Хищения средств в интернете проходят по нескольким сценариям:

Онлайн банкинг

С помощью сайтов-зеркал (копий настоящих сайтов банков) или вредоносного ПО мошенники получают доступ к личному кабинету клиента.
Также мошенники совершают звонки, представляясь сотрудниками банка и запрашивая у клиента его идентификационные данные.

Мобильный банкинг

На мобильное устройство пользователя загружается вредоносное ПО, с помощью которого мошенники могут посредством SMS списывать деньги с банковского счета без ведома его законного владельца.

Онлайн шоппинг

При совершении покупок в онлайн-магазинах злоумышленники получают данные карты, в том числе и CVV/ CVC-код.
Другой вид обмана реализуется, когда хотят что-то купить у пострадавшего: мошенник переводит на его счет бОльшую сумму, а затем требует вернуть ему разницу. После возвращения переплаченной суммы, мошенник отзывает свой первоначальный платеж.

Информация о наиболее распространенных видах мошенничества с использованием средств связи и сети Интернет

На сегодняшний день основной проблемой при раскрытии мошенничеств, совершенных с помощью средств сотовой сети, является установление лиц, непосредственно занимающихся мошенничеством. Анализ показал, что в большинстве случаев телефонные мошенники находятся в других регионах Российской Федерации, многие из них уже отбывают наказание в исправительных учреждениях ФСИН. Сим-карты поступающие в исправительные учреждения нелегально, и как правило, зарегистрированы на несуществующих лиц.

Существуют следующие способы совершения преступлений, с использованием средств связи и сети Интернет:

1. Взлом личных страниц в социальных сетях;

Пример: Неустановленное лицо, взломав страницу в социальной сети «ВКонтакте», гражданина «А» т от его имени осуществило переписку с гражданской «М» в ходе которой попросило перевести ему на счёт карты №Х, денежные средства в сумме 5 400 рублей, которые гражданка «М» перевела с помощью услуги «Сбербанк онлайн» 5 400 рублей на указанный счёт карты.

2. Преумножение имеющихся накоплений (получение выигрыша);

Пример: на абонентский номер гражданина «Х» позвонил неизвестный мужчина и предложил заработать, а именно вкладывать денежные средства на счет, на что гражданин «Х» согласился. Поле чего, через «Сбербанк Онлайн» гражданин «Х»начал пополнять банковские счета. Таким образом ущерб оставил 1 406 658 рублей.

3. Компенсация за приобретенные БАДЫ;

Пример: Позвонил неизвестный мужчина, который представился следователем по особо важным делам следственного комитета города Москвы и сообщил, что за ранее приобретенные гражданкой «П» лекарственные препараты ей полагается компенсация, так как они оказались фальсифицированными, но для ее получения необходимо перевести комиссию. Гражданка «П» через отделение ПАО «Сбербанк России», по платежной системе «Колибри», перевела денежные средства в сумме 362 000 рублей.

4. Оформление кредита через Интернет;

Пример: В сети Интернет гражданка разместила заявку в различные банки на получение кредита в сумме 100 000 рублей. На ее абонентский номер телефона позвонила неизвестная женщина, которая представилась сотрудником «Инвест-Банка» и сообщила, что кредит одобрен и для получения кредита необходимо перевести на банковскую карту №XXX комиссию, на что гражданка согласилась и через «Сбербанк Онлайн» со своей банковской карты перевела денежные средства в сумме 20 450 рублей.

5. Покупка товара через сети Интернет;

Пример: В сети интернет гражданка «Х» заказала сотовый телефон стоимостью 13 490 рублей. В этот е день, на сотовый телефон, принадлежащий гражданке «Х» пришло СМС сообщение с засекреченного абонентского номера, в котором был указан трек номер заказа, согласно которому почтовое отправление было отправлено по адресу. Гражданка «Х» на почтовом отделении оплатила полную стоимость посылки с доставкой в сумме 14 250 рублей. При вскрытии посылки гражданка обнаружила дешевый мобильный телефон иной более дешевой марки.

Пример: Гражданин «В» на интернет сайте «Авто.Ру» нашел объявление о продаже автомобиля ГАЗ 3307. Позвонив на указанный в объявлении номер ответил молодой человек, который сказал, что нужно произвести предоплату за машину. Гражданин «В» произвел предоплату на банковскую карту в размере 83 000 рублей.

6. Покупка авиа и ж/жд билетов (путёвки);

Пример: Гражданка «В» в сети «Интернет» на сайте «Авиатрэел» осуществила заказ 4 авиабилетов «Салехард-Краснодар» и обратно, в дальнейшем перейдя по ссылке, полученной посредством электронной почты совершила оплату покупки билетов, после чего с банковской карты, принадлежащей гражданке «В» произошло списание денежных средств в размере 39 418 рублей. Купленные билеты гражданке «В» не поступили.

7. Сообщили преступнику номер банковской карты.

Пример: Гражданке «Г» поступил входящий звонок, в ходе которого неустановленный мужчина представился сотрудником служб безопасности Сбербанка России и сообщил, что с ее банковской карты произошло списание денежных средств, осуществленное мошенниками, затем передал телефон другому мужчине, который подтвердил, что в отношении гражданки действительно действовали мошенники и стал задавать вопросы в ходе которых гражданка сообщила данные банковской карты на которой находились денежные средства. Впоследствии произошло списание денежных средств.

Рекомендации гражданам:
Как не стать жертвой мошенников, покупая товары в интернете

Особенностью розничных интернет-продаж является то, что у покупателя отсутствует возможность непосредственного ознакомления с товаром в момент принятия решения о покупке. Такая схема торговли определена ст. 497 ГК РФ. Отношения же с покупателями интернет-магазина регулируются Постановлением Правительства РФ от 27 сентября 2007 г. № 612 «Об утверждении правил продажи товаров дистанционным способом» и ст. 26.1 закона РФ «О защите прав потребителей».

Для того, чтобы радость онлайн-покупок не была омрачена получением некачественного товара или потерей денег мы рекомендуем вам **обратить внимание на некоторые признаки потенциально опасных Интернет-магазинов.**

1. Низкая цена. Если вы нашли объявление или магазин, предлагающий товары по ценам существенно ниже рыночных, имейте в виду, что мошенники часто используют данный прием для привлечения жертв.

На что следует обратить внимание? Посмотрите стоимость аналогичных товаров в других Интернет-магазинах, она не должна отличаться слишком сильно. Не поддавайтесь на слова «акция», «количество ограничено», «спешите купить», «реализация таможенного конфиската», «голландский аукцион».

2. Требование предоплаты. Если продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица, нужно понимать, что данная сделка является опасной.

На что следует обратить внимание? Учитывайте риски при совершении Интернет-покупок. Помните о том, что при переводе денег в счет предоплаты вы не имеете никаких гарантий их возврата или получения товара. Если вы решили совершить покупку по предоплате, проверьте рейтинги продавца в платежных системах.

3. Отсутствие возможности курьерской доставки и самовывоза товара. Данные факторы вынуждают покупателей пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

На что следует обратить внимание? Выбирая из нескольких магазинов, следует отдать предпочтение тому, в котором есть возможность забрать товар самостоятельно. Злоумышленники могут предоставить поддельные квитанции об отправке товара транспортной компанией.

4. Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном, такой магазин может представлять опасность.

На что следует обратить внимание? Внимательно изучите сведения о продавце. Помните о том, что вы собираетесь доверить деньги лицу или компании, о которой вы ничего не знаете. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем другие организации. Проверьте отзывы о магазине в открытых Интернет-рейтингах, пролистайте отзывы как можно дальше, злоумышленники могут прятать негативные отзывы за десятками фальшивых положительных оценок. В случае совершения покупок посредством электронных досок объявлений посмотрите историю сделок продавца и ознакомьтесь с его рейтингом, многие торговые площадки предлагают подобную услугу.

5. Отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной.

На что следует обратить внимание? Создание Интернет-магазина - дело нескольких часов, изменение его названия и переезд на другой адрес - дело нескольких минут. Будьте осторожны при совершении покупок в только что открывшихся Интернет-магазинах.

6. Неточности или несоответствия в описании товаров. Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению.

На что следует обратить внимание? Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

7. Излишняя настойчивость продавцов и менеджеров. Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия.

На что следует обратить внимание? Злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все нюансы

сделки. Тщательно проверяйте платежную информацию и при наличии любых сомнений откладывайте сделку.

8. Подтверждение личности продавца путем направления отсканированного изображения паспорта. Ожидая перевода денег, продавцы в социальных сетях часто направляют изображение своего паспорта покупателю с целью подкупить его доверие.

На что следует обратить внимание? Помните, что при современном развитии техники изготовить изображение паспорта на компьютере не представляет никакого труда. Данное изображение никаким образом не может подтверждать личность лица, направившего его вам.

ВЫВОД: Если Интернет-магазин или объявление соответствуют хотя бы одному из указанных признаков, это серьезный повод задуматься о целесообразности совершения сделки.