

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 чаще 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 узнаете 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-дублиеры, 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», «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 неизвестных номеров;
- ▶ внимательно относиться к звонкам с неизвестных номеров.

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 web-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 обращайтесь 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.