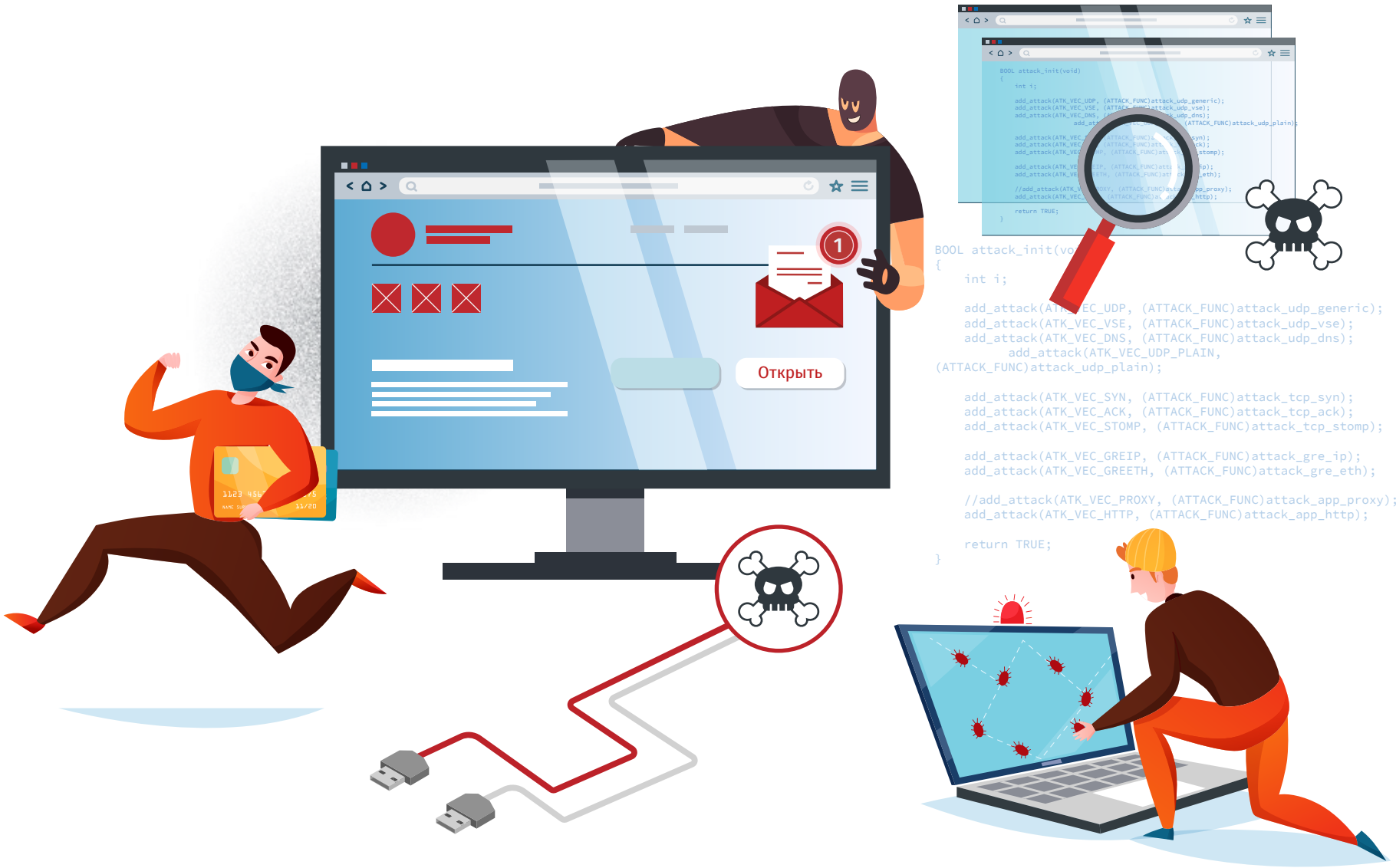
Digital Security

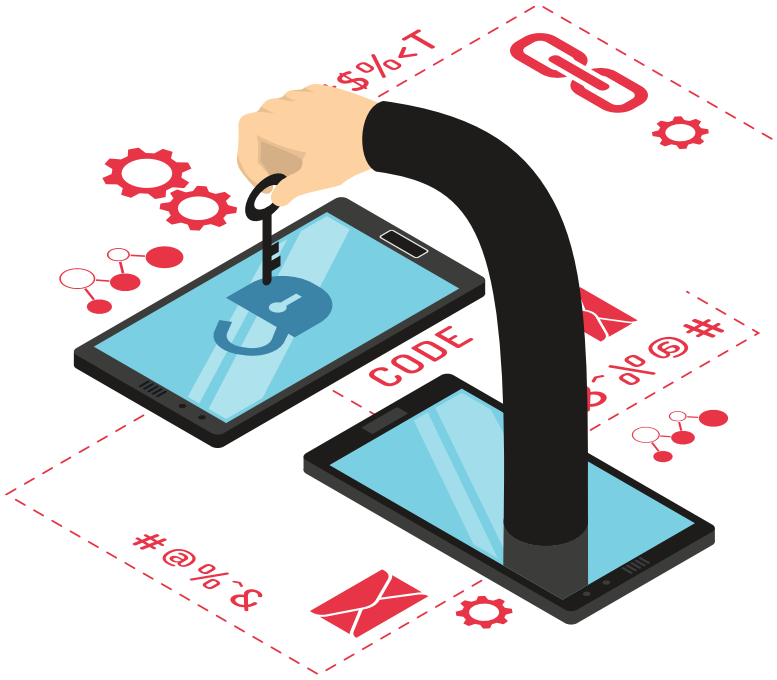
Опасность вредоносов и как от них защититься



Тема вредоносов, заражающих наши устройства, не теряет актуальности. Заражение обычно ведёт к финансовым потерям. **Программы-вымогатели угрожают раскрыть конфиденциальную информацию** или вносят изменения на устройстве, например, шифруют данные, а затем требуют деньги для их отмены. Также **вирусы могут получить данные банковских карт пользователя и вывести средства** со счетов самостоятельно. И это лишь малая часть возможностей вредоносов.

Иногда для заражения компьютера не требуется никаких действий со стороны человека. Так сетевые черви могут заражать устройства автоматически при наличии в устройстве определённой уязвимости. Однако в большинстве случаев это всё же «совместный проект» беспечного пользователя и хитроумной программы.

Мы подготовили ряд советов, которые помогут уберечься от программ-вымогателей.

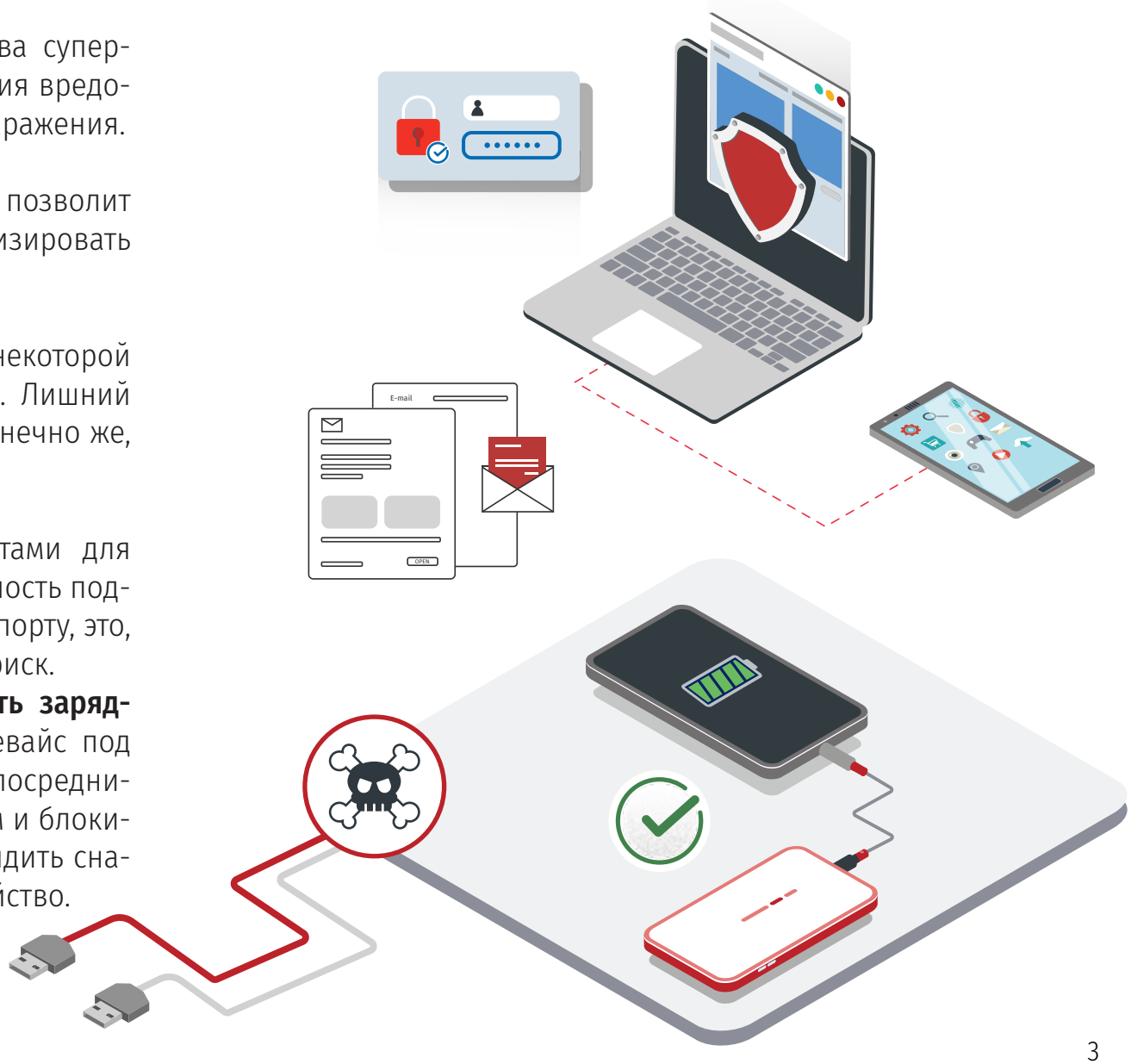


Не получайте на своём устройстве права суперпользователя. Это повысит риск заражения вредоносом и усугубит последствия в случае заражения.

>>> Настройте **резервное копирование.** Это позволит сохранить ценные данные и минимизировать потери в случае заражения.

>>> Установите на компьютер антивирус и с некоторой периодичностью проверяйте устройство. Лишний раз подчеркнём, что устройства Apple, конечно же, тоже подвержены вирусам.

>>> С осторожностью пользуйтесь USB-портами для зарядки в общественных местах. Возможность подключить телефон к питанию, сидя в аэропорту, это, конечно, благодать, но и определённый риск.
Злоумышленник может модифицировать зарядную станцию. Некоторые используют девайс под названием USB-condom, он выступает посредником между портом зарядки и устройством и блокирует передачу данных. Ещё вариант: зарядить сначала пауэрбанк, а уже от него своё устройство.

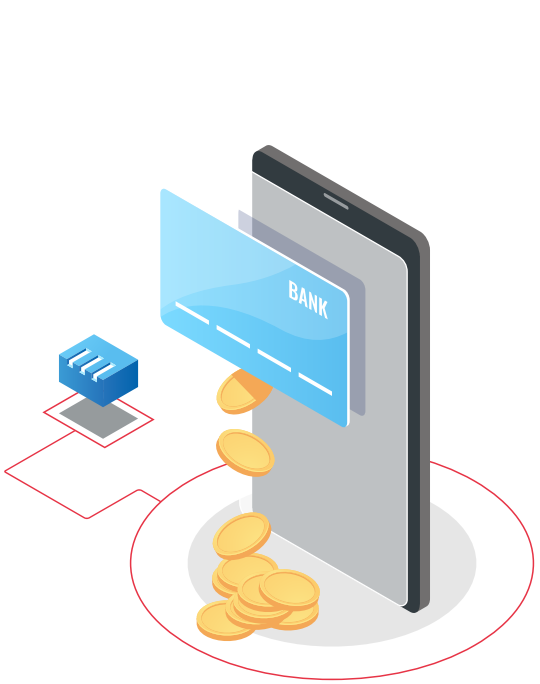


Своевременно устанавливайте обновления для операционной системы и приложений, но исключительно из доверенных источников.

>>> Скачивать приложения на рандомных сайтах и форумах – большой риск. Прежде чем добавить приложение в Play Маркет, Google проверяет, нет ли в нем зловредного кода. То же самое и с другими официальными магазинами приложений. К сожалению, даже это не стопроцентная гарантия, поэтому всегда **читайте разрешения и смотрите рейтинг перед установкой приложения.**

>>> Если крайне необходимо установить что-то от неизвестного источника, проверьте файл, например, здесь **virustotal.com** или антивирусом. По ссылке также можно проверить сомнительный сайт.

>>> Плагины для браузеров могут как улучшить пользовательский опыт, так и стать источником проблем. Не так давно в Chrome Web Store **выявили** 111 вредоносных расширений, занимавшихся сбором конфиденциальных данных пользователей. В общей сложности они были загружены 32 962 951 раз. Опять-таки не ленитесь почитать отзывы.

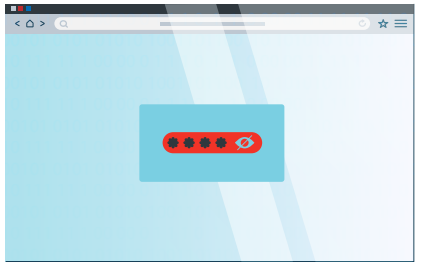


Не переходите по ссылкам из СМС и ММС сообщений, а также в мессенджерах и соцсетях. Особенно если сообщение пришло от неизвестного отправителя.

>>> Будьте аккуратны со всплывающими рекламными окнами. На них можно нечаянно нажать, чего и добиваются злоумышленники. Для защиты можно поставить блокировщики рекламы.

>>> Следите за безопасностью электронной почты. **Вредонос может быть как во вложении, так и по ссылке в письме.** Поэтому письма от неизвестных отправителей лучше вообще не открывать. Касается это, конечно, не только компьютеров, вредонос в письме может быть опасен и для смартфона.

Мы подготовили отдельный **гид по безопасности электронной почты.** Проверьте, всем ли рекомендациям вы следуете.



Спасибо, что уделили внимание вопросам безопасности. Следуйте этим простым советам, развивайте здоровый скептицизм и не бойтесь видеть опасность там, где её может и не быть.

Свяжитесь с нами

inbox@dsec.ru

7 (495) 223-07-86