ШКОЛА БЕЗОПАСНОСТИ:

Мошенничество

Теоретический курс: Как не стать жертвой аферистов.

Презентация подготовлена юрисконсультом
ГОАУСОН «Терский КЦСОН»
Ятковской О.И.

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.

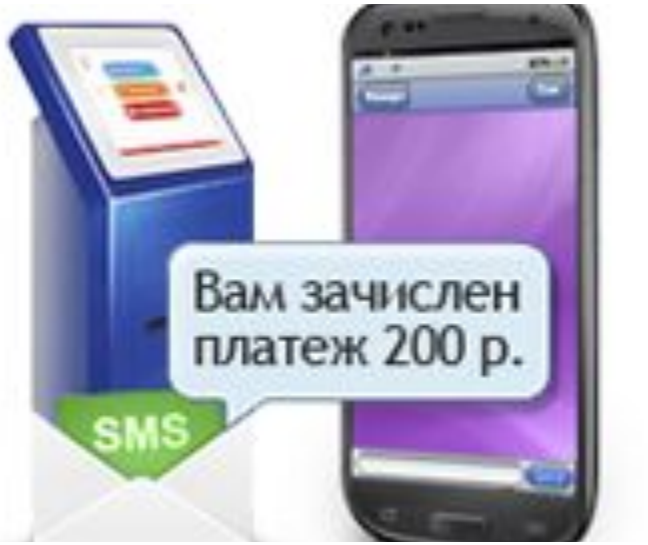
Выигрыши

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

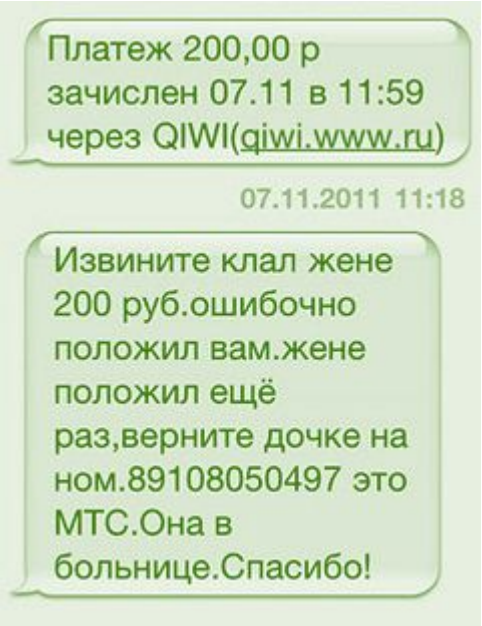
Каждому приятно получить подарок — внезапно почувствовать себя обладателем миллиона или дорогой машины.

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.



Ошибочные платежи



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 SMS

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.

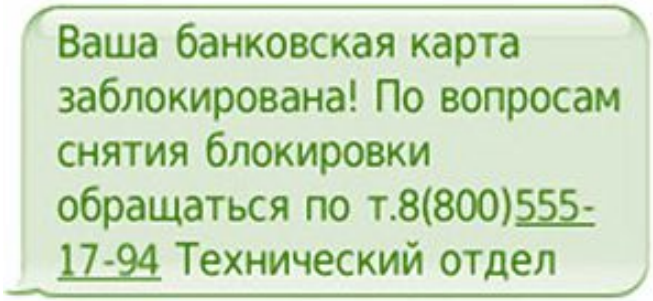
Опасные «открытки»

Получен ММС-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»



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.

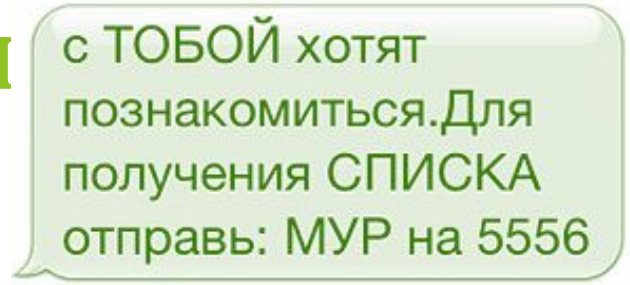
Wangiri — о-очень дорогой звонок

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 удержать 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.

Предложения познакомиться



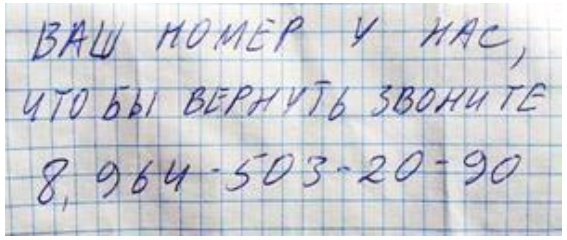
Каждому хочется найти свою «вторую половинку». Мобильные мошенники используют это желание и рассылают своим потенциальным жертвам предложения познакомиться — на сайтах знакомств, в социальных сетях, по электронной почте и SMS.

В самом простом варианте Вы получаете сообщение: **«Привет! Меня зовут Эмилия. Мне очень хочется с тобой познакомиться. Скинь мне SMS, я тебе позже отвечу. Напиши слово Emilia и отправь на номер XXXX. Я буду знать, что это ты».**

После отправки SMS со словом «Emilia» с Вашего счёта списываются деньги, а знакомство заканчивается, даже не начавшись.

Другой вариант мошенничества: собеседник на сайте знакомств сообщает о том, что уезжает, но не хочет прерывать переписку. Он предлагает Вам перейти на общение с помощью SMS или по телефону «через служебную связь». Может даже упомянуть вскользь, что стоимость сообщения и разговора будет чуть-чуть выше.

Требование выкупа



Потеряли ключи, паспорт, любимую собачку? Украли 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».

Рекомендуем вообще не переводить деньги неизвестным лицам до тех пор, пока пропажа не вернётся к Вам.

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 встроенную микросхему.

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

Ливанская петля

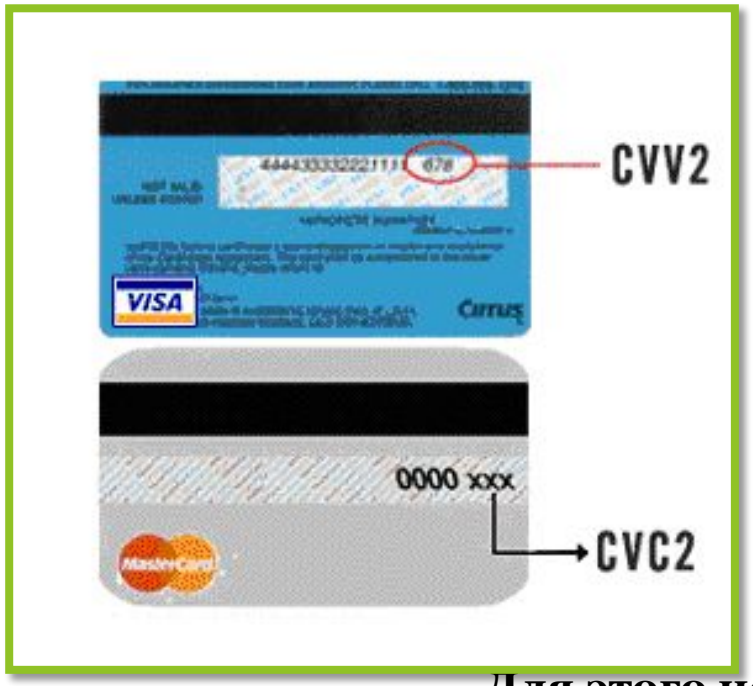
1. Мошенник вставляет в щель банкомата блокиратор, чаще изготавливаемый из обычной фотопленки. Блокиратор (ливанская петля) препятствует возврату карты из банкомата.

2. Клиент вводит карту в щель банкомата, карта застревает в блокираторе и клиент не может ее получить обратно. Обычно в подобных случаях клиент думает, что в банкомате произошел сбой и находится в смятении, не зная что делать.

3. Рядом "случайно" оказывается дружелюбный "помощник", который может быть похож на сотрудника банка, либо просто «опытного» прохожего, который начинает активно помогать клиенту в проблеме.

4. Доброжелатель начинает изображать бурную деятельность по спасению карты, жмет на различные кнопки и в один из моментов предлагает ввести ПИН-код. Как вариант мошенник может предложить ввести ПИН-год одновременно с нажатием одной из клавиш (к примеру "Ввод", или "Отмена")

5. Если клиент поддается на афёру и вводит ПИН-код, "доброжелатель" запоминает его и некоторое время якобы продолжает "спасать карту".
6. Получить карту обратно, обычно, так и не удается и «доброжелатель» говорит, что сделал все, что мог и рекомендует обратиться в банк с заявлением на возврат карты.
7. Клиент уходит, а мошенник вынимает из банкомата ливанскую петлю вместе с картой и используя запомненный ПИН-код за несколько минут опустошает карту, используя тот же банкомат.
8. В случае, если ПИН-код узнать так и не удалось, мошенник направляется в ближайший магазин и совершает покупки, пока деньги на карте не закончатся.



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 сомом деле СМС код подтверждает инициированную 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, банзин, 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.

Будьте бдительны и осторожны!

СПАСИБО ЗА ВНИМАНИЕ!