

О преступлениях, совершаемых с использованием информационно-коммуникационных технологий

Развитие технологий в современном мире обуславливает их проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели, в том числе личное обогащение.

Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, у физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа хищения предусмотрена ст.ст. 158, 159, 159.3, 159.6 УК РФ.

Данные деяния могут совершаться любым лицом, имеющим необходимые навыки работы, включая школьников и лиц, отбывающих наказание в местах лишения свободы.

Потерпевшим от данных преступлений может стать любой человек, имеющий банковский счет, привязанный к банковской карте.

Основные способы телефонного мошенничества:

- мошенник звонит или отправляет SMS/MMS-сообщение на мобильный телефон, представляется сотрудником банка или иной коммерческой организации, сообщает потерпевшему о начислении бонусов на банковский счет и просит сообщить пришедшие посредством SMS-сообщений персональные данные по банковскому счету, после чего получив соответствующие необходимые данные с банковского счета потерпевшего похищает денежные средства;

- мошенник звонит или отправляет SMS-сообщение на телефоны, сообщая информацию о том, что банковская карта или счет мобильного телефона заблокированы в результате преступного посягательства, а затем представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на сотовом телефоне или банкомате якобы для разблокировки, в результате чего денежные средства перечисляются на счет мошенника или его доверенного лица;

- поступает звонок от якобы сотрудника службы технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников;

- на сотовый телефон абонента приходит сообщение о том, что его банковская карта заблокирована и ему предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда владелец

карты звонит по указанному телефону, ему сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и пин-код для ее перерегистрации. Получив реквизиты банковской карты, злоумышленники переводят денежные средства на свой телефон, а затем снимают их со счета;

- мошенничество при покупке товаров через социальные сети, т.е. потерпевшие заказывают товар через сеть, оплачивают заказ путем перечисления денежных средств на банковскую карту продавца, но не получают заказ.

Чтобы не стать жертвами мошенников следует придерживаться следующих советов:

Не торопитесь сообщать реквизиты вашей карты. Ни одна организация, включая банк, не имеет право требовать данные вашей пластиковой карты. Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, вам ответят, что никаких сбоев на сервере не происходило, а ваша карта продолжает обслуживаться банком.

Если вам поступило предложение от радиостанции активировать карточки экспресс-оплаты с целью получения приза, включите радиостанцию и прослушайте ее эфир. Радиостанция никогда не требует активировать карточки экспресс-оплаты при проведении лотереи.

На мобильный телефон может прийти SMS-сообщение с предложением оградить вас от СПАМ-рассылки, либо принять участие в акции от вашего сотового оператора. В сообщении предлагается отправить «бесплатное» SMS-сообщение, состоящее из набора цифр, на один из коротких номеров, а затем перейти по ссылке. В результате этих манипуляций вы теряете деньги, но СПАМ все равно будете получать.

SMS-сообщения могут быть весьма разнообразны, и в данном случае совет может быть один - критически относиться к таким сообщениям и не спешить выполнить то, о чем вас просят. Лучше позвоните оператору связи, узнайте, какая сумма спишется с вашего счета при отправке SMS-сообщения или звонка на указанный номер, затем сообщите о пришедшей на ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

Также рекомендуется исключить факты покупки товаров через социальные сети на условиях предоплаты.

Распространены случаи обмана людей в интернете: от спама до создания сайтов-двойников. В этой связи необходимо пользоваться последними версиями браузеров и лицензионным антивирусным программным обеспечением, следить за тем, что бы при входе на сайты было установлено защищенное соединение <https>.

Будьте внимательны!!! В случае если вы стали жертвой мошенников следует незамедлительно сообщить об этом в правоохранительные органы, в первую очередь – в полицию.