ПАМЯТКА

Способы совершения мошенничеств с использованием дистанционных технологий

1. Телефонные мошенничества, при которых преступник использует сотовую (стационарную) связь, как средство совершения преступления, контактируя с потерпевшим лишь по телефону. Наиболее часто используются следующие способы:

- Проблема у родственника (знакомого) потерпевшего;
- Блокировка банковской карты (банковского счета) потерпевшего;
- Выигрыш приза потерпевшим;

2. Мошенничества в сети Интернет, при которых преступник использует различные информационные системы (сайты с объявлениями, социальные сети, форумы) как средство совершения преступления, контактируя с потерпевшим посредством электронной переписки. Наиболее часто используются следующие способы:

- продажа товаров через электронные объявления;
- продажа товаров через сайты, интернет магазины;
- мошенничество, вымогательство через социальные сети.

3. Неправомерный доступ к компьютерной информации, при котором преступники используют вредоносное программное обеспечение для получения доступа к денежным средствам на счетах банковских карт, сотовых телефонов. Наиболее часто используются следующие способы:

- через средства дистанционного банковского обслуживания (мобильный банк, интернет - банкинг);
- через компьютерную технику и сотовые телефоны потерпевших.

Действия преступника для случая «Проблема у родственника»:

1-2. Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) проблема (попал в ДТП, совершил преступление, иное) и предлагает разрешить проблему, но при этом необходимо заплатить определенную денежную сумму. Потерпевший соглашается и ждет человека, которому необходимо передать деньги.

3-4. Преступник звонит в такси и через оператора узнает номер таксиста.

5. Таксисту преступник сообщает, что ему необходимо подъехать к условленному адресу, где ему передадут деньги.

6-7. Таксист, прибыв на адрес, получает определенную денежную сумму.

8. Таксист, после того как получил деньги сообщает об этом преступнику.

9. Преступник сообщает таксисту номера телефонов, на которые необходимо перевести денежные средства, полученные от потерпевшего.

10. Таксист с помощью банкомата (терминала) осуществляет перевод денежных средств на номера телефонов, указанных ему преступником (телефонных номеров может быть несколько).

11. При поступлении денежных средств на различные номера телефонов, осуществляется их перевод на единый расчетный счет банка (пластиковой карты).

12-14. Подельник преступника, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или интернет) осуществляет перевод денежных средств преступнику.

Для данной схемы часто случается упрощенная вариация, при которой из схемы исключаются действия с таксистом, при этом платежные операции производятся потерпевшим самостоятельно (схема аналогична случаю с сообщениями о блокировке банковских карт):

1. Преступник осуществляет звонок на телефон (мобильный, стационарный) потерпевшего и сообщает о том, что у его родственника (знакомого) проблема (попал в ДТП, совершил преступление, иное) и предлагает разрешить проблему, но при этом необходимо заплатить определенную денежную сумму. Потерпевший соглашается, преступник указывает ему номера телефонов, банковских карт и т. п., на которые необходимо зачислить деньги.

3. Потерпевший с помощью банкомата (терминала) осуществляет перевод денежных средств на номера телефонов, указанных ему преступником (телефонных номеров может быть несколько).

4. При поступлении денежных средств на различные номера телефонов, осуществляется их перевод на единый расчетный счет банка (пластиковой карты).

5. Подельник преступника, осуществивший снятие денежных средств с расчетного счета, используя банкомат (терминал или интернет) осуществляет перевод денежных средств преступнику.

Действия преступника «Ваша карта заблокирована»:

1-2. Преступник осуществляет звонок на телефон (отправляет СМС-сообщение), потерпевшего и сообщает о том, что «Ваша карта заблокирована» (или о иной проблеме со счетом, пластиковой картой). Для того чтобы решить проблему необходимо в короткий срок оказаться рядом с банкоматом и осуществить ряд операций, которые будет диктовать преступник.

3. Потерпевший, дойдя до банкомата, созванивается с преступником и выполняет все его действия.

4. Преступник сообщает потерпевшему набор цифр для устранения проблем с картой (счетом).

5. При поступлении денежных средств на различные номера телефонов, осуществляется их перевод на единый расчетный счет банка (пластиковой карты).

6-8. Подельник преступника, осуществивший снятие денежных средств с расчетного счета, использует банкомат (терминал или интернет) осуществляет перевод денежных средств преступнику.

Действия для случаев, когда предлогом мошенничества является выигрыш приза потерпевшим, оказание медицинских услуг и т. п. аналогичны вышеизложенным.

Мошенничества в сети Интернет

При осуществлении мошенничества в сети Интернет преступления в основном совершаются под предлогами реализации потерпевшим различных товаров, при которых преступники делают якобы выгодные предложения, обещают бесплатную доставку, сниженные цены и т. п. Потерпевшими становятся в основном лица, которые ранее приобретали какие-либо товары и услуги через Интернет и доверяют этому способу реализации, сайтам с объявлениями и т. п.

Действия преступника при мошенничестве через электронные объявления:

1. Преступник размещает на сайте электронных объявлений (Из Рук в Руки, Авито или иных) объявление о продаже каких-либо товаров, для связи указывает телефон либо электронную почту.

2. Потерпевший обнаруживает объявление и решает приобрести заявленные в нем товары.

3. Потерпевший созванивается с преступником по указанному в объявлении абонентскому номеру сотовой связи, преступник сообщает ему, что товар имеется в наличии и он готов его продать. Показать товар преступник под разными предлогами отказывается, сообщает что находится в другом городе (субъекте РФ), и предлагает переслать фото товара на электронную почту.

4. Преступник сообщает потерпевшему адрес электронной почты для связи либо узнает у потерпевшего адрес его электронной почты.

5-6. Преступник и потерпевший некоторое время ведут электронную переписку, при этом преступник как правило демонстрирует потерпевшему фотографии товара, возможно направляет сканированную копию «своего» паспорта и заверяет в надежности. Оговаривается цена товара, способ оплаты и сроки поставки.

7. Потерпевший перечисляет денежные средства на указанный ему банковский счет, карту, электронный кошелек, мелкие суммы на счет абонентского номера.

8. Преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т. п.

9-10. Преступник, либо его сообщники обналичивают собранные денежные средства.

Действия преступника при мошенничестве через Интернет-магазины:

1. Преступник создает в сети Интернет сайт в виде магазина для продажи различных товаров, указывает значительный ассортимент, невысокие цены и т.п. для привлечения клиентов.

2. Потерпевший обнаруживает сайт и решает заказать какой-либо товар, регистрируется на сайте, указывает свои данные, оформляет доставку.

3. Потерпевший получает от магазина электронные письма с подтверждением заказа, ему высылается счет на оплату либо указываются реквизиты банка, электронной платежной системы для платежа.

4. В некоторых случаях потерпевший звонит на указанные на сайте либо в электронных письмах номера, где преступник либо его сообщники заверяют потерпевшего в том, что заказ принят, оговаривают сроки поставки и т.п., создавая у потерпевшего впечатление о реальности и честности магазина.

6. Потерпевший оплачивает выставленный ему счет, перечисляет денежные средства на указанный ему банковский счет, карту, электронный кошелек.

7. Преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т. п.

8. Преступник, либо его сообщники обналичивают собранные денежные средства, после чего прекращается всякое взаимодействие с потерпевшим.

9. Некоторое время после перечисления потерпевшим денежных средств, с целью сокрытия следов своей деятельности преступники отвечают потерпевшему на его звонки, электронные письма, под рядом предлогов откладывая поставку товара.

При осуществлении мошенничества в социальных сетях схема преступной деятельности аналогична для случаев с мошенничеством через электронные объявления или Интернет-магазины, с той разницей, что преступники размещают предложения о продаже товаров в тематических группах и иным способом в социальных сетях.

Действия преступника при мошенничестве в социальных сетях

1. Преступник создает в социальной сети (Одноклассники, В Контакте) тематические группы либо объявления о продаже различных товаров, указывает значительный ассортимент, невысокие цены и т.п. для привлечения клиентов. Социальные сети допускают публикацию изображений и видеоматериалов, отражающих свойства товаров.

2. Потерпевший обнаруживает объявления и решает приобрести товар, для чего вступает с преступником в электронную переписку посредством системы обмена сообщениями в социальной сети.

3. Потерпевший ведет с преступником электронную переписку, по достижению договоренности о покупке ему высылается счет на оплату либо указываются реквизиты банка, электронной платежной системы для платежа.

4. В некоторых случаях потерпевший звонит на указанные в объявлении телефоны, где преступник либо его сообщники заверяют потерпевшего в том, что заказ принят, оговаривают сроки поставки и т.п., создавая у потерпевшего впечатление о реальности и честности продавца.

6. Потерпевший оплачивает выставленный ему счет, перечисляет денежные средства на указанный ему банковский счет, карту, электронный кошелек.

7. Преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т. п.

8. Преступник либо его сообщники обналичивают собранные денежные средства, после чего прекращается всякое взаимодействие с потерпевшим.

9. Некоторое время после перечисления потерпевшим денежных средств, с целью сокрытия следов своей деятельности преступники отвечают потерпевшему на его звонки, электронные письма, под рядом предлогов откладывая поставку товара.

Действия преступника при использовании вредоносных программ:

1. Преступники размещают в сети Интернет вредоносное программное обеспечение, которое распространяется через различные сайты, электронную почту и т. п., либо под видом различных программ, объявлений для современных абонентских устройств сотовой связи.

2 - 3. Потерпевшие, используя сеть Интернет, заражают свою компьютерную технику вредоносным программным обеспечением.

4. Вредоносные программы устанавливаются на компьютерной технике потерпевших.

5 - 6. Преступник через вредоносное программное обеспечение путем операций вручную или автоматизированных получает доступ к компьютерной технике потерпевшего, при этом:

- происходит хищение денежных средств с банковских карт, счетов потерпевшего (если на компьютерной технике использовались системы дистанционного банковского обслуживания);
- происходит хищение денежных средств со счетов электронных платежных систем, используемых потерпевшим;
- происходит хищение денежных средств с абонентского номера сотовой связи потерпевшего (при заражении современных абонентских устройств сотовой связи, смартфонов);

7. Преступник переводит похищенные денежные средства на используемые им банковские счета, карты, электронные платежные системы, счета сотовых телефонов.

8. Преступник собирает денежные средства с промежуточных платежных средств на какой-либо банковский счет, карту и т. п.

9 - 10. Преступник, либо его сообщники обналичивают собранные денежные средства.

11. Преступники с целью сокрытия следов своей деятельности могут уничтожить следы вредоносного программного обеспечения на компьютерной технике (телефоне) потерпевшего.