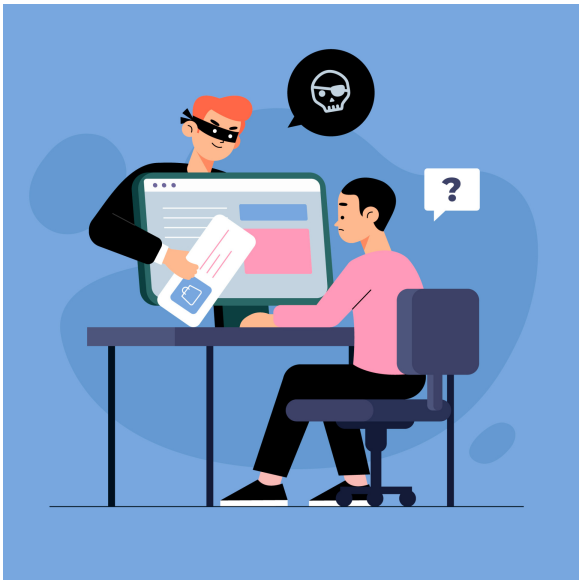
ПАМЯТКА

о наиболее распространенных способах совершения IT-преступлений, рисках хищений с применением цифровых технологий и методах защиты от них



С каждым годом мошенники придумывают все более изощренные схемы отъема денежных средств. Вот простые рекомендации, соблюдение которых поможет Вам сохранить деньги и ценности.

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

- не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан сотрудниками полиции за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом;
- не следует отвечать на звонки или SMS-сообщения с неизвестных номеров с просьбой положить на счет деньги;
- не следует сообщать по телефону кому бы то ни было сведения личного характера.

Мошенники в образе операторов связи. Лжепредставители операторов связи звонят абонентам и утверждают, что скоро ваша SIM-карта перестанет действовать и ее надо заменить, продлить или актуализировать паспортные данные. Цель - войти в личный кабинет абонента. Преступник постарается настроить переадресацию сообщений на свой телефон для дальнейшего получения доступа к личному кабинету банка. Возможно так же, что преступник надеется на то, что человек не заметит, что СМС пришло от банка или с Госуслуг.

Деньги за опрос. Злоумышленники предлагают жителям поучаствовать в предвыборном опросе за вознаграждение, а после завершения просят указать данные банковской карты. Для этого нужно скачать мобильное приложение, ответить на несколько вопросов, а затем - указать данные карты и предоставить доступ к контактным данным и СМС. В результате человек может потерять свои деньги.

СМС-сообщение о неожиданном выигрыше. Задумайтесь! Настоящий розыгрыш призов не должен подразумевать денежные выплаты с Вашей стороны! Не торопитесь расставаться со своими деньгами!

Близкие попали в беду. Вам звонят с незнакомого номера и тревожным голосом сообщают, что Ваши близкие попали в беду. А для того, чтобы решить проблему, нужна крупная сумма денег – по такой схеме работают мошенники! Самостоятельно прекратите разговор и позвоните родственникам, чтобы проверить полученную информацию.

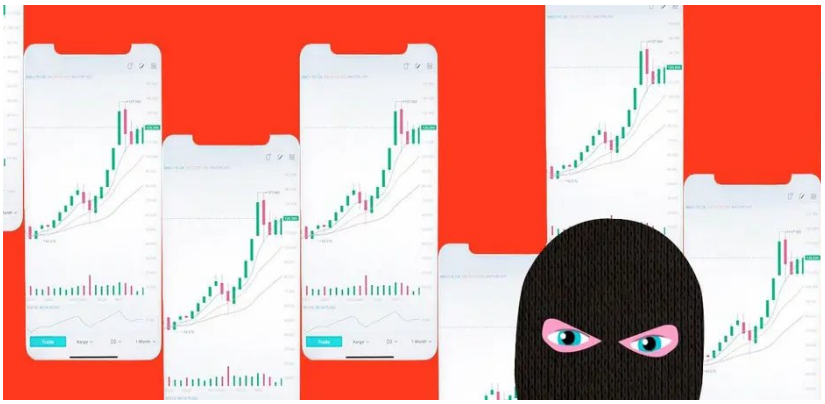
В интернет-магазине просят предоплату. Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов и сайтов по продаже авиабилетов. Чем привлекают потенциальных жертв мошенники? Прежде всего - необоснованно низкими ценами. При заказе товаров вас попросят внести предоплату. Далее магазин в течение нескольких дней будет придумывать отговорки и обещать вам скорую доставку товара, а потом бесследно исчезнет либо пришлет некачественный товар.

Банковская карта заблокирована. Необходимо помнить о том, что единственная организация, которая сможет проинформировать вас о состоянии вашей карты – это банк, обслуживающий ее. Если у вас есть подозрения о том, что с вашей картой что –то не в порядке, если вы получили смс-уведомление о ее блокировке, немедленно обратитесь в банк. Телефон клиентской службы банка обычно указан на обороте карты. Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении.

Крик о помощи. Один из самых отвратительных способов хищения денежных средств. В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.
Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка, убедитесь в честности намерений.

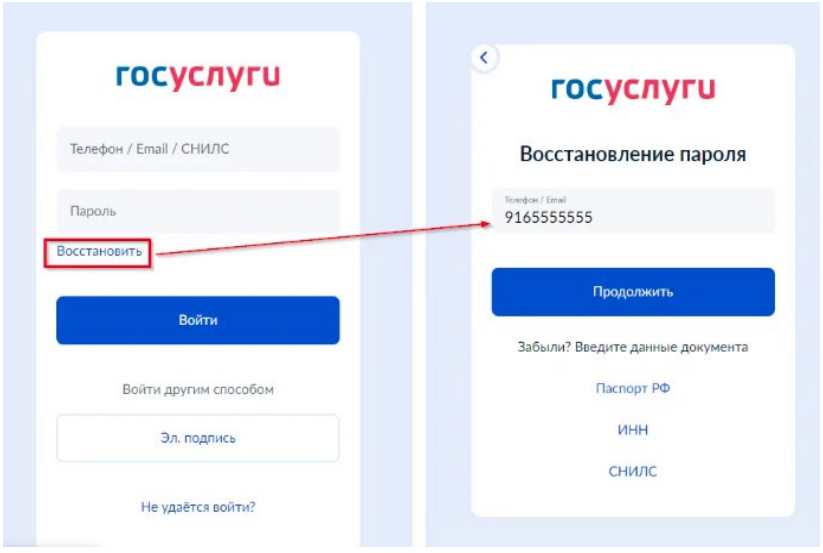
Фишинг. Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. К примеру, потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на "сайт-двойник" такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы.

Ошибочный перевод средств. Абоненту поступает SMS-сообщение о поступлении средств на его счет. Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно.
В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются средства.
Для решения вопроса по возврату денег предложите человеку обратится в банк.

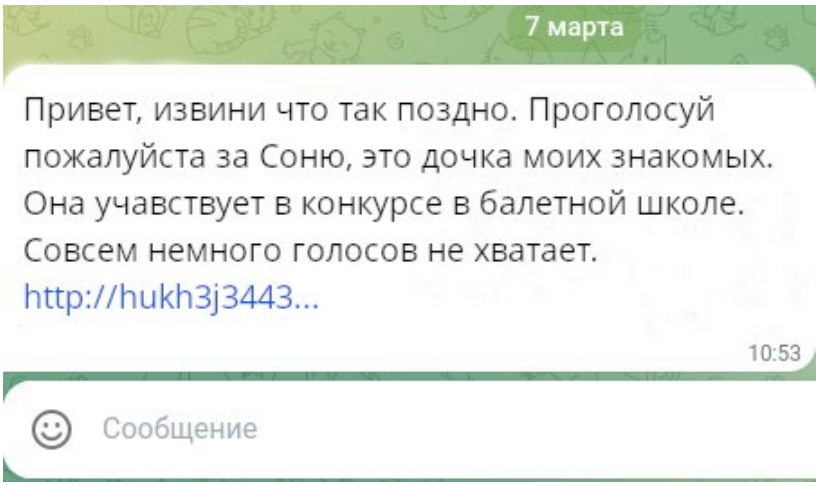


Мошенники под видом брокеров. Признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам-трейдерам.
Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

Кража Cookie. Cookie (куки) — это небольшие текстовые файлы, сгенерированные сайтами. Они необходимы для сохранения персональной информации и предпочтений пользователя. Если на сайте есть личный кабинет, то cookie могут хранить логин и пароль, номера телефонов, номера карт, паспортные данные, адреса.
Злоумышленники могут достаточно просто перехватить файлы cookie и воспользоваться информацией, которая в них хранится. Главная рекомендация - не используйте автозаполнение, вводите свои данные каждый раз вручную. Используйте режим инкогнито и регулярно удаляйте сохраненные куки. Не переходите по сомнительным ссылкам, не устанавливайте сомнительные расширения и плагины для браузера.



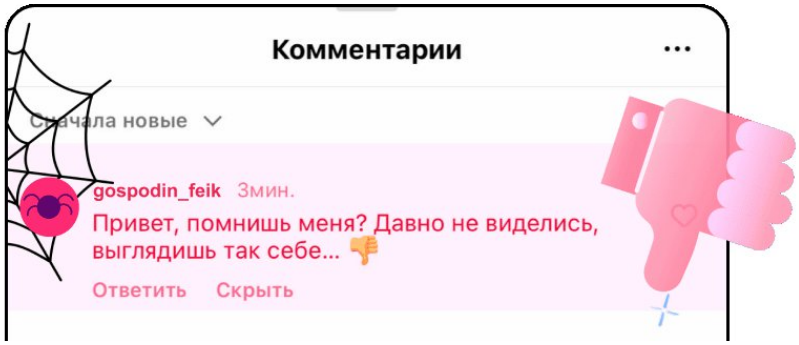
Госуслуги. Мошенники инициируют смену пароля в личный кабинет жертвы и под разными предлогами пытаются получить СМС. Учетная запись на Госуслугах стала универсальным ключом, который открывает много дверей. Получив доступ, мошенники могут например оформить кредит без визита в банк.
Для защиты необходимо включить двухфакторную идентификацию (для входа потребуется вводить код из СМС) и не использовать простые пароли.



Проголосуй за Соню. Знакомый пишет вам с просьбой: «Проголосуй, пожалуйста, за племянницу в конкурсе». Почему бы не помочь? Вы переходите по ссылке — там просят указать номер телефона и ввести на сайте код из СМС.

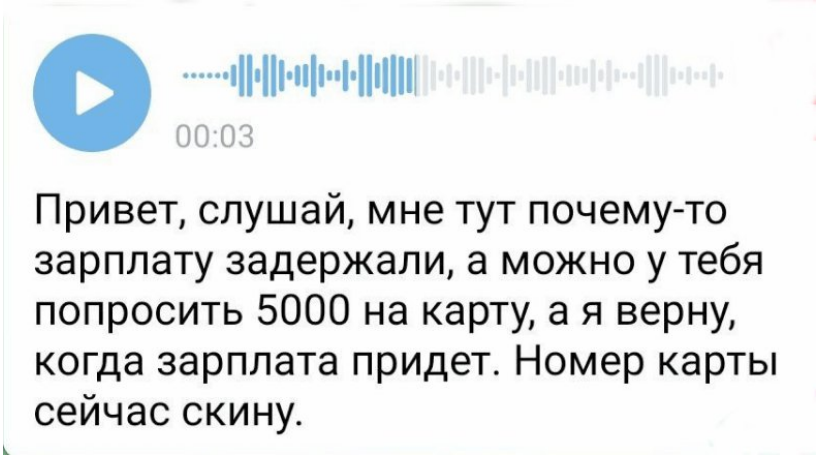
Телефон и одноразовый код — это ключи к вашим аккаунтам в социальных сетях и мессенджерах.

Не переходите по ссылкам, в которых не уверены.



Комментарии. Вы опубликовали новую фотографию в соцсети. Под постом появляется очень обидный комментарий. Но кто его оставил? Аккаунт закрыт, зато есть ссылка на другую популярную соцсеть. Вы идёте туда.

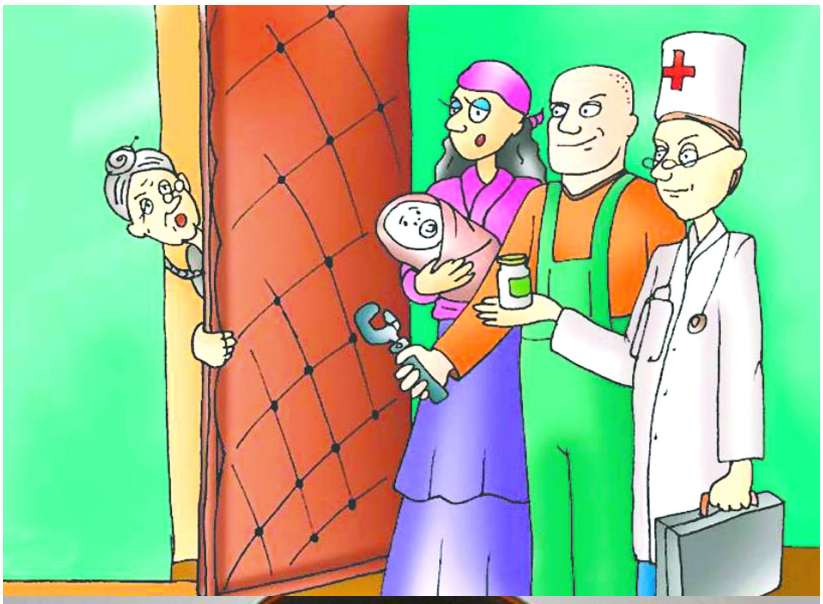
Популярная соцсеть оказалась фальшивкой. Страничка была во всём похожа на оригинал, но теперь пароль от вашего аккаунта у мошенников.



Голосовое сообщение. Мошенники взламывают аккаунт человека, а потом «обучают» нейросеть с помощью его голосовых сообщений. Дальше нейросеть генерирует небольшое аудио с просьбой перевести денег. И отличить такую запись от настоящего голоса очень сложно.

Когда дело касается денег, проверяйте трижды. Свяжитесь с человеком другим способом, спросите что-нибудь, известное только вам двоим.

Лжеврачи. Сценарии самые разнообразные. К примеру пожилому человеку звонит якобы врач, который заявляет, что получил результаты анализов или другого исследования, которые показали, что пенсионер серьезно болен. Далее предлагается дорогостояще лечение, возможно в кредит. Предлагают сделать бесплатно прививку, а между делом обчищают квартиру.



Мошенники по видом социальных служб. Мошенники под видом социальных работников звонят пенсионерам и говорят, что им положена какая-то выплата, компенсация или денежный подарок. Для получения необходимо вложить определенную сумму. Либо просят пенсионеров сообщить номер банковской карты и пин-код якобы для того, чтобы перевести сумму на счет. Естественно, все деньги на карте после этого пропадают.

Повторный «развод». Обманывают уже обманутых однажды пенсионеров от лица правоохранительных органов, например, сотрудников прокуратуры, адвокатов и других. Мошенник просит поспособствовать раскрытию преступления, а именно — выступить в качестве приманки, чтобы поймать злоумышленников по горячим следам.

Часто в разговоре по телефону мошенники представляются участковыми, оперативниками, следователями, сотрудниками банка и т.д. Если есть сомнения, спросите адрес учреждения, чтобы подойти туда лично. У настоящего сотрудника будет рабочее место, куда он может «пригласить вас для беседы». Если он отказывается – кладите трубку. Помните о возможной подмене номера, мошенник может позвонить с официального номера организации, предложите самим перезвонить на этот номер. Насторожитесь если Вас торопят, говорят что время на исходе, обещают выгоду.

Самыми уязвимыми для мошенников являются пожилые люди и дети, они доверчивы и порой наивны. Объясните им, что не стоит верить человеку, даже если он представился работником поликлиники, Минздрава, полиции, прокуратуры, социальной службы и так далее. Пусть они не стесняются звонить вам в подобной ситуации.

Телефон – самый популярный способ мошенничества. Самый действенный метод защиты - использование «белого списка» для входящих звонков. Неизвестные - те, кого нет в списке контактов будут блокироваться. Функция «белый список» прекрасно работает на большинстве мобильных телефонов, но реализована у разных производителей по разному.

Если Вы или Ваши близкие стали жертвами мошенников, или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обратитесь в полицию!