

Интернет - это безграничный мир информации. здесь ты найдёшь много интересного и полезного для учёбы. В интернете можно общаться со знакомыми и даже заводить друзей.



но кроме хорошего, виртуальном мире есть и плохое. Неправильное поведение в интернете может принести вред не только тебе, но также твоим родным и близким.



чтобы обезопасить себя в интернете, достаточно соблюдать правила, которые содержатся в этой памятке. В этих правилах нет ничего трудного. Отнесись к ним внимательно - и расскажи о них своим друзьям!



ТЕСТ на знание правил поведения в интернете

- 1) Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.
А Попрошу его фото, и потом отправлю своё.
В Посоветуюсь с родителями.
- 2) В чате тебя обозвали очень грубыми словами.
А Скажу в ответ: «Сам дурак».
В Прекращу разговор с этим человеком.
- 3) Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.
А Потребую доказательств, что она плохая.
В Сразу откажусь.
- 4) Пришло сообщение с заголовком «От провайдера» - запрашивают твой логин и пароль для входа в Интернет.
А Вышлю только пароль: они сами должны знать логин.
В Отмечу письмо как Спам.

посчитай, сколько получилось ответов «а» и сколько «в».

- 4 «А»**
Тебе ещё многому надо научиться.
- 3 «А» и 1 «В»**
Внимательно прочитай эту памятку.
- 2 «А» и 2 «В»**
Неплохо, но ты защищён лишь наполовину.
- 1 «А» и 3 «В»**
Ты почти справился, но есть слабые места.
- 4 «В»**
Молодец! К Интернету готов!



Министерство
внутренних дел
Российской
Федерации

Управление «К»

Безопасный Интернет - детям!



Полезные
советы
для тебя
и твоих
друзей



Осторожно: вирусы и другие (ЧЕРВИ, ТРОЯНЫ) вредоносные программы



В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья.

Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут **уничтожить** важную информацию **или украсть** деньги через Интернет.

- ▶ Для защиты компьютера на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
- ▶ Не сохраняй подозрительные файлы и не открывай их.
- ▶ Если антивирусная защита компьютера не рекомендует, **не заходи на сайт, который считается «подозрительным».**
- ▶ Никому **не сообщай свой логин с паролем** и не выкладывай их в Интернете - относись к ним так же бережно, как к ключам от квартиры.

Виртуальные мошенники (Воры) и другие преступники интернета

Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники - ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- ▶ Не сообщай свой адрес или телефон незнакомым людям и никогда не выкладывай в Интернете. Никогда **не высылай свои фотографии** без родительского разрешения. Помни, что **преступники могут использовать эту информацию** против тебя или твоих родных.
- ▶ Если ты хочешь поучаствовать в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
- ▶ Никогда **не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете.**

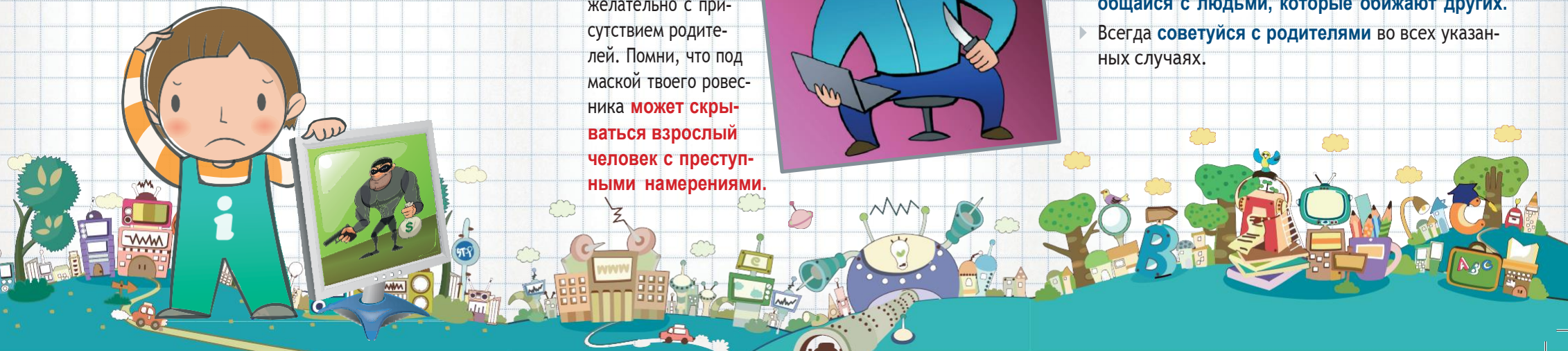
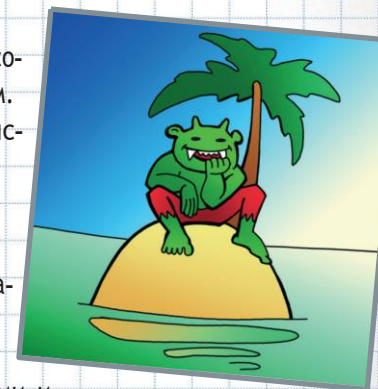
Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника **может скрываться взрослый человек с преступными намерениями.**



Грубияны и хулиганы (ТРОЛЬ, ПРОВОКАТОР) в интернете: как себя вести?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

- ▶ Помни: **ты не виноват**, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей - просто прекрати общение.
- ▶ Если тебе угрожают по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз - испугать тебя и обидеть. Но **подобные люди боятся ответственности.**
- ▶ Коллективное преследование - это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. **Никогда не участвуй в травле и не общайся с людьми, которые обижают других.**
- ▶ Всегда **советуйся с родителями** во всех указанных случаях.



ВНИМАНИЕ!

Будьте бдительны, не поддавайтесь на провокации мошенников.



Вы разместили в Интернете объявление о продаже своего имущества. Вам позвонил (иным образом связался) человек, которого устраивает предстоящая сделка и он предлагает Вам получить задаток на Вашу банковскую карту, для чего ему нужны реквизиты Вашей карты.

ЭТО МОШЕННИК!!!

Как только вы передадите свои реквизиты, деньги будут переведены Ваших счетов через Интернет.



Вам позвонил человек, представившийся работником банка (социальных служб, правоохранительных органов), который сообщил, что Вам полагается компенсация за ранее приобретенный некачественный товар (либо услуги), в крупной сумме (порядка 500 тысяч рублей), для получения которой необходимо оплатить налог в размере 13%.

ЭТО МОШЕННИК!!!

Вопросы различных компенсаций посредством телефонных звонков не решаются.



Вам позвонил близкий родственник (сын, дочь, внук), который сообщил что у него серьезные проблемы (попал в ДТП, избил человека) и передал трубку сотруднику полиции, который, в свою очередь, предлагает урегулировать вопрос путем перевода денег на номера сотовых телефонов свидетелей происшествия.

ЭТО МОШЕННИКИ!!!

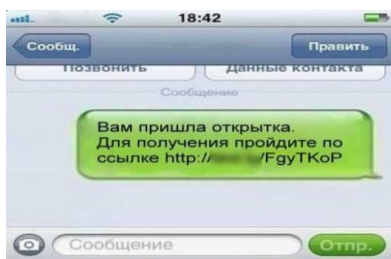
Законным путем с проблемами разобраться возможно только в помещениях органов внутренних дел.



Вам на сотовый телефон приходит СМС-сообщение о том, что Ваша банковская карта заблокирована и необходимо перезвонить по указанному в сообщении номеру.

ЭТО МОШЕННИКИ!!!

В случае сомнений, необходимо звонить по телефону горячей линии, указанному на оборотной стороне Вашей банковской карты.



На Ваш смартфон приходит СМС-сообщение со ссылкой на фотографию (страницу, сайт, документ) в Интернете.

ЭТО МОШЕННИК!!!

Переходя по ссылке, Вы получаете вирус, который передает мошенникам Ваши личные данные, в том числе реквизиты доступа к банковским операциям.

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Управление «К» МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

1. **никому и никогда не сообщать пин-код карты**
2. **выучить пин-код либо хранить его отдельно от карты и не в бумажнике**
3. **не передавать карту другим лицам – все операции с картой должны проводиться на ваших глазах**
4. **пользоваться Только банкоматами не оборудованными дополнительными устройствами**
5. **по всем вопросам советоваться с банком, выдавшим карту**



Сегодня банковские пластиковые карты постоянно используются в повседневной жизни. Они упрощают процесс оплаты, а главное - являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать ПИН-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет. Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Проанализировав все случаи мошенничества такого рода, специалисты Управления «К» МВД России подготовили для Вас понятную и полезную памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать нашим рекомендациям. Они защитят Вас от действий мошенников и сэкономят Ваши средства.



Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает!

Владельцам пластиковых банковских карт

**будьте
осторожны
и внимательны!**

Мошенничества
с пластиковыми картами



пин-код — ключ к вашим деньгам

Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду, как к ключу от сейфа с вашими средствами.

Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё - в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

ваша карта – Только ваша

Не позволяйте никому использовать Вашу пластиковую карту - это всё равно что отдать свой кошелек, не пересчитывая сумму в нём.

ни у кого нет права требовать ваш пин-код

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

помните: хранение реквизитов и ПИН-кода в тайне - это Ваша ответственность и обязанность.

немедленно блокируйте карту случае ее утери

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

пользуйтесь защищёнными банкоматами

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

Использование банкоматов без видеонаблюдения опасно вероятностью нападения злоумышленников.

опасайтесь посторонних

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

банкомат должен быть «чистым»

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

банкомат должен быть полностью исправным

В случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - откажитесь от его использования. Велика вероятность того, что он перепрограммирован мошенниками.

советуйтесь только с банком

Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. Свяжитесь с Вашим банком - он обязан предоставить консультацию по работе с картой.

не доверяйте карту официантам и продавцам

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Тактика борьбы с вредоносными программами

Вредоносные программы представляют собой файлы, которые срабатывают при активировании на компьютере. Тактика борьбы с ними достаточно проста:

- а) не допускать, чтобы вредоносные программы попадали на Ваш компьютер;
- б) если они к Вам все-таки попали, ни в коем случае не запускать их;
- в) если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.

Самый действенный способ оградить от вредоносных программ свой почтовый ящик - запретить прием сообщений, содержащих исполняемые вложения.

расширение файла – это важно!

Особую опасность могут представлять файлы со следующими расширениями:

- ▶ *ade, *adp, *bas, *bat;
- *chm, *cmd, *com, *cpl;
- *crt, *eml, *exe, *hlp;
- *hta, *inf, *ins, *isp; *jse,
- *lnk, *mdb, *mde; *msc,
- *msi, *msp, *mst; *pcd,
- *pif, *reg, *scr; *sct,
- *shs, *url, *vbs; *vbe,
- *wsf, *wsh, *wsc.

Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети.

Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы.

вредоносные программы

способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами.

Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

Управление «К» МВД РФ напоминает: для защиты пользователей от вредоносных программ разработано множество действенных контрмер. Надо лишь знать их и своевременно использовать.



Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает:

Вредоносные программы В Интернете

- Правила поведения в Интернете
- Безопасное использование электронной почты
- Защита от вредоносных программ



Рекомендации по обеспечению безопасной Работы в интернете

1. антивирусные программы –ваши первые защитники

Установите современное лицензионное антивирусное программное обеспечение.

Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

2. обновления – это полезно и безопасно

Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки.

Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления.

Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

3. настройте свой компьютер против вредоносных программ

Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети.

Не забудьте подкорректировать настройки почты, браузера и клиентов других используемых сервисов, чтобы уменьшить риск воздействия вредоносных программ и подверженность сетевым атакам.

4. проверяйте новые файлы

Будьте очень осторожны при получении сообщений с файлами-вложениями.

Обращайте внимание на расширение файла.

Вредоносные файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов.

Подозрительные сообщения лучше немедленно удалять.

Чтобы удалить сообщение в почтовой программе полностью:

- ▶ удалите сообщение из папки «Входящие»;
- ▶ удалите сообщение из папки «Удаленные»;
- ▶ выполните над папками операцию «Сжать» (Файл/Папка/Сжать все папки).

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных веб-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять.

Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

5. будьте бдительны и осторожны

По возможности не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их.

При получении извещений о доставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

6. резервное копирование – гарантия безопасности

Регулярно выполняйте резервное копирование важной информации.

Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

НЕ ДАЙ ОБМАНУТЬ СЕБЯ МОШЕННИКАМ!



1

МОШЕННИКИ ШЛЮТ «ПИСЬМА СЧАСТЬЯ» И ЖДУТ, КОГДА ВЫ ПОПОЛНИТЕ ИХ КОШЕЛЕК СВОИМИ ДЕНЬГАМИ!

НЕ ОТВЕЧАЙТЕ НА ТАКИЕ СМС!!!

- КАРТА ЗАБЛОКИРОВАНА. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- ВЫ ВЫИГРАЛИ АВТОМОБИЛЬ! ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- ПОПОЛНЕНИЕ СЧЕТА НА 20 000 РУБЛЕЙ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- НАПОМИНАЕМ ПОГАСИТЬ ЗАДОЛЖЕННОСТЬ ПО КРЕДИТУ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- МАМА, У МЕНЯ ПРОБЛЕМЫ. ПОТОМ ВСЕ ОБЪЯСНЮ. ПЕРЕВЕДИ 300 РУБЛЕЙ НА ТЕЛ. ХХХХХ.



2

У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН

МОШЕННИКИ ПРЕДЛАГАЮТ ПО АКЦИИ УДВОИТЬ ПЕНСИЮ. ПОМОЧЬ ПОПАВШЕМУ В ДТП ВНУКУ, ВНЕ ОЧЕРЕДИ ПРОЙТИ МЕДИЦИНСКОЕ ОБСЛЕДОВАНИЕ.

НЕ ПЕРЕДАВАЙТЕ И НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЬГИ НЕЗНАКОМЦАМ.

ПРОВЕРЬТЕ ПОСТУПИВШУЮ ИНФОРМАЦИЮ, ПОЗВОНИТЕ РОДСТВЕННИКАМ ИЛИ 02.



3

МОДНЫМ И НАИВНЫМ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯМ ПОСВЯЩАЕТСЯ!



В СОЦИАЛЬНЫХ СЕТЯХ, НА САЙТАХ «АВИТО», «ДРОМ.РУ» ДОВЕРЧИВЫМ ПОКУПАТЕЛЯМ ПРЕДЛАГАЮТ ВНЕСТИ ПРЕДОПЛАТУ ЗА НЕСУЩЕСТВУЮЩИЙ ТОВАР, ОДНАКО В ДАЛЬНЕЙШЕМ СВЯЗЬ С ЛЖЕПРОДАВЦАМИ ПРЕКРАЩАЕТСЯ.

4

РУЧКУ ПОЗОЛОТИ, ВСЮ ПРАВДУ РАССКАЖУ

МОШЕННИКИ ПРЕДЛАГАЮТ ЧУДОДЕЙСТВЕННОЕ ИСЦЕЛЕНИЕ ОТ ПОРЧИ ИЛИ СГЛАЗА. ОДНАКО, ГЛАВНАЯ ИХ ЦЕЛЬ - ЗАВЛАДЕТЬ ВАШИМИ ДЕНЕЖНЫМИ СРЕДСТВАМИ, ЦЕННЫМИ ВЕЩАМИ И СКРЫТЬСЯ. **НЕ ВЕРЬТЕ «ЛЖЕЦЕЛИТЕЛЯМ» И ГАДАЛКАМ!!!**



- При поступлении телефонного звонка из «банка» с сообщением о «подозрительной операции по банковскому счёту», «оформлении третьим лицом кредита на Ваше имя», «несанкционированном списании денежных средств» **помните - это мошенник!** Немедленно прекратите разговор и обратитесь в ближайшее отделение банка для уточнения информации, либо позвоните в организацию по официальному номеру, который указан на оборотной стороне банковской карты.

- Если потенциальный продавец или покупатель просит вас перейти по ссылке, якобы для оформления «безопасной сделки или доставки», или же под предлогом «зачисления денег на карту», «оплаты покупки» **помните - это мошенник!** Внимательно изучите информацию о «безопасной сделке» или «безопасной доставке» на официальном сайте торговой площадки, прежде чем совершить необдуманные операции!

- Не сообщайте никому, в том числе по телефону даже «роботу» или по «роботизированной линии» свои данные, данные банковских карт и коды из SMS-сообщений.

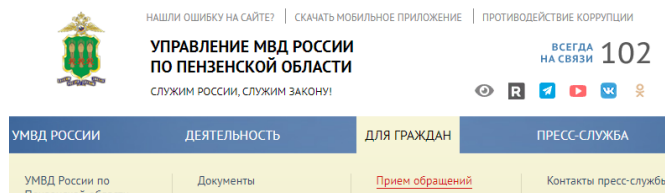
- Не устанавливайте на свои мобильные устройства приложения по просьбе незнакомых Вам лиц.

- При совершении покупок и продаж в сети Интернет внимательно изучите информацию о «продавце» или сайте в сети Интернет, не сообщайте и не указывайте дополнительные данные своих банковских карт, не проводите операции через банкомат по указанию незнакомых Вам лиц, воздержитесь от полной или частичной оплаты посредством перевода и совершайте сделки только «из рук в руки».

- При поступлении сообщения от близкого родственника, друга или просто знакомого с просьбой о помощи, в том числе занять денежные средства, необходимо самостоятельно перепроверить информацию, позвонив на номер телефона человека, и убедиться в необходимости осуществления финансовой операции.

КУДА СООБЩАТЬ О ПРЕСТУПЛЕНИИ

Если вы стали жертвой мошенников или столкнулись с мошенническими действиями, незамедлительно обращайтесь в ближайшее отделение полиции или сообщайте в полицию по телефону «02», с сотового «102». Также для направления обращений, заявлений о правонарушениях или преступлениях возможно использовать сервис «Прием обращений» на официальном сайте УМВД России по Пензенской области - <https://58.мвд.рф/>



ВНИМАНИЕ!
Будьте бдительны,
не поддавайтесь на провокации мошенников.

Зачастую граждане, зная об основных видах и способах телефонного и Интернет мошенничества, попадают на уловки злоумышленников, которые убеждают сообщить им конфиденциальную информацию, оперируя знаниями о личных данных.

Главное помнить:

Мошенники могут обладать информацией о некоторых данных Вашего паспорта, месте жительства, детализации по банковскому счёту, платежах по кредиту, о некоторых данных Вашей банковской карты, кодовом слове. Не поддавайтесь на провокации мошенников!

Будьте бдительны! Не дайте себя обмануть! Поделитесь информацией со своими близкими!



УМВД России по Пензенской области

ОСТОРОЖНО!!!
ТЕЛЕФОННЫЕ И
ИНТЕРНЕТ
МОШЕННИКИ!



СОХРАННОСТЬ ВАШИХ ДЕНЕГ – ТОЛЬКО
В ВАШЕЙ КОМПЕТЕНЦИИ

г. Пенза

Основные виды и способы преступлений, совершаемых с использованием IT-технологий:

«Лжесотрудник банка»

Наиболее распространённым способом обмана остается схема, при которой гражданину звонит неизвестный, представляется работником банка или службой безопасности банка, и предупреждает о якобы несанкционированной попытке или списании денежных средств, оформлении третьими лицами кредита на имя жертвы или совершения подозрительных операций по счетам. После чего, якобы для сохранности финансов, или же отмены подозрительных операций, мошенники просят сообщить им или «роботу» («роботизированной линии») реквизиты банковских карт, защитный код на оборотной стороне карты, состоящий из трех или четырех цифр, а также коды подтверждения операций из SMS-сообщений. Иногда мошенники убеждают граждан пройти до ближайшего банкомата и осуществить перевод денежных средств на «безопасный счёт» или «безопасную ячейку» банка. В некоторых случаях злоумышленники предлагают установить на телефон программу безопасности для мобильного банка, которая на самом деле является программой удаленного доступа, и, получая доступ к мобильному банку на мобильном устройстве жертвы, похищают денежные средства.

«Ложный покупатель»

Другой схемой обмана остается хищение денежных средств при осуществлении продажи товаров через популярные торговые площадки сети Интернет. Зачастую, граждане, которые решили продать свои личные вещи, или же различные предметы, сталкиваются с таким видом мошенничества, при котором потенциальный покупатель (он же мошенник) поясняет, что он из другого города, или даже области, и просит отправить ему товар службой доставки, оформив «безопасную доставку» или же «безопасную сделку», и для этого предлагает перейти по ссылке, которую отправляет в мессенджере или по электронной почте. Перейдя по ссылке, потерпевшие попадают на «фейковую» страницу, которая визуально схожа с официальным сайтом торговой площадки, или платёжной системы. На поддельной странице предлагается ввести полные реквизиты банковской карты, чтобы якобы получить деньги за товар, оплатить

покупку или доставку. Если человек введет полные данные карты, включая трехзначный код с обратной стороны, то мошенник сможет украсть деньги с его счета. Также «ложный покупатель» может попросить сообщить ему номер карты, а также трёхзначный код, расположенный на оборотной стороне банковской карты и код подтверждения операции из SMS-сообщения, якобы необходимые ему для зачисления на

Вашу карту денежных средств, а в действительности произойдет списание Ваших финансов.

«Ложный продавец»

Иногда потерпевшие «на доверии» или «на честном слове» переводят деньги в счет оплаты товара или услуги, объявление о продаже которого они нашли в Интернете, в результате чего не получают оплаченный товар, а продавец перестает выходить на связь. Или же продавец отправляет посылку, в которой содержится товар, не соответствующий заявленному.

«Займи-помоги»

Не менее распространённым способом обмана является мошенничество в социальных сетях, при котором, злоумышленник, получив доступ к странице пользователя, от его имени, под различными предлогами, просит у Вас занять денежные средства, и рассылает данное сообщение всему списку «друзей». Граждане, которым приходит данная просьба от «друга», не перепроверяют информацию и осуществляют переводы на указанные им номера и счета, в результате чего становятся жертвами мошенников.

«Фальшивое знакомство»

В связи с участившимися случаями стоит отметить мошенничество, при котором молодые люди знакомятся в социальных сетях и различных сайтах знакомств с якобы девушками, которые в процессе переписки, предлагают совместный поход в кино/театр, или же посидеть в уютной домашней обстановке, наслаждаясь суши или пиццей. Далее, злоумышленники присылают ссылку на «фейковый» сайт (театр, кино, служба доставки суши и пиццы) и завлеченные знакомством граждане совершают покупки билетов на несуществующие сеансы кино и спектакли, или же оплачивают доставку мнимой еды, указывая реквизиты

своих банковских карт на мошеннических страницах, после чего лишаются всех денежных средств, которые находятся на их счетах.

«Родственник в беде»

Данный вид телефонного мошенничества по-прежнему имеет место быть и заключается в том, что Вам поступает звонок с неизвестного номера и незнакомец представляется сотрудником правоохранительных

органов. Далее злоумышленник сообщает, что Ваш близкий человек задержан и в настоящее время принимается решение о привлечении его к уголовной или же административной ответственности. Могут указываться разные причины (ДТП, незаконное хранение оружия, совершенное убийство, обнаружение наркотиков, нанесение телесных повреждений другому лицу и т.п.). Затем мошенник передает трубку якобы близкому человеку, который взволнованным, нечетким голосом или шёпотом сообщает, что попал в беду.

Телефон при этом якобы передается сотруднику правоохранительных служб, который предлагает свою помощь в этой ситуации за денежное вознаграждение. Если жертва соглашается, то звонящие сообщают место, куда необходимо привезти деньги или передать «курьеру». Иногда деньги просят перевести на номер телефона или по номеру карты.

«Ложный выигрыш или выплата»

Зачастую, пользователи Интернета получают сообщения, уведомления или рекламу, о том, что именно они стали победителем в розыгрыше, и им положен выигрыш. Или же гражданам полагается большая выплата и поддержка. Далее, для получения денежных средств, предлагается перейти по ссылке и указать свои данные и реквизиты карты, якобы для расчета положенной суммы. Указывая данные банковских карты, граждане прощаются со своими деньгами, так и не получив обещанные денежные средства.



Наиболее распространенные схемы телефонного мошенничества

обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сын» и т.п.

Телефонный номер-«грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

выигрыш в лотерею, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

простой код от оператора связи: предложение услуги или другой выгоды - достаточно ввести код, который на самом деле спишет средства с Вашего счёта.

штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.

ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

Телефонное мошенничество известно давно - оно возникло вскоре после массового распространения домашних телефонов.

В настоящее время, когда личный номер мобильного телефона может быть у любого члена семьи, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества множатся с каждым годом.

В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях.

Мошенники разбираются в психологии и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении.

Управление «К» МВД РФ напоминает, что чаще всего в сети телефонных мошенников попадают пожилые люди или доверчивые подростки. При этом **каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.**



Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает:

телефонные мошенники

Телефонные мошенники используют мобильные телефоны для обмана и изъятия денежных средств граждан.

- основные схемы
- тактика мошенников
- как реагировать



тактика телефонных мошенников

Для общения с потенциальной жертвой мошенники используют либо SMS, либо телефонный звонок.

SMS - это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме - в надежде на доверчивого получателя.

Телефонный звонок позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом.

цель мошенников – заставить вас передать свои денежные средства «добровольно». Для этого используются различные схемы мошенничества.

Изъятие денежных средств может проходить разными способами. Вас попытаются заставить:

- 1. передать деньги из рук в руки или оставить в условленном месте;**
- 2. приобрести карты экспресс-оплаты и сообщить мошеннику коды карты;**
- 3. перевести деньги на свой счёт и ввести специальный код;**
- 4. перевести деньги на указанный счёт;**
- 5. позвонить на специальный телефонный номер, который окажется платным, и с вашего счёта будут списаны средства;**

как правильно реагировать на попытку вовлечения в мошенничество

Мошенники очень хорошо знают психологию людей.

Они используют следующие мотивы:

- а.** Беспокойство за близких и знакомых.
- б.** Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.
- в.** Желание выиграть крупный приз.
- г.** Любопытство - желание получить доступ к SMS и звонкам других людей.

Чтобы противодействовать обману, достаточно знать о существовании мошеннических схем и в каждом случае, когда от Вас будут требовать перевести сумму денег, задавать уточняющие вопросы.

Телефонные мошенники рассчитывают на доверчивых, податливых людей, которые соглашаются с тем, что им говорят, и выполняют чужие указания. Спокойные, уверенные вопросы отпугнут злоумышленников.

что надо знать, чтобы не стать жертвой телефонных мошенников

Если Вы сомневаетесь, что звонивший действительно ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

Помните, что никто не имеет права требовать коды с карт экспресс-оплаты!

Оформление выигрыша никогда не происходит только по телефону или Интернету. Если Вас не просят приехать в офис организатора акции с документами - это мошенничество.

Не ленитесь перезванивать своему мобильному оператору для уточнения правил акции, новых тарифов и условий разблокирования якобы заблокированного номера.

Для возврата средств при якобы ошибочном переводе существует чек. Не возвращайте деньги - их вернет оператор.

Услуга «узнайте SMS и телефонные переговоры» может оказываться исключительно операторами сотовой связи и в установленном законом порядке.

есть несколько простых правил:

- ▶ отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;
- ▶ не реагировать на SMS без подписи с незнакомых номеров;
- ▶ внимательно относиться к звонкам с незнакомых номеров.

