СПОСОБЫ

противодействия мошенничеству с использованием информационно-телекоммуникационных технологий и методов социальной инженерии

1. Мошенник представляется сотрудником безопасности банка, сотрудником государственных органов:
   Действующий сотрудник
   - ✓ никогда не запрашивает кодов безопасности из смс сообщений
   - ✓ никогда не требует проведения каких либо операций с денежными средствами
   - ✓ всегда сможет объяснить ситуацию при личной встрече
   - ✓ расписка о неразглашении информации оформляется только в личном присутствии гражданина

2. Мошенник представляется работником сотовой компании, портала госуслуг, работником страховой компании и сообщает об окончании договора
   - ✓ Положить трубку
   - ✓ Не перезванивать по предложенным номерам
   - ✓ Не переходить по предложенным ссылкам
   - ✓ Перезвонить в организацию по телефону, который размещен на официальном сайте организации
   - ✓ Не сообщать коды из смс сообщений
   - ✓ Не сообщать личные сведения

3. Мошенник звонит с незнакомого номера и представляется **родственником**, который попал в ДТП или совершил преступление
   - ✓ Положить трубку
   - ✓ Перезвонить по известному вам телефону
   - ✓ Уточнить информацию у родственников
   - ✓ Уточнить информацию в отделении полиции

4. В мессенджере или в социальной сети от имени знакомого человека вас просят перевести денежные средства на указанный телефон, либо банковскую карту
   - ✓ Не переходить по предложенным ссылкам
   - ✓ Перезвонить знакомому на известный вам телефон
   - ✓ Перезвонить общим знакомым, не присылали ли им подобную просьбу

5. Незнакомый собеседник предлагает вам заработать крупную сумму с помощью инвестиций, просит установить на свой телефон специальное приложение
   - ✓ Проверьте информацию о компании в сети Интернет
   - ✓ Не устанавливайте непроверенные приложения, среди них есть программы предоставляющие удаленный доступ к вашему устройству
   - ✓ Не переводите денежные средства на личные счета незнакомых людей
   - ✓ Большую выгоду от инвестиций обещают только мошенники

6. Если вы осуществляете покупку или сами продаете по объявлению на специализированных сайтах
   - ✓ Общайтесь только на сайте, не переходите в мессенджеры
   - ✓ Не переходите по предложенным ссылкам
   - ✓ Используйте сервис «безопасная сделка»
   - ✓ Не сообщайте личные данные, помните для перевода денег достаточно номера телефона или номера карты
   - ✓ Никому не сообщайте коды из смс сообщений

7. Если вы сделали заказ на каком-либо сайте или в интернет-магазине, после чего вам стали поступать угрозы
   - ✓ Поставьте телефон в режим записи разговора и предупредите собеседника, что ваш разговор записывается
   - ✓ Не переводите никому денежные средства
   - ✓ Если восприняли угрозы реально, обратитесь в полицию

МО МВД России «Чердаклинский»

Уважаемые граждане!

► Если Вам позвонили, представились сотрудником банка или правоохранительных органов и сообщили о попытке хищения денежных средств с Вашей карты (счета)…

► Если Вам позвонили с неизвестного номера и представились родственником, пояснив, что у него сейчас проблемы и ему срочно необходимы денежные средства, которые нужно перевести на неизвестный счет или передать курьеру…

► Если Вам поясняют, что с целью предотвращения хищения денежных средств Вы должны сообщить коды и реквизиты банковских карт (счетов), коды подтверждения операций, поступающие на телефон, либо самостоятельно перевести денежные средства на предоставленный Вам «безопасный счет»…

► Если вам предлагают перейти по ссылкам в смс сообщениях на интернет-сервисах «Авито», «Юла»…

ЗНАЙТЕ – ЭТО МОШЕННИКИ!!!

ПРЕКРАТИТЕ РАЗГОВОР, ПРЕРВИТЕ СОЕДИНЕНИЕ!!!

Никому ни при каких обстоятельствах не сообщайте персональные данные и коды из смс сообщений!!!

При необходимости Вы всегда можете связаться с банком по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты), обратиться в отделение банка или полицию по номеру 02