**Осторожно, мошенники!**

На протяжении уже нескольких лет на территории Архангельской области увеличивается количество уголовных дел, связанных с хищением денежных средств при помощи информационно-телекоммуникационных технологий, то есть при помощи средств мобильной связи или интернет ресурсов.

Не смотря на принимаемые меры профилактического характера оперативная обстановка остается сложной.

В 2020 году в Онежском районе зарегистрировано 82 (в 2019 - 70) преступления в сфере IT-технологий.

В 2021 году уже зарегистрировано 32 преступления в сфере IT-технологий.

Личность мошенника значительно отличается от личности других преступников, в большинстве своем мошенники обладают хитрым, изворотливым умом, актерскими способностями, ими используются любые возможные способы обмана или злоупотребления доверием простых граждан. Они стремятся внушить своим потенциальным жертвам чувство полного доверия и лишь после этого приступают к непосредственному обману.

**Что может быть орудием преступления в руках мошенников?**

Сейчас у граждан в пользовании находятся смартфоны, планшеты, ноутбуки, которые подключены к сети интернет и в которых установлены онлайн приложения различных банков, которые позволяют осуществлять переводы денежных средств с карты на карту. Зачастую граждане не перезванивают своим близких и знакомым и переводят денежные средства не убедивших в правильности своих действий.

**Телефон (**Телефонное мошенничество). В руках мошенников простой мобильный телефон является орудием (средством) совершения преступления. Их цель завладеть денежными средствами. Так мошенники звонят на стационарные или мобильные телефоны потерпевших, представляются их знакомыми, родственниками, сотрудниками правоохранительных органов, сотрудниками службы безопасности банка и путем обмана вымогают денежные средства. Одной из причин совершения данных преступлений, является то, что мошенники застают граждан врасплох не давая им времени и возможности справиться с переживанием и успокоится, подумать и созвониться со своими родственниками. С этой целью злоумышленники постоянно находятся на связи со своей «жертвой», отвлекая ее различными разговорами и советами внушая чувство полного доверия.

**Хищение денежных средств с банковских карт**. На сотовый телефон абонента приходит сообщение о том, что его банковская карта заблокирована либо заявка на перевод определенной денежной суммы полу­чена, 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, которые приходят в смс сообщении якобы для ее регистрации. Получив реквизиты пластиковой карты, злоумышленники переводят денежные средства на номер своего телефона. Либо под предлогом разблокирования банковской карты «подводят» потер­певшего к банкомату и под видом введения «кода» (абонентских номеров злоумышленников) перечисляют денежные средства потерпевших на ука­занные абонентские номера.

В это время мошенники постоянно находятся на связи с гражданином, не дают ему опомнится, позвонить близким.

**Розыгрыш призов и предоставления кредитов на выгодных условиях.** В этом случае мошенник звонит на мобильный телефон абонента представляется ведущим популярной радиостанции, поздравляет его с крупным выигрышем (телефон, ноутбук, автомобиль) в лотерее, организованной радиостанцией, также представляются сотрудником банка и говорят, что заявителю предложен кредит на очень выгодных условиях. Затем сообщает, что для того, чтобы получить приз необходимо в течение минуты дозвониться на радиостанцию по указанному номеру. Перезвонившему абоненту отвечает сотрудник «призового отдела» «банка» и подробно объясняет условия игры (кредита): просит представиться и назвать год рождения, грамотно убеждает в честности акции (никаких взносов, переигровок) и предлагает перечислить 13% от стоимости приза на абонент­ский номер путем использования систем оплаты «Киви-кошелек» или «Мо­бильный кошелек». Затем мошенник объясняет, что при поступлении пла­тежа на указанный номер, призовой отдел присваивает ему персональный номер «победителя», с которым гражданин должен ехать за призом, либо приз будет выслан ему по почте.

**Взлом страниц в социальных сетях**

Вы находитесь в социальной сети, вдруг от Вашего знакомого Вам приходит сообщение с целью одолжить ему денег либо оказать иную финансовую помощь. Не нужно без оглядки переводить свои денежные средства, перезвоните знакомому либо его родным и близким и уточните ситуацию.

Вы находитесь в социальной сети, вдруг от Вашего знакомого Вам приходит сообщение с вопросом, не получили ли Вы положенную Вам от государства выплату, после чего предлагают помощь в ее получении, для чего нужно передать данные своей банковской карты и коды в поступившх СМС-сообщениях. Опять же перезвоните и уточните ситуацию и ни в коем случае не передавайте никому данные, поступившие Вам в СМС-сообщении.

**Вымышленные кредиты**

Вам звонят и говорят, что кто-то пытается от Вашего имени взять в банке кредит, и чтобы этого избежать, необходимо реально оформить на себя онлайн-кредит, после чего снять полученные денежные средства и перевести на указанный счет, якобы для их сохранности и во избежание взятия кредита от Вашего имени посторонним лицом.

**Мнимая атака**

Вам звонят и говорят, что кто-то пытается с Вашего банковского счета снять денежные средства, и чтобы этого избежать, необходимо снять со счета все свои денежные средства и перевести их на защищенный счет, якобы для их сохранности.

Все это обман, банк никогда не звонит своим клиентам по подобным поводам, никогда не уточняет у своих клиентов их личные данные либо данные об их банковских счетах и картах, максимум, почему может позвонить банк, это чтобы уточнить, клиент ли выполняет некую операцию, которая для банка кажется подозрительной, чтобы при необходимости заблокировать ее.

**ОМВД России по Онежскому району в очередной раз призывает граждан быть бдительными и обратить внимание на следующее:**

**-** При получении сообщений от своих знакомых, родственников с просьбой перевести им денежные средства, или о возможности получения денежных выплат в первую очередь созвонитесь и убедитесь, что именно **Ваш знакомый просит о помощи**.

**-** При вводе личной информации (в особенности данные электронной почты, абонентские номера, ФИО, банковские реквизиты) либо намерении совершить покупку, заранее проверьте дату создания сайта, используя бесплатные Whois-сервисы (например 2ip.ru), где по адресу сайта можно установить информацию о владельце домена и дату его регистрации (сайты размещенные мошенниками и сайты-фальшивки имеют как правило небольшой «возраст»)

**-** С недоверием относитесь к ссылкам в публикациях, посвященным скидкам, а также не переходите по ссылкам, обещающим денежное вознаграждение за совершение простейших действий, связанных с совершением звонков, направлением смс-сообщений, вводом персональных данных, перечислением денежных средств с обещанием их преумножить.

**-** Никому и никогда, ни при каких обстоятельствах не сообщайте код подтверждения операции по переводу денежных средств, поступивший в смс-сообщении, так как **никакая организация не станет просить Вас сообщить данный код** **– это мошенники.**

**-** Если звонивший, представился представителем банка**, ни в коем случае не сообщайте информацию о Вашей карте или счете, обратитесь в ближайшее отделение банка.**

**ОМВД России по Онежскому району**