



Свердловская региональная социально
ориентированная общественная организация
«Право на защиту и помощь»



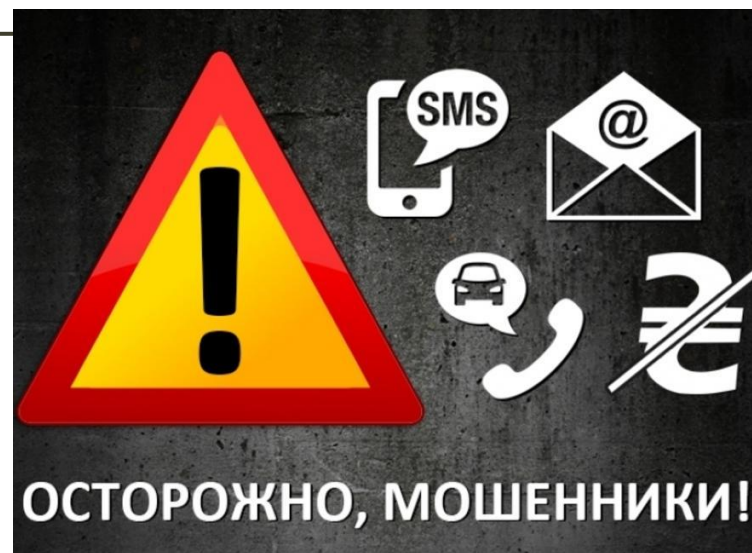
Проект:

Правовое просвещение пожилых людей

Лекция-семинар на тему:

ОСТОРОЖНО- МОШЕННИКИ!

(виды мошенничества и
способы защиты)



Что важно знать пожилым людям, чтобы защититься от мошенников



Распространенные виды обмана

- Проникновение в жилище под видом работников разных госслужб.
- Посещение квартир с сообщениями о надбавке к пенсии, перерасчете квартплаты, обмене денег "для ветеранов и пенсионеров".
- Продажа дорогостоящих товаров, которые не соответствуют требованиям к качеству.

Будьте бдительны!

- ✗ Не принимайте незнакомых людей, когда вы одни.
- ✗ Не отдавайте в руки чужим людям паспорт.
- ✗ Не сообщайте ПИН-код и CVV банковской карты.
- ✗ Не пересчитывайте деньги при незнакомцах.

Что важно знать пожилым людям, чтобы защититься от мошенников

Позвонили в дверь: что происходит и что делать

Пришли представители служб, которых вы не вызывали.



Позвоните в учреждение, от которого якобы пришли незнакомцы.

Вы почувствовали потенциальную опасность от незнакомцев.



Сообщите в полицию и предупредите о ситуации родных.

Вам предлагают совершить покупку на дому с большой скидкой.



Скорей всего, это мошенники. Не совершайте такие покупки без обсуждения с близкими.

Повесьте на видное место телефоны важных служб, банка, соседей и родственников.

8 (800) 100-29-26

горячая линия по вопросам нарушений прав потребителей финансовых услуг.

02, 102 — полиция.

Мошенничество с помощью мобильных телефонов

Мобильным телефоном сейчас уже никого не удивишь. Телефон перестал быть привилегией состоятельных людей. Современные технологии сегодня доступны и дошкольникам, и старшему поколению. Но с развитием технологий развиваются и способы мошенничества.

Главная группа риска для мобильного мошенничества — пенсионеры и дети.

Тем не менее, практика показывает, что жертвой мошенников может стать каждый, ведь мошенники применяют особые методы психологического воздействия.



- ▶ В основном преступники прибегают к отказу от откровенного криминала. Мошенники трепетно следят за последними изменениями и направляют свою деятельность по самому эффективному пути.
- ▶ По данным специалистов годовой доход мошенников превышает \$ 160 млн. долларов.



Выигрыши

priz.europapluz.ru
Pozdravlaem! Vy vyigrali
noutbuk `Asus VX-2`.
Podrobno po telefonu:
[+7-912-144-78-67](tel:+7-912-144-78-67).
Europa+

Каждому приятно получить подарок — внезапно почувствовать себя обладателем миллиона или дорогой машины.

На Ваш телефон пришло SMS о выигрыше ценного приза? Не спешите радоваться внезапной удаче и звонить по телефону «для справок», указанному в сообщении.

Как говорится, бесплатный сыр бывает только в мышеловке. Чаще всего мошенники выманивают деньги «победителя» под предлогом налога на выигрыш. Не поддавайтесь на уловки злоумышленников! Уточните информацию об акции на сайте компании-организатора, где должны быть представлены все условия розыгрышей и способы связи.



Ошибочны е платежи

Платеж 200,00 р
зачислен 07.11 в 11:59
через QIWI(qiwi.www.ru)

07.11.2011 11:18

Извините клал жене
200 руб.ошибочно
положил вам.жене
положил ещё
раз,верните дочке на
ном.89108050497 это
МТС.Она в
больнице.Спасибо!

Кто-то пополняет Ваш счёт на приличную сумму (может даже прийти SMS-уведомление, что «через платёжную систему «N» в 08:56 на Ваш счёт зачислен платёж в размере 300 руб.»), а затем раздаётся звонок, и вежливый молодой человек или девушка говорит, что случайно положил(а) деньги не на свой счёт, а на Ваш. Незнакомец (или приятная незнакомка) настойчиво просит Вас перевести такую же сумму в ответ. Как только Вы выполняете просьбу, «ошибочный» платёж с Вашего счёта исчезает.

Ещё один вариант — платёж на Ваш номер не совершается, а после SMS-уведомления об оплате сразу приходит второе SMS от мошенников: «Извини, я ошибся и положил на твой счёт 300 руб., переведи их мне, пожалуйста!».

Просьбы о помощи

Наверняка Вам или Вашим родственникам приходили SM с текстом вроде

«Мам, кинь на этот номер деньги.

У меня серьезные проблемы. Утром все объясню».



Похожий вариант — звонок от незнакомца, который говорит: **«Ваш сын сбил человека (или задержан с наркотиками). За выкуп можно все уладить».** Испуганные родители принимают такое сообщение за чистую монету и несут любые деньги в терминал оплаты, лишь бы помочь своему чаду.

В этот момент они даже не задумываются о том, что это ещё одна хитрая уловка мошенников. Обман обнаруживается только после звонка ребёнку, который жив и здоров, и в недоумении развеивает все родительские страхи.

Злоумышленники пытаются играть на чувствах людей. Если Вы столкнулись с подобным мошенничеством, не впадайте в панику и не спешите переводить деньги на незнакомый номер. Сразу же сами перезвоните «попавшему в беду» человеку или тем людям, которые могут находиться рядом с ним.



Выманивание паролей

Ваши пароли — секретная информация, известная только Вам.

Но мошенники знают, как её у Вас выманить. Есть масса мошеннических схем.

Вам звонит **ребёнок** с просьбой сообщить код, который придёт Вам в SMS, объясняя это тем, что он ошибся. После того, как Вы сообщите код, мошенники тут же оформят на Ваш номер платную подписку.

«Эффектная блондинка» в говорит Вам, что ошиблась номером, и просит сообщить код, который придёт Вам по SMS. После получения кода злоумышленник покупает виртуальную валюту на деньги с Вашего лицевого счёта.

Никогда не сообщайте людям, которых Вы не знаете, свои пароли от электронной почты, социальных сетей и форумов. Не поддавайтесь на уловки злоумышленников.



Опасные «открытки»

Получен MMS-Подарок
от Кати. Открыть:
<http://opera.wop.su>

Перед праздниками мошенники любят рассылать SMS с поздравительными «открытками» или ссылками на фотографии. Переходите по ссылке — и со счёта списывается часть денег, или в телефон загружается вирус.

На Ваш телефон пришло SMS- или MMS-сообщение с предложением пройти по ссылке, чтобы получить открытку или фотографию, либо прочитать поздравление? Если абонент Вам незнаком, а номер неизвестен, не открывайте вложенные файлы и не переходите по ссылкам.

SMS из несуществующего «банка»



Ваша банковская карта заблокирована! По вопросам снятия блокировки обращайтесь по т.8(800)555-17-94 Технический отдел

Представим ситуацию: Вы собрались в отпуск, проходите паспортный контроль на входе в поезд, и в этот момент Вам приходит сообщение: «**Ваша банковская карта заблокирована. По вопросам снятия блокировки обращайтесь по такому-то телефону**», а дальше подпись: «**Технический отдел банка**».

В состоянии стресса Вы импульсивно звоните по номеру, указанному в сообщении. А на том конце Вас уже поджидают злоумышленники. Представившись сотрудниками банка, они спросят у Вас данные кредитной карты, чтобы в считанные часы снять с неё деньги.

Как же действовать в такой ситуации?

При поступлении подобных SMS ни в коем случае не сообщайте персональные данные неизвестным лицам. Даже если они представляются сотрудниками банка.



Wangiri — о-очень дорогой звонок

За таинственным словом «Wangiri» кроется мошенническая схема, которая появилась в Японии. Кто-то звонит Вам с неизвестного номера, но как только Вы берёте трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого — как можно дольше удерживать Вас на линии, пока с Вашего счёта утекают деньги.

Стоимость звонка на подобный номер может достигать нескольких десятков рублей за минуту, и даже несколько секунд ожидания на линии может стоить Вам серьёзных денег.

Самая лучшая профилактика подобного вида мошенничества — Ваша бдительность. Не перезванивайте на неизвестные номера. Если Вы всё-таки стали жертвой злоумышленников, сообщите нам номер, с которого Вам звонили, и подробности вызова.



Требование выкупа

ВАШ НОМЕР У НАС,
ЧТО БЫ ВЕРНУТЬ СВОИТЕ
8,964-503-20-90

Потеряли ключи, паспорт, любимую собачку? Украла автомобильный номер? Мошенники не упустят шанс нажиться на Вашей беде.

Сегодня встречаются мошеннические схемы, по которым жертве предлагают перевести деньги на чужой мобильный номер в качестве выкупа за возврат пропажи. В стрессовой ситуации растерянный человек чаще всего действует импульсивно, а мошенники — тут как тут, и готовы «помочь» за небольшое вознаграждение.

Не поддавайтесь на уловки злоумышленников. Если у Вас украли автомобильный номер и оставили записку с предложением вернуть его за вознаграждение, не верьте преступникам. Лучше сразу обратитесь в ближайший полицейский участок с заявлением о краже.

Если Вам звонят с радостным известием, что Ваш пропавший домашний питомец (телефон, паспорт и т.д.) нашёлся, — не спешите переводить неизвестному человеку «вознаграждение».



Мошенничества с банковскими картами



Самые популярные схемы
мошенничества

СКИММИНГ в банкоматах

Мошенники устанавливают на банкоматы считывающие устройства - скиммеры, для копирования магнитной полосы.



или на клавиатуру приклеивают накладку, очень похожую на настоящую клавиатуру, которая запоминает нажатия клавиш и также записывает их на

Банк устанавливает на щель картоприемника специальные **встроенные** накладки, препятствующие установке посторонних устройств.



ФИШИНГ



Цель мошенника проста - узнать логины, пароли, номера карт и кодов CVV2/CVC2 жертвы. Далее, используя полученные данные, мошенники получают доступ к банковским картам, on-line кабинетам интернет-банков и пересылают средства на мошеннические счета или совершают покупки в интернет-магазинах.

Для этого используются разнообразные приемы

1. Мошенник звонит клиенту и представившись сотрудником банка сообщает, что у клиента возникла некая проблема (возможны варианты), для решения которой клиент срочно должен назвать ряд сведений о карте.
2. Жертва получает СМС с сообщением, что его карта заблокирована и номером телефона якобы службы поддержки, звонящих на указанный номер, мошенники "обрабатывают", используя растерянность клиента и в ходе разговора узнают, необходимые для мошенничества данные
3. Мошенник, зная логин и пароль клиента, направляет жертве письмо, что с его карты произошло мошенническое списание средств и для отмены транзакции необходимо назвать код, полученный по СМС от банка. На самом деле СМС код подтверждает иницированную мошенником операцию и используя названный жертвой код мошенник отправляет средства со счета жертвы на свой счет, либо оплачивает услуги провайдеров.

Кража карт



Схема мошенничества:

1. Мошенник ворует сумку с кошельком, кошелек, либо саму карту

Если в кошельке вместе с картой лежит ПИН-код, то мошенник опустошает карту в ближайшем банкомате. Если ПИН-кода нет, то мошенник делает попытку опустошить карту, покупая высоко ликвидные товары (бытовая и компьютерная техника, ювелирные изделия, мобильные телефоны, бензин, алкоголь и т.д.) в магазинах, принимающих карты, либо интернет-магазинах и сервисах интернет-оплаты банковской картой.

Хранение карт (недопущение хищения)

- Не храните и не оставляйте карты на столах, в шкафах, сервантах, на полках и не разбрасывайте их на видном месте, ни дома, ни на работе
- Не храните карту в кошельке, если носите его в сумке
- Не носите карты вместе с паспортом и другими документами, удостоверяющими вашу личность
- Лучшее место для стационарного хранения карт - сейф или запирающийся ящик стола
- Если вы носите кошелек с деньгами в сумочке, карты лучше хранить в отдельном кармашке сумочки
- Чтобы не забыть карту в магазине, возьмите за правило каждый раз, совершая покупку, проверять куда положили карту.





КАК НЕ СТАТЬ ЖЕРТВОЙ **МОШЕННИКОВ.**

НЕ СОГЛАШАЙТЕСЬ

на предложения
снять порчу или сглаз,
погадать, предсказать
будущее, - это хороший
повод завладеть
Вашими деньгами.

НЕ СОГЛАШАЙТЕСЬ

на приглашения
принять участие в
розыгрыше призов,
купить
чудодейственные
лекарства, приборы
или дешевые вещи
и продукты.

НЕ ДОВЕРЯЙТЕ

информации, если Вам
сообщают, что Ваш
родственник или
знакомый попал в беду
и нужны крупная
сумма денег, чтобы
«вытащить» его.
Это 100% обман!

НЕ ДОВЕРЯЙТЕ

информации, что у Вас
или у Вашего
родственника обнаружена
опасная болезнь и нужны
деньги на лечение или
покупку дорогостоящих
лекарств – **ВРАЧИ НЕ
СООБЩАЮТ .**



**Будьте бдительны
и осторожны!**

СПАСИБО ЗА ВНИМАНИЕ!