ПЛАН – КОНСПЕКТ
информационных выступлений перед гражданами и трудовыми коллективами

ОМВД России по Коношскому району сообщает, что в 2022 году участились случаи совершения мошеннических действий с использованием мобильных средств связи, информационных технологий и сети «Интернет».

В последнее время на территории района распространены два вида мошенничества:

Звонки и СМС из банка

Вам звонит неизвестное лицо, и представляется оператором или сотрудником службы безопасности банка и сообщает о том, что ваша карта заблокирована, либо были совершены попытки снятия денежных средств. При этом мошенники могут обратиться к вам по имени и отчеству, а также назвать иные ваши личные данные, полученные ими из различных источников. Чтобы исправить ситуацию, и под предлогом уточнения информации злоумышленники выясняют данные карты, трёхзначный код безопасности, просят сообщить пароли, пришедшие в СМС-сообщении, или вынуждают жертву подойти к банкомату, набрать комбинацию клавиш и совершить тем самым операцию по переводу средств.

Объявление о покупке (продаже) товара

На страницах распространенных сайтов в сети Интернет («Авито», «Вконтакте» и т.д.) размещаются заведомо ложные объявления о продаже различных товаров, после того как преступники получают задаток за обещанный товар, либо стопроцентную предоплату по переводу на неизвестный номер счёта, либо на счет сотового телефона, они прерывают связь с покупателями, не предоставив товар.

В иных случаях, когда гражданин подал объявление о продаже товара на одном из сайтов в сети Интернет («Авито», «Вконтакте» и т.д.), мошенники осуществляют звонки на указанный им номер телефона, и предлагают предоплату за товар, так как хотят данный товар приобрести, но не могут незамедлительно его забрать. В этом случае, преступники просят потенциальную жертву назвать данные его банковской карты для перечисления предоплаты за товар, тем самым получают доступ ко всем сведениям банковского счета. После этого, происходит хищение денежных средств.

Отличие мошенничества от других видов хищений заключается в том, что потерпевшая сторона, введенная преступником в заблуждение, добровольно и сознательно передает последнему имеющиеся денежные средства в надежде получить материальную выгоду или избежать нежелательных последствий. Мошенничество совершается всегда открыто для потерпевшего, но связано с введением его в заблуждение относительно тех или иных фактических обстоятельств. При этом обман обнаруживается, как правило, не сразу, а через период времени, позволяющий не только полностью завладеть имуществом, но и скрыть какие-то важные обстоятельства.

Игнорируйте SMS сообщение от неизвестных вам абонентов с просьбой перезвонить на данный абонентский номер. С Вашего счета может быть автоматически снята значительная сумма денег.

Проведите беседу с детьми о том, чтобы они не вели телефонных разговоров с незнакомыми людьми, не называли персональных данных и адреса проживания неизвестным лицам.

Получив сообщение о блокировании банковской карты, не звоните на номера указанные с смс-сообщении, а свяжитесь с банком по телефону «горячей линии» как правило, он указан на оборотной стороне банковской карты. При разговоре с «операторами» не называйте пароль карты, ее реквизиты, свои персональные данные: **вся необходимая информация у банковских работников имеется и она сообщается при открытии счета**.

Убедительно просим вас быть бдительными и остерегаться общения, либо переписки с незнакомыми вам абонентами, а также посещения сайтов по сомнительным интернет-адресам и ссылкам.

Памятка по профилактике дистанционных мошенничеств и хищений денежных средств со счетов граждан

Дистанционное мошенничество, преимущественно, совершается следующими способами:

1. Потерпевшие под различными предлогами перечисляют денежные средства мошенникам.

2. Потерпевшие сообщают мошенникам реквизиты и пароли доступа к операциям по счету посредством поступившего им СМС-сообщения, что приводит к хищению денежных средств.

Участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Для разблокировки карты, абонента просят позвонить или отправить смс на короткий номер

Мошенники выступают в роли «сотрудников службы безопасности банков» и в ходе телефонного разговора получают информацию по банковской карте (номер банковской карты, а также CV-код).

Дальнейшим шагом является получение злоумышленниками разового пароля (в виде СМС-сообщения), который поступает на абонентский номер, привязанный к банковской карте. Держатель банковской карты сообщает разовый пароль мошенникам, тем самым предоставляет доступ к денежным средствам.

Уважаемые граждане, в целях пресечения и противодействия преступных намерений и действий мошенников, информируем Вас о том, что ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и карт, тем более пароли от них.

Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов или продажи товара от частных лиц. При заказе товаров вас попросят внести предоплату, а потом продавец бесследно исчезает, либо присылает некачественный товар.

Если вы хотите купить товар по предоплате, поищите информацию о магазине либо продавце в сети Интернет, посмотрите, как долго он находится на рынке. При необходимости свяжитесь с администратором магазина и уточните информацию о юридическом лице, проверьте ее, используя общедоступные базы данных налоговых органов и реестр юридических лиц.

Следующий вид мошенничества - просьба в предоставлении денежных средств родственнику или знакомому, чаще всего через социальные сети, доступ к которым взламывается злоумышленниками. Мошенники могут представляться сотрудниками правоохранительных органов, знакомыми и даже вашими родственниками. Обязательно свяжитесь с теми, от чьего имени действуют незнакомцы, и убедитесь в правдивости информации.

Значительную распространённость имеют преступления, совершенные с использованием высоких технологий, то есть в сети Интернет, в том числе объявления о продаже и рассылка вирусных ссылок в социальных сетях. Перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Рекомендации гражданам:

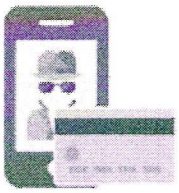
1. Не диктовать пароли из смс-сообщений.

2. При поступлении подобного рода звонка, незамедлительно завершить разговор, и перезвонить по официальному телефону банка.

3. Не перечислять денежные средства по просьбам родственников и знакомых, полученных через социальные сети в личных сообщениях. Обязательно свяжитесь с теми, от чьего имени получены сообщения, и убедитесь в правдивости информации.

4. Никому не сообщать ПИН-код, CVC или CVV коды банковской карты.

5. В случае утери телефона незамедлительно сообщите в банк о приостановлении (блокировке) имеющихся на счетах сбережений.



КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей
- Задайте звонящему вопросы личного характера, помогающие отличить близкого Вам человека от мошенника
- Под любым предлогом постарайтесь прервать контакт с собеседником, перезвоните родным и узнайте, все ли у них в порядке

Вам позвонили/прислали SMS «из банка» с неизвестного номера

- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка
- Незамедлительно обратитесь в правоохранительные органы

Вам прислали MMS или ссылку с неизвестного номера

- Не открывайте вложенные файлы, не переходите по ссылкам, удалите подозрительное сообщение
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков
- Защитите свой телефон, подключите БЕСПЛАТНУЮ услугу «Стоп-контент»

Вы заподозрили интернет-продавца в недобросовестности

- Необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки
- Встречаться с продавцом в общественном месте, так как это наиболее безопасный и гарантированный способ покупки. Следует передавать деньги продавцу лично в руки сразу после получения товара
- Никогда не переводить незнакомым лицам деньги в качестве предоплаты

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

УМВД России по Архангельской области предупреждает!
Виды телефонного и интернет-мошенничества и способы защиты от них.

1. Сотрудники банков или правоохранительных органов никогда не звонят гражданам с сообщениями о проблемах с банковским счетом или попытках незаконного оформления кредита. Не предлагают перевести деньги на «безопасный» счет. Любой подобный звонок, даже если он поступает якобы с официального номера организации – дело рук мошенников!

2. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного банка, трехзначный код на обороте карты, коды из СМС. Не переходите по ссылкам в сообщениях, которые пришли от незнакомых людей по электронной почте, в соцсетях или СМС.

3. Совершая покупки в интернет-магазинах или на сайтах с бесплатными объявлениями, будьте осторожны. Отдавайте предпочтение проверенным интернет-ресурсам, использующим сервис «безопасная сделка».

4. Поступил звонок о компенсации за некачественные лекарства или медицинские приборы? Для получения денег предлагают оплатить ряд услуг? Это обман! Не переводите денежные средства незнакомым людям.

5. Звонит оператор сотовой связи и сообщает об окончании срока действия сим-карты? Это мошенник! Действие сим-карты бессрочно. Не вводите на телефоне комбинации цифр и символов под диктовку третьих лиц.

6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!

7. «Родственник» по телефону сообщает, что попал в ДТП. Срочно просит крупную сумму денег. Это уловка аферистов! Прекратите разговор. Перезвоните родственнику, убедитесь, что с ним все в порядке. Не передавайте деньги посторонним людям.

8. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером! Используйте лицензионное антивирусное программное обеспечение.

9. Нашли в сети Интернет информацию о возможности заработать на курсах акций? Будьте бдительны! Вас могут обмануть! Пользуйтесь услугами официально зарегистрированных брокерских организаций.

Если вы стали жертвой преступления, незамедлительно обратитесь в полицию по номерам телефонов: 02 (102) или 112.