Всем главам Ермаковского района

ИНФОРМАЦИЯ
для опубликования на сайтах

Одним из важнейших направлений деятельности правоохранительных органов является профилактика мошенничеств с использованием средств мобильной связи.

Пользуясь доверчивостью, преступники представляются работниками различных социальных учреждений, благотворительных фондов или жилищно-коммунальных служб, коммерческих организаций и банков, вводят людей в заблуждение, завладевают денежными средствами. Наиболее уязвимыми являются люди пожилого возраста.

Чтобы не стать жертвами мошенников обращаем внимание на ситуации, которые должны вас насторожить.

Телефонное мошенничество

Вам звонят с сообщением, что родственник или знакомый попал в беду. Для решения вопроса необходимы деньги, которые следует доставить в определенное место или передать какому-либо человеку. Находясь в стрессовом состоянии, люди выполняют эти указания.

Во-первых, не паникуйте, прервите разговор и перезвоните «попавшему в беду». Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации.

Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции, его должность и фамилию.

Также вы можете задать вопрос личного характера (например, попросите уточнить фамилию, имя, отчество или дату рождения родственника или знакомого, от лица которого вам звонят), так как данная информация обычно неизвестна мошенникам.

СМС-мошенничества

Типичные для таких случаев сообщения: «Мама, закончились деньги, срочно положи на этот номер» или «Вы стали участником лотереи! Вы выиграли приз, необходимо оплатить за него налог блиц-переводом или через терминал оплаты услуг».

Вам сообщают о крупном денежном или вещевом выигрыше по SMS и предлагают отправить SMS-сообщение или позвонить по указанному номеру для получения приза. Не делайте этого! Это, как правило, мошенничество!

Мошенничества с пластиковыми картами

Вам приходит сообщение о том, что ваша банковская карта заблокирована и предлагается бесплатно позвонить на определенный номер для получения подробной информации, не торопитесь звонить по указанному телефону.

Чтобы похитить денежные средства, злоумышленникам нужен номер вашей карты и ПИН-код. Как только вы их сообщите, деньги будут сняты с вашего счета.

Не сообщайте реквизиты вашей карты! Ни одна организация, включая банк, не вправе требовать ваш ПИН-код.

Для того, чтобы проверить поступившую информацию о блокировании необходимо позвонить в клиентскую службу поддержки банка.

«Вирусные» хищения

На мобильный телефон потерпевшего заносится сторонняя вредоносная программа (ВИРУС), которая блокирует операционную систему телефона и дистанционно управляет ею.

В телефон, к абонентскому номеру которого подключена услуга «мобильный банк», она может быть занесена как неумышленными действиями потерпевшего, так и целенаправленными действиями мошенников.

Это наиболее сложные к разрешению сообщения о преступлениях, т.к. денежные средства с банковской карты потерпевшего переводятся на различные счета и абонентские номера, зачастую используемые как транзитные. SMS – оповещения о производимых операциях со счетами в большинстве случаев скрываются указанной программой от потерпевшего, т.е. SMS о списании денег на абонентский номер потерпевшего не приходят.

Лучше всего использовать комплексное решение для борьбы с вредоносными программами – антивирус. Такой инструмент защищает сразу по всем фронтам: не только выявляет вирусы, но и проверяет СМС, инспектирует ссылки в браузере и загружаемые файлы, а также периодически сканирует телефон на предмет угроз.

Мобильный банк

Потерпевшими становятся граждане, которые, сменив телефонный номер, забывают отключить услугу «мобильный банк» и новый владелец абонентского номера получает доступ к управлению денежными средствами бывшего пользователя.

Интернет-покупки

При покупке товаров через Интернет пользуйтесь только проверенными сайтами. Однако и там могут действовать мошенники. Вас должна насторожить неоправданно низкая цена, а также требования о полной предоплате.

Ни при каких обстоятельствах не сообщайте по телефону неизвестным лицам свои личные данные, а тем более номера банковских карт. Тогда денежные средства останутся на вашем счету, а не пополнят кошельки мошенников!

Основные правила безопасности:

- Во избежание использования вашей карты другим лицом храните ПИН-код отдельно от карты, не пишите ПИН-код на карте, не сообщайте ПИН-код другим лицам (в том числе родственникам), не вводите ПИН-код при работе в сети Интернет.
- Пользуйтесь только защищенными банкоматами. Немедленно блокируйте карту при ее утере.
- Храните свою карту в недоступном для окружающих месте. Не передавайте карту другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, особенно в поездках.
- Требуйте проведения операций с картой только в вашем присутствии, не позволяйте уносить карту из поля вашего зрения.
- Если к вам обратились по телефону, в Интернете, через социальные сети или другими способами, и под различными предлогами пытаются узнать данные о

вашей банковской карте, пароли или другую персональную информацию, будьте осторожны: это явные признаки мошенничества. При любых сомнениях рекомендуем прекратить общение и обратиться в банк по телефону, указанному на обратной стороне вашей банковской карты.

- Для борьбы с вредоносными программами используйте антивирус.
- При смене телефонного номера не забывайте отключить услугу «мобильный банк».
- При покупке товаров через Интернет пользуйтесь только проверенными сайтами.

Старший помощник прокурора М.А.Морозова

«СОГЛАСЕН»

Прокурор района

советник юстиции Е.В.Карабатов