ПАМЯТКА
о видах мошенничества и способах их предотвращения

Основным инструментом злоумышленников для хищения денег остается использование приемов и методов социальной инженерии, когда человек под психологическим воздействием добровольно переводит (передает) деньги или раскрывает банковские сведения, позволяющие злоумышленникам совершить хищение.
Телефонный звонок - ключевой инструмент мошенников, которые занимаются хищением денежных средств. Они постоянно придумывают все более изощренные схемы и сценарии для звонка, чтобы заполучить доступ к деньгам. Схемы злоумышленников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Чтобы вызвать доверие, они могут обращаться по имени и отчеству. С первых минут разговора мошенники начинают давить авторитетом и должностью. Распространенные способы обмана:

Якобы сотрудник Пенсионного фонда, соцслужбы
Мошенники сообщают, что гражданину положены дополнительные выплаты, компенсации от государства или какого-нибудь фонда. Причем для получения этой выплаты никуда ходить не надо: все деньги переведут на карту, необходимо только продиктовать все ее реквизиты, в том числе код с обратной стороны.

Якобы сотрудник поликлиники, аптеки, медицинского центра
Мошенники соотносят информацию о проблемах со здоровьем гражданина и сообщают ему о появлении дефицитного и дорогого лекарства по специальной цене, которое надо срочно выкупить. Злоумышленники объясняют, что человек платит полную стоимость, а разницу в цене по скидке вернут ему на карту, реквизиты которой необходимо сообщить

Якобы друг или родственник
Мошенник может представиться родственником/другом, попавшим в неприятную ситуацию, или ее случайным свидетелем, а также представителем правоохранительных органов, который готов помочь гражданину с решением проблемы (например, требование передачи курьеру или перечисления денежных средств на банковский счет за не привлечение родственника/друга к уголовной ответственности).

Поддельные Интернет-ресурсы (фишинг)

Мошенники подделывают сайты известных магазинов, марке плейсов, туристических компаний и др. Например, замаскированный под официальный сайт «Госуслуги». Несмотря на то, что внешне он очень похож на настоящий, при внимательном рассмотрении можно заметить, что наименование сайта в адресной строке отличается от официального домена.

Якобы сотрудник правоохранительного органа или банка (как правило, следователь, представитель службы безопасности банка)
Гражданам звонят якобы от имени Центробанка сообщают, что по их карте зафиксирована подозрительная активность: пытаются перевести все деньги за рубеж. Чтобы сохранить свои деньги гражданину необходимо открыть в Центробанке «защищенный/безопасный/специальный» личный счет. Для этого уточняют паспортные данные, просят подтвердить данные по счету/карте, а для открытия счета просят подтвердить небольшой перевод на этот счет, который Центробанк якобы совершает для своих клиентов, то есть сообщить код из СМС.
Также иногда злоумышленники представляются сотрудниками правоохранительных органов. Такие мошенники долго и подробно рассказывают об обстоятельствах уголовного дела, участником которого, по их словам, гражданин является. Далее для уточнения информации они просят сообщить личную и финансовую информацию. Это и является признаком того, что гражданин разговаривает с мошенником: правоохранительные органы не просят назвать по телефону финансовую информацию. Сценарии могут быть разные: от классического «с вашей карты пытаются перевести деньги» до пугающего «по карте замечены подозрительные операции, и она заблокирована». В любом случае итогом будет просьба сообщить информацию по карте или счету, код из СМС-сообщения.

Общие правила поведения с кибермошенниками

Для того чтобы обезопасить свои данные, установите двухфакторный способ аутентификации (например, логин и пароль, а также подтверждающий код из СМС) - это, как правило, бесплатно.
Пользуйтесь только проверенными и официальными сайтами финансовых организаций в поисковых системах (Яндекс, Mail.ru), помеченными цветным кружком с галочкой

Новая схема мошенничества. Сначала мошенники настаивают на том, что общение может продолжаться только по видеосвязи, а затем под разными предлогами просят включить демонстрацию экрана смартфона.
Сами аферисты в это время уже сидят на сайте банка, в котором у человека есть карта, и рассчитывают по номеру его телефона или все той же карты, попасть в личный кабинет. Они планируют сбросить старый пароль и установить новый. Но для этого им нужны коды, которые придут на смартфон человека. И именно для этого они просят включить демонстрацию экрана — чтобы разглядеть уведомление от банка. Если человек следует инструкциям собеседника, то мошенники получают доступ к его мобильному банку и опустошают банковские счета.

заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получат доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней

установите антивирусные программы на все свои телефоны и компьютеры. Важно регулярно обновлять антивирусную базу

В случае если вам позвонили и представились якобы сотрудником банка, положите трубку и самостоятельно позвоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка. Не нужно перезванивать на номера, с которых вам звонили, - вы рискуете попасть на мошенников

не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и другие) и финансовые (номер, срок действия, трехзначный код с оборотной стороны карты) данные. Переданные мошенникам личные и финансовые данные могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;

не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы. Сомнительные ссылки могут быть опасны для вашего гаджета наличием вируса или вредоносного ПО на сайте, на который они ведут, а скачивание программ с неофициальных источников может дать мошенникам доступ к вашему гаджету

не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, а звонки на неизвестные пропущенные телефонные номера могут быть чреваты как минимум списанием значительной суммы с вашего мобильного счета, а как максимум - быть поводом для мошенников активизировать против вас мошенническую схему

Что делать, если мошенники все же похитили денежные средства?

Как только вы это обнаружите, сразу же заблокируйте карту, а также сообщите о хищении (не позднее суток с момента получения информации о хищении необходимо написать о несогласии с операцией). Сделать это можно через мобильное приложение банка, а также позвонив в контактный-центр или обратившись в отделение банка.
Затем как можно скорее напишите заявление в полицию, лично обратившись в ближайший территориальный орган внутренних дел с заявлением о возбуждении уголовного дела.
В случае если вы утратили электронное средство платежа и (или) оно использовалось без вашего согласия, банк обязан в течение 30 дней возместить сумму хищения.

Как противостоять телефонным мошенникам?
Ни в коем случае не отвечайте на звонки с незнакомых номеров. Как правило, если вам звонят с работы или из другой организации, от которой вы ожидаете звонка, вам дополнительно напишут СМС-сообщение или сообщение в мессенджере. Никогда не перезванивайте по незнакомым вам номерам.
Если разговор касается финансовых вопросов, не продолжайте разговор и положите трубку. Сотрудники банков или правоохранительных органов не запрашивают Ваши личные и финансовые данные по телефону