В настоящее время с развитием информационных технологий в обществе и государстве, растет и количество преступлений, связанных с Интернетом и средствами связи.

Все виды мошенничеств в этой сфере условно подразделяются на **контактные и бесконтактные.** Контактные предполагают непосредственное личное общение злоумышленника со своей «жертвой». Бесконтактные же мошенничества происходят с помощью телефонной связи либо Интернета, при этом «жертва» не видит преступника.

**Виды контактного мошенничества:**

**Гадание и снятие порчи.**

На улице к вам подходит женщина и начинает гадать, предсказывать будущее. Потом выясняется, что на человека навели порчу и гадалка предлагает ее снять.  После «снятия порчи» у человека не остается ни денег, ни золотых украшений.

***Социальные работники.***

Следующий вид контактного мошенничества можно назвать «социальные работники». Эти мошенники ходят по домам и квартирам под видом социальных работников либо работников газовых служб. И вариаций здесь очень много. Кто-то говорит о замене газового оборудования, кто-то о выплате пенсий и социальных пособий, а кто-то – о замене старых денежных купюр. Их цель одна – проникнуть в квартиру, заболтать хозяина и похитить деньги.

**Бесконтактные мошенничества** делятся на два вида:

**- интернет-мошенничества**

**- телефонные мошенничества.**

Интернет – простор для злоумышленников, поэтому интернет-мошенничество получило широкое распространение.

**Сайты-двойники (или фишинговые сайты).**

Мошенники создают сайт-двойник официального сайта, на котором совершаются онлайн-покупки. При этом потерпевший оплачивает услугу и переводит деньги на счет преступников. Так, например, часто происходит при заказе страхового полиса на сайте страховой компании. Не убедившись в подлинности сайта, посетители заказывают страховку, в результате чего деньги перечисляются на счет мошенников, а поддельный сайт удаляется.

**Покупка товаров в социальных сетях.**

 Многие предпочитают покупать товары в интернете через аккаунты социальных сетей – кто-то из граждан вносит только предоплату, а кто-то, увидев привлекательную цену, в счет оплаты за приобретаемый товар полностью переводит сумму на банковские карты незнакомцев. Итог один – пострадавшая сторона остается и без товара, и без денег. После перечисления задатка «продавец» исчезает вместе с деньгами и удаляет аккаунт из социальных сетей.

Сотовая связь уже давно перестала быть роскошью, а стала общедоступным средством видов телефонного мошенничества. Однако указанные виды не носят исчерпывающий характер и могут изменяться.

**Случаи с родственниками.**

Мошенник представляется родственником или знакомым и взволнованным голосом сообщает о том, что задержан за совершение того или иного преступления или правонарушения (ДТП, хранение наркотиков, нанесение побоев). Избежать проблем предлагается путём перечисления денежных средств на банковскую карту, например, для того, чтобы оплатить услуги адвоката. При этом, чтобы не дать возможности гражданину выяснить у родственника действительно ли с ним произошло то, что указали мошенники, последние будут вести беседу с потерпевшим до той минуты, пока не получат деньги.

**Покупка и продажа товаров.**

Мошенниками на различных сайтах размещается информация о продаже автомобиля либо ещё чего-то по заниженной цене.  Подробно описывается товар, выкладываются фотографии, указывается цена. Потенциальный покупатель звонит продавцу, где последний предлагает внести предоплату, тогда необходимый товар гарантированно станет его. Деньги злоумышленники просят перечислить переводом через банк либо на абонентский номер телефона. Как правило, многие граждане переводят не только задаток, но и сразу всю сумму за товар. Получив деньги, мошенники отключают телефоны и на связь с обманутым покупателем больше не выходят. Впрочем, рискует не только тот, кто покупает, но и продает. Мошенники могут использовать чужие объявления о продаже. Звонят и говорят, что покупают товар. Однако деньги могут перевести только на банковскую карту, так им удобнее, и они уверены, что товар не продадут. Доверчивые граждане называют данные своих карт для перевода денег. Заполучив нужные реквизиты, злоумышленники снимают все деньги с банковских счетов добропорядочных граждан.

**Сотрудники банков и сотовых операторов.**

Злоумышленник представляется сотрудником безопасности банка, сообщает о сбое в системе или о мошенниках, которые хотят похитить деньги со счетов. Просят назвать реквизиты карт, секретный код, который приходит в смс-оповещениях, либо просят гражданина пройти до ближайшего терминала или банкомата и произвести действия с картой, которые они будут диктовать. В результате у человека списываются все денежные средства со счетов.

Также может поступить звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи. Он может предложить подключить новую услугу или наоборот ее отключить, а также вернуть излишне потраченные денежные средства за пользование сотовой связью. Для этого предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

     Следует отметить, что это далеко не полный перечень мошеннических схем отъёма денег у населения. Злоумышленники находят все новые и новые способы для достижения своих преступных замыслов.

Чтобы не стать жертвой злоумышленников, необходимо соблюдать простые правила безопасного поведения и обязательно довести их до сведения родных и близких:

1. Не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Необходимо прервать разговор и попытаться связаться с тем родственником, который якобы попал в беду. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом;

2. Не доверяйте незнакомым и малознакомым людям, а также подозрительным звонкам и смс - сообщениям. Следует помнить: не стоит впускать в свой дом незнакомца, даже если он представился сотрудником социальной службы или государственной структуры. Попросите его предъявить удостоверение. Не стесняйтесь тут же, не пуская посетителя в дом, проверить данные по телефону. Если не можете сделать это сами, попросите родственников или соседей. В случае, если возникли сомнения, немедленно звоните в полицию;

3. При получении SMS с неизвестных номеров с просьбой положить на счет деньги, якобы ошибочно зачисленные на Ваш счет, или с сообщением о крупном денежном выигрыше и предложением отправить SMS-сообщение или позвонить по указанному номеру для получения приза, не делайте этого. Получив подозрительное смс-сообщение, немедленно удалите его и ни в коем случае не перезванивайте по указанному номеру. Помните, что, вступив в разговор с мошенниками, которые представляются сотрудниками банков и сотовых операторов, и выполнив любые действия по карте, вы лишитесь своих сбережений. Обратитесь лично к сотрудникам в офис вашего банка или же в офис вашей сотовой связи. Никому не сообщайте пин-код и реквизиты вашей банковской карты. Помните, что ни один банк самостоятельно не блокирует карту – сделать это можете только вы. Сообщения о блокировании карты присылают мошенники.

4. Не перечисляйте предоплату или полностью сумму за товар «продавцу». Все операции по купле-продаже необходимо проводить лично и только после того, как ознакомитесь с документами на приобретаемый товар и лично увидите то, что вам продают.

5. Не совершайте по просьбе незнакомых лиц операции по карте, а также не производите никаких манипуляций посредством платежного терминала (банкомата). В результате таких действий мошенники получают исчерпывающую информацию о счетах и переводят ваши денежные средства на свои банковские карты.



**Прокуратура Белгородской**

**области**

**Прокуратура Волоконовского района**

**ПАМЯТКА**

**ГРАЖДАНАМ ПО СОБЛЮДЕНИЮ «КОМПЬЮТЕРНОЙ ГИГИЕНЫ»**

**Волоконовка**

**2022**