Всероссийская просветительская Эстафета по финансовой грамотности.
Этап — **«Финансовая безопасность для всей семьи: защити свои деньги»**

Минфин России

мои финансы

ЗАЩИТИТЕ СВОИ ДЕНЬГИ!

7 базовых правил финансово-цифровой безопасности, которые помогут вам защитить свои данные и деньги, независимо от того, какую схему решат использовать злоумышленники.

1 Не сообщайте коды из СМС-сообщений — никому и никогда

Код из СМС — часть системы двухфакторной аутентификации, которая защищает доступ к вашим персональным данным и банковским счетам.

2 Не совершайте финансовые операции по инструкции от незнакомых, кем бы они ни представлялись

Незнакомцы могут предлагать схемы, направленные на кражу ваших денег.

3 Остерегайтесь фишинга

Будьте внимательны к сайтам, которые требуют вводить личные данные.

4 Не используйте публичный Wi-Fi, когда заходите в важные для вас аккаунты

Ваши логины, пароли и другая личная информация могут оказаться в руках преступников.

5 Не возвращайте деньги, присланные по ошибке неизвестными

Такие переводы могут быть связаны с мошенническими схемами.

6 Не спешите реагировать на тревожные звонки и сообщения

Мошенники манипулируют эмоциями, которые притупляют бдительность.

7 Не делитесь персональными данными с посторонними

Не сообщайте свои пароли, PIN-коды, данные банковских карт, паспортные данные и другую конфиденциальную информацию.

На портале **моифинансы.рф** рассказываем больше про финансово-цифровую безопасность →

Всероссийская просветительская Эстафета по финансовой грамотности.
Этап — **«Финансовая безопасность для всей семьи: защити свои деньги»**

Минфин России

мои финансы

КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА!

Аферисты постоянно находят новые способы украсть деньги или личные данные. Но какими бы хитрыми ни были их схемы, есть пять признаков, по которым легко их разоблачить.

Признак 1

НА ВАС ВЫХОДЯТ САМИ

У мошенников много личин. Помните, что инициатору контакта всегда от вас что-то нужно.

Признак 2

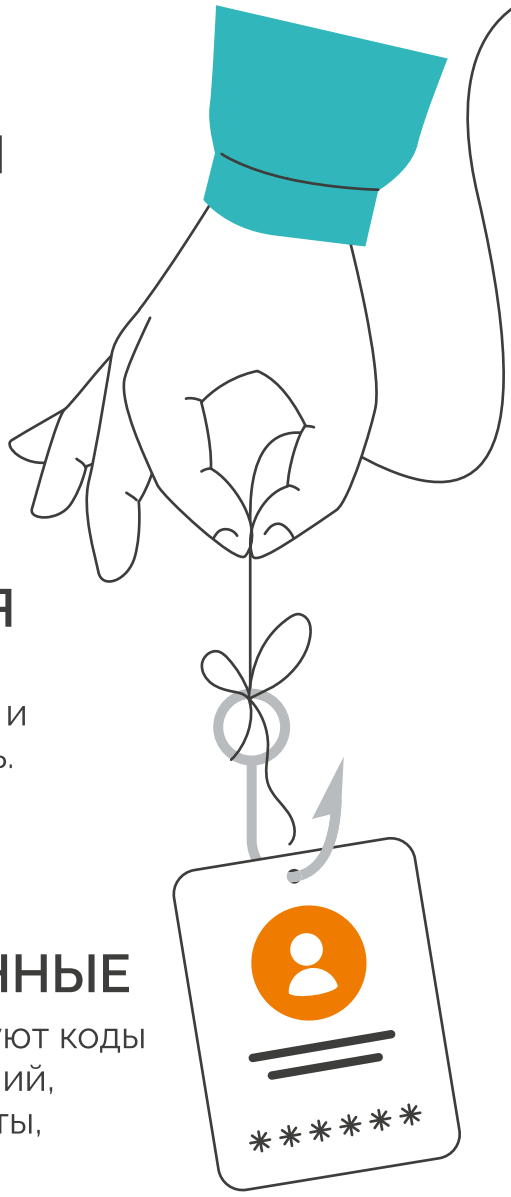
ВАС ВЫВОДЯТ ИЗ РАВНОВЕСИЯ

Радуют или пугают, чтобы сбить вас с толку и притупить бдительность.

Признак 3

ВАС ПРОСЯТ СООБЩИТЬ ДАННЫЕ

Преступников интересуют коды из СМС, пуш-уведомлений, данные банковской карты, персональные данные.



Признак 4

ВАС ТОРОПЯТ

Преступникам важно, чтобы вы действовали импульсивно.

Признак 5

ВАШИ ВОПРОСЫ ИГНОРИРУЮТ

Мошенник будет стараться следовать своему сценарию.

На портале
моифинансы.рф

рассказываем больше про финансово-цифровую безопасность

ВНИМАНИЕ! Кладите трубку в разговоре с незнакомцем, если распознаете хотя бы два из этих признака. Помните, что цель любой схемы мошенников — получить от жертвы сведения, достаточные для доступа к ее деньгам. БУДЬТЕ ВНИМАТЕЛЬНЫ И ОСТОРОЖНЫ!

Всероссийская просветительская Эстафета по финансовой грамотности.
Этап — **«Финансовая безопасность для всей семьи: защити свои деньги»**

Минфин России

мои финансы

КАК НАУЧИТЬ РЕБЕНКА ЗАЩИЩАТЬСЯ ОТ ОНЛАЙН-МОШЕННИКОВ

10 важных рекомендаций родителям

1 Сделайте разговоры с ребенком о мошенниках регулярными

Обсудите реальные случаи мошенничества, спрашивайте, как бы ребенок действовал в этих ситуациях. Это поможет донести, что риск быть обманутым в интернете выше, чем кажется.

2 Изучите сами как мошенники обманывают детей

Распознать мошенника легче, когда знаешь, как он действует.

3 Расскажите, что такое личные данные и почему их надо хранить в секрете

Реквизиты карты, пароли, коды для подтверждения операций — перехватив их, мошенник может лишить семью финансов.

4 Убедитесь, что ребенок пользуется проверенными приложениями и сайтами

Это важно, чтобы избегать фишинговых ресурсов.

5 Объясните, как безопасно делать денежные переводы

Переводы по номеру телефона безопаснее, чем по номеру карты. При отправке средств со счета одного банка на карту другого не видно имя владельца карты.

6 Подключите карту ребенка к своему счету

Так вы быстро заметите подозрительные покупки и переводы.

7 Помогайте ребенку искать подработку в интернете

За обещаниями легких и быстрых денег могут стоять преступные схемы, которые родителям легче распознать.

8 Обсуждайте с ребенком его виртуальных друзей

Притворяться в интернете другим человеком гораздо проще, чем в реальной жизни.

9 Обозначьте правило: если кто-то в интернете просит деньги, нужно убедиться, что это не мошенник

Даже если сообщение пришло от друзей и знакомых.

10 Чаще говорите с ребенком о финансах в целом

Так он быстрее поймет ценность денег.

На портале **моифинансы.рф** рассказываем больше про финансово-цифровую безопасность

ПОМНИТЕ! Финансовая безопасность ребенка в интернете — это процесс воспитания. Поддерживайте с ними открытость и доверие!

Эстафета Мои финансы

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**

ГАЙД

ТОП-5 САМЫХ АКТУАЛЬНЫХ СХЕМ ТЕЛЕФОННЫХ МОШЕННИКОВ

СХЕМА 1. Меняем медицинский полис

Мошенник под видом сотрудника страховой компании сообщает, что у вас истек срок действия медицинского полиса. Документ нужно заменить. Для этого назовите код из смс, который придет на телефон.

***Работники страховых компаний не просят** устанавливать приложения или называть им коды из смс и данные. А медицинский полис действует бессрочно, и его не нужно менять.*

СХЕМА 2. Вам цветы, примите доставку!

Мошенник под видом курьерской службы сообщает, что вам отправили букет, уточняет, куда и когда его привезти. После получения букета курьер просит назвать код из смс, чтобы подтвердить доставку заказа.

***Курьерские службы не просят** коды из смс для подтверждения доставки. Свяжитесь с отправителем подарка и уточните детали. Если это сделать не удается — не принимайте презент.*

СХЕМА 3. Получите письмо!

Мошенник под видом сотрудника «Почты России» сообщает, что вам пришла посылка/заказное письмо. Для его получения надо воспользоваться несуществующим чат-ботом и ввести код из смс.

***Сотрудники «Почты России» никогда не звонят** клиентам и не запрашивают код из смс. Вы можете самостоятельно подключить или отказаться от услуг сервиса на его официальном сайте или в приложении.*

Подробнее на портале **моифинансы.рф**

СХЕМА 4. Заканчивается договор сотовой связи

Мошенник под видом оператора сотовой связи сообщает, что у вас заканчивается контракт на мобильную связь. Его нужно продлить, иначе вы не сможете звонить, отправлять смс и пр. Это можно сделать через «Госуслуги»: просто продиктуйте код из смс.

***Сотрудники оператора могут отключить связь,** если вы не оплачиваете услуги или ваши персональные данные, указанные в договоре, необходимо актуализировать. Но это произойдет не сразу. Вы можете обновить данные не только через «Госуслуги», но в салоне связи.*

СХЕМА 5. Зафиксирована подозрительная операция по вашей карте!

Мошенник под видом сотрудника банка сообщает, что по вашей карте зафиксирован подозрительный перевод или кто-то пытается оформить кредит на ваше имя. Для отмены этих финансовых операций вы должны назвать код из смс, который направит специалист.

***Сотрудники банков, правоохранительных органов и государственных ведомств не звонят** гражданам и не запрашивают у них персональные данные, коды из сообщений. Положите трубку и позвоните в организацию, по номеру с ее официального сайта.*

БУДЬТЕ БДИТЕЛЬНЫ! Если вас просят назвать код из СМС, не поддавайтесь на уговоры. Мошенники могут придумывать разные предлоги, чтобы выманить его. Этот код дает доступ к вашим персональным данным и банковским счетам.

Эстафета Мои финансы

Минфин России

мои финансы

Всероссийская просветительская Эстафета по финансовой грамотности

Этап: **«Финансовая безопасность для всей семьи: защити свои деньги»**

ГАЙД

ТОП-5 САМЫХ АКТУАЛЬНЫХ ИНТЕРНЕТ-СХЕМ МОШЕННИКОВ

СХЕМА 1

Вам открытка!

Мошенники маскируют вредоносный код под открытку или картинку и рассылают ее по электронной почте. При нажатии на них пользователь скачивает на гаджет вирусную программу, которая похищает его персональные данные.

***Не доверяйте** сообщениям от неизвестных людей. Если вы знаете отправителя, с настороженностью отнеситесь к нестандартным сообщениям, в том числе с вложением фото или картинки без предпросмотра. Уточните у него через другой способ связи, что во вложении.*

СХЕМА 2

Очень выгодное предложение!

Мошенники подделывают сайт маркетплейса и присылают пользователю на почту электронное письмо с промокодом на определенную сумму. Для его получения нужно перейти на сайт, там добавить товары в корзину, ввести реквизиты банковской карты, а подаренная сумма якобы зачтется.

***Не переходите** по ссылкам из электронных писем. Проверяйте акции, промокоды и другую информацию на официальном сайте интернет-магазинов.*

СХЕМА 3

Инвестиционный проект с высоким доходом

Лжеброкеры рассылают письма на электронную почту с рекламой крупного инвестиционного проекта. При минимальных вложениях они обещают высокий доход в ближайшее время.

***Не верьте** обещаниям про легкое и быстрое обогащение! Прежде чем вложить деньги в такой проект, соберите информацию о нем, прочитайте отзывы, уточните контакты брокерской компании.*

СХЕМА 4

Предлагаем работу!

Мошенники публикуют объявления об удаленной работе. Условия привлекательные, зарплата высокая. Они предлагают человеку оформить банковскую карту на свое имя и передать ее курьеру, получить деньги на собственную банковскую карту, часть передать доверенному лицу или перевести кому-то, а вознаграждение оставить себе или стать администратором лотереи и рассылать победителям выигрыши. Подобные предложения — замаскированная схема дропперства.

***Не соглашайтесь** на сомнительные предложения о легком заработке. Помните, что, участвуя в такой схеме, вы становитесь участником преступления и несете уголовную ответственность.*

СХЕМА 5

Получите выплату!

Мошенники под видом специалиста портала «Госуслуги» или СФР рассылают письма на электронную почту и сообщают пользователю о назначении дополнительной выплаты. Для ее получения необходимо перейти по ссылке, ввести паспортные данные и указать реквизиты банковской карты, на которую переведут деньги.

***Внимательно проверяйте** адрес отправителя электронного письма. Помните, что информация о выплатах и льготах отображается в личном кабинете на «Госуслугах». Не переходите по ссылкам из подобных писем и не оставляйте свои данные на сомнительных ресурсах.*

Подробнее на портале **моифинансы.рф**

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 сберегут 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 кошелёк, 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 В 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.

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, в 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 ВРЕДОНОСНЫЕ ПРОГРАММЫ (ЧЕРВИ, ТРОЯНЫ)

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

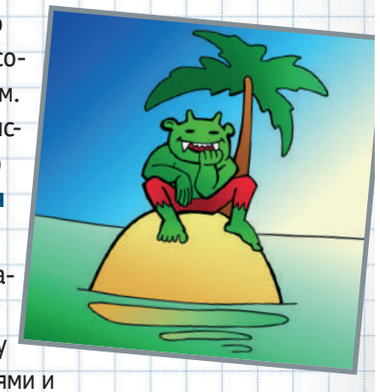
Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- **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 (ТРОЛЛЬ, 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.

САЙТ-ДУБЛЁР –

это сайт, который внешне на 99% повторяет настоящий сайт благотворительной организации или активиста, собирающего средства на доброе дело.

Отличия сайта-дублёра от оригинального минимальны: одна или две буквы в доменном имени сайта (имени, которое указано в адресной строке браузера) и другой номер счёта, куда перечисляют средства.

Изготовить такой сайт-дублёр очень просто: он может появиться в самое кратчайшее время после публикации настоящего – оригинального сайта. Поэтому мошенники всё чаше прибегают к этой схеме обмана.

На сегодняшний день Интернет является очень эффективным инструментом для использования его в благотворительных целях.

Развитие электронных кошельков и расширение возможностей по перечислению денежных средств, упрощает участие в благотворительной деятельности для каждого пользователя Интернета.

Одновременно злоумышленники приспособились использовать сбор средств на благотворительных сайтах в своих мошеннических схемах.

Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает!

ПОЛЬЗОВАТЕЛЯМ ИНТЕРНЕТА

Будьте осторожны!

МОШЕННИЧЕСКОЕ
ДУБЛИРОВАНИЕ
БЛАГОТВОРИТЕЛЬНЫХ
САЙТОВ

КАК ОРГАНИЗОВАНО МОШЕННИЧЕСТВО:

Вы узнаёте о трагической ситуации, в которой требуется помощь.

Достаточно зайти на некий сайт и перевести деньги на указанные реквизиты.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Злоумышленники отслеживают социальную ситуацию и активно используют темы, которые являются заведомо выигрышными с точки зрения возможных откликов граждан.

Тематика благотворительных сайтов может быть самой разной:

- помощь больным детям – сбор средств на операцию;
- помощь жертвам терактов;
- помощь пострадавшим во время стихийных бедствий – землетрясений, цунами, сходов лавин и оползней;
- восстановление храмов;
- помощь приютам, заботящимся о брошенных животных.

Для осуществления своих противоправных замыслов мошенники создают сайты-дублеры, которые являются точной копией официальных сайтов с той лишь разницей, что на них указаны другие расчетные счета, по которым гражданам предлагается направлять денежные средства.

Учащаются случаи создания полностью выдуманных историй, созданных на основе правдивых.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Не поленитесь перепроверить информацию в Интернете.

Ей можно будет доверять только в том случае, если на нескольких сайтах будет указан один и тот же расчетный счет и номер телефона.

Если вы планируете постоянно участвовать в благотворительной деятельности, используйте сайт, принадлежащий благотворительной организации или группе активистов. Помогайте тем, кто даёт информацию «из первых рук» и известен своей надёжной репутацией.

Посмотрите, указан ли на сайте номер телефона для связи.

Если да, то следует позвонить по нему и уточнить все детали. Например, если необходимы деньги на операцию ребенку, спросите о диагнозе, узнайте имя лечащего врача, номер больницы, в которой наблюдается ребенок и т.д.

Задавайте как можно больше уточняющих вопросов: если на другом конце провода вам не смогут ответить на поставленные вопросы, либо ответы будут уклончивыми и неуверенными, или ответы вообще не будут совпадать с тем, что указано на сайте, то, скорее всего, вы общаетесь с мошенниками.

Зачастую мошенники вообще не указывают никаких телефонных номеров, чтобы их было сложнее вычислить.

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», «сынок» и т.п.

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

Выигрыш в лотерее, 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 попадаются 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.