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.



Южная транспортная прокуратура

Назрановская транспортная прокуратура

Адрес: 386100, Россия, Республика Ингушетия, г. Назрань, улица Победы, 3;
Контактные телефоны: +7 (8732) 22-27-82, +7 (8732) 22-27-92; E-mail: nazran_prok@donpac.ru

Официальный сайт: https://epp.genproc.gov.ru/web/utp

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В СЕТИ-ИНТЕРНЕТ

Будьте осторожны!



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.



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 при - нять меры, чтобы, по возможно - сти, 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:

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 дей - ствует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы.

ВРЕДОНОСНЫЕ ПРОГРАММЫ

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

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

напоминает: для защиты пользователей от вредоносных программ разработано множество действенных контрмер. Надо лишь знать их и своевре - менно использовать.



Южная транспортная прокуратура

Назрановская транспортная прокуратура

Адрес: 386101, Россия, Республика Ингушетия, г. Назрань, улица Победы, 3; Контактные телефоны: +7 (8732) 22-27-82, +7 (8732) 22-27-92; E-mail: nazran_prok@donpac.ru

Официальный сайт:

https://epp.genproc.gov.ru/web/utp

"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.



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 недоставке 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.