку, если нет, идите к банкомату я вас проинструктирую как подключить мобильный банк».

При получении сообщения не нужно перезванивать на указанные номера. Мошенники могут потребовать передать деньги курьеру, перечислить их на карту, номер мобильного телефона, попытаются получить от вас сведения о Вашей банковской карте, предложить пройти к банкомату и совершить какие-либо операции у банкомата, попросят сообщить коды которые приходят к Вам на телефон. В случае получения входящего звонка необходимо прекратить разговор, даже если собеседник вселяет уверенность в своей правдивости.

При сомнении в правдивости полученной информации следует перезвонить близким от имени кого пришло сообщение, позвонить в банк по указанному на карте, либо в договоре телефону, посетить ближайшее отделение банка.

Банк никогда не запрашивает по телефону сведения о карте клиента: ее номер, код на обратной стороне, Ф.И.О. владельца карты и срок её действия, а тем более пин-код. Если собеседник пытается получить от вас такую информацию, либо просит сообщить коды, которые пришли на Ваш телефон от банка, прекратите с ним разговор.

4) сотовый телефон используется мошенниками для передачи СМС сообщения, сообщений через мессенджеры Viber, WhatsApp с вредоносной информацией. Типы сообщений: «здесь наши с тобой фото http:\\...», , «ваш акакунт, страница «вКонтакте» взломаны, пройдите регистрацию http:\\...», «вы выиграли автомобиль, подробности http:\\...", «я по вашему объявлению, согласны ли вы на обмен на это http:\\foto3.inc...»

При получении данного сообщения откажитесь от прохождения по указанной ссылке и активации полученных ссылок.

Мошенничества, совершаемые в сети Интернет и с помощью сети Интернет

1. «Чудесные» автоматические программы

На ваш почтовый ящик приходит письмо с заманчивым предложением. Авторы рассылки обещают, что выполнив несколько элементарных действий, вы начнете получать, к примеру, от 7 до 22 тысяч рублей. Программа, естественно, не предоставляется бесплатно. За скачивание придется заплатить. Однако цена возможности «молниеносного обогащения» редко превышает 200-250 рублей. Вы вносите нужную сумму, и что же дальше? Ничего. Быстро становится понятно, что никакой автоматической программы не существует.

2. Фишинг – обман с приманкой

Для того, чтобы воспользоваться вашими деньгами, махинаторы должны для начала «выудить» необходимые сведения.

На практике это выглядит следующим образом. К примеру, вы получаете письмо, где ваш банк весьма убедительно просит ввести и подтвердить персональные данные: логин, пароль, пин-код. Делается это якобы для безопасности при срочном обновлении или технической перезагрузке сайта. При этом оформление фиктивного онлайн-ресурса по дизайну очень напоминает оригинальную страницу банка в сети. Как только данные предоставлены, злоумышленники присваивают ваши деньги.

Обратите внимание, что персональные данные и, самое главное, пин-код – информация исключительно конфиденциальная.

3. Уловки интернет-магазинов

Защитить себя в данном случае несложно. Оплачивайте товар только после доставки, проверяйте его качество и технические характеристики, заранее обговорите с продавцом возможность и способы возврата, а также перед заказом почитайте отзывы и задайте онлайн-консультанту вопросы о товаре. Полную и внятную информацию мошенники обычно предоставить не могут.

4. Компьютерные вирусы и блокировщики операционных систем

Если вы столкнулись с тем, что операционная система вашего компьютера заблокирована, а для разблокировки необходимо заплатить или ввести платный sms-код, не пугайтесь и не ведитесь на этот развод. В данном случае придется просто переустановить операционную систему и просканировать ее с помощью Avast, Dr.Web, Касперского или любого другого антивируса.

5. «Благотворительный» лохотрон

Для поддержки людей, которые оказались в сложной ситуации, создаются благотворительные фонды и организации. Однако огромное количество махинаций прикрывается именно просьбами о помощи. Сайты-подделки полностью дублируют ресурсы, которые действительно собирают средства на лечение детей, защиту природы, приюты для животных и т.д., изменив только реквизиты для перечисления финансовой помощи. Чтобы ваши деньги получили те, кто действительно в этом нуждается, проверяйте данные, обратитесь в банк, запрашивайте дополнительные информацию, уточняйте, на что будут потрачены средства.