Kaspersky® Academy

Образовательные программы
«Лаборатории Касперского»

KASPERSKY lab

Компьютерная безопасность:
МИФЫ И РЕАЛЬНОСТЬ

МИФ 1

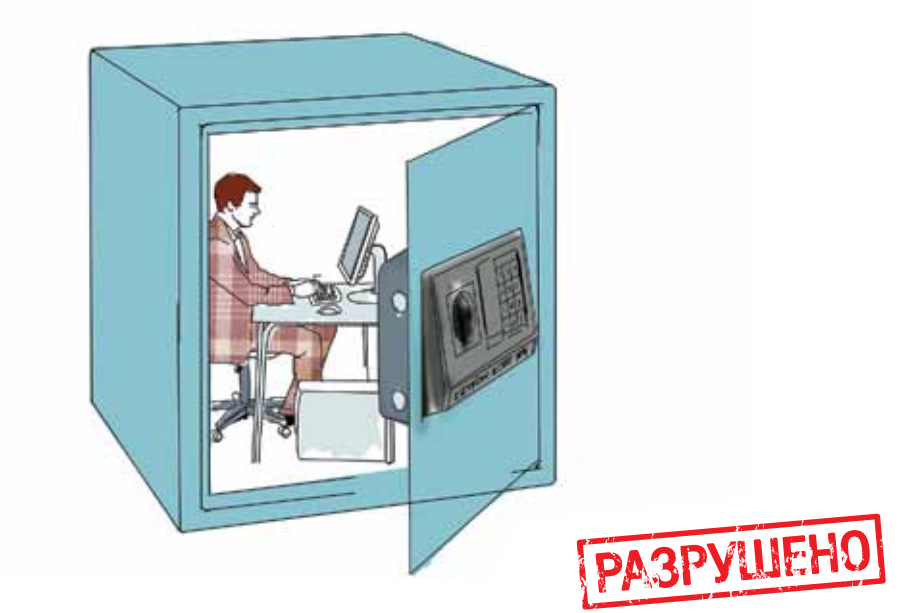
Мой компьютер не нужен злоумышленникам

РАЗРУШЕНО

Для того чтобы стать мишенью киберпреступников, достаточно просто иметь компьютер, подключенный к интернету. Даже, если вы не покупаете ничего в интернет-магазинах и не пользуетесь системами интернет-банкинга и платными сервисами, ваш компьютер может быть использован злоумышленниками для спам-рассылок и различных сетевых атак на другие компьютеры, для распространения вредоносных программ, запуска программ для перебора паролей с целью взлома чужих учетных записей, показа рекламы и накрутки счетчиков на интернет-сайтах, для кражи ваших учетных записей на интернет-ресурсах и в онлайн-играх с целью продажи, а также иных противоправных действий. Если ваш компьютер окажется заражен, могут пострадать люди, с которыми вы ведете переписку, получив вместе с вашим письмом вредоносную программу.

МИФ 2

Надежная антивирусная программа гарантирует абсолютную защиту от всех видов киберугроз



РАЗРУШЕНО

Современные системы безопасности обеспечивают высокий уровень защиты от многих видов интернет-угроз, но даже самые продвинутые защитные системы бессильны против методов социальной инженерии (атак, прово-димых с помощью обмана и хитрости, когда беспечный пользователь сам отправляет пароли злоумышленнику или отключает антивирусную программу, попавшись на удочку мошенников).

Для надежной защиты от киберугроз необходимо выполнение двух условий:

1 Современная техническая защита с обновлением антивирусных баз как минимум раз в сутки.

2 Знание основ компьютерной безопасности и осторожность.

МИФ 3

Антивирусные программы не нужны — провайдеры автоматически проверяют передаваемые данные на наличие вредоносных программ

РАЗРУШЕНО

Провайдеры действительно занимаются фильтрацией трафика, однако этого недостаточно для защиты персонального компьютера. Каждому пользователю следует иметь на своем компьютере свою защитную систему.

МИФ 4

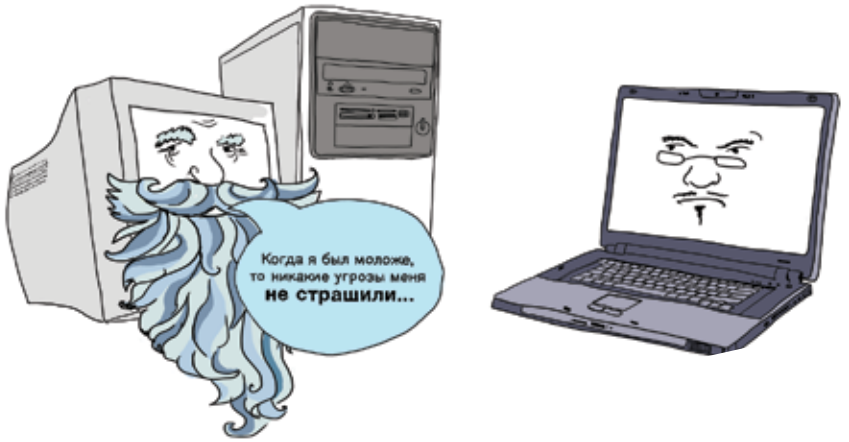
Новый вирус — большая редкость

РАЗРУШЕНО

Вирусописатели постоянно совершенствуют свои творения, чтобы те могли беспрепятственно обойти антивирусные программы, поэтому новые модификации вредоносных программ – явление обыденное.

МИФ 5

Если у меня ранее не было проблем с безопасностью, значит, их не будет в будущем

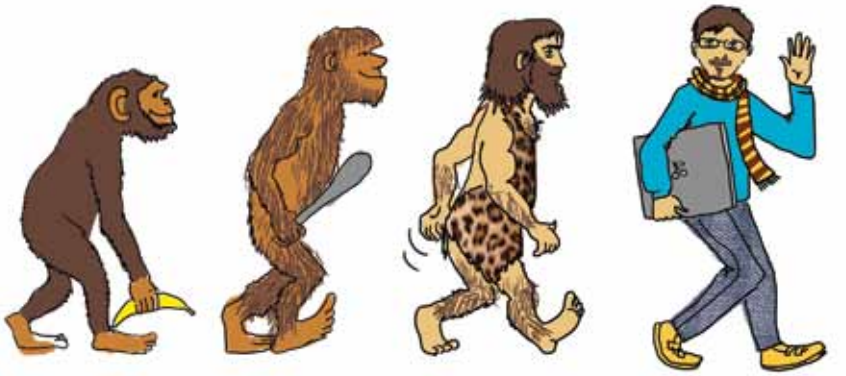


РАЗРУШЕНО

Злоумышленники постоянно совершенствуют методику атак на компьютеры пользователей, поэтому о безопасности нужно думать всегда. Безопасность — это процесс, который требует постоянной поддержки.

МИФ 6

Новая версия программы всегда лучше старой



ПОДТВЕРЖДЕНО

В новых версиях программного обеспечения исправлены многие ошибки, обнаруженные в предыдущих версиях и касающиеся защиты. Домашнему пользователю всегда следует использовать актуальное программное обеспечение.

МИФ 7

Если не загружать файлы из интернета, можно обезопасить себя

Большинство пользователей уже поняли, что нельзя запускать исполняемые файлы из подозрительных источников. Но существует другой, очень опасный путь заражения компьютеров – drive-by загрузки: достаточно открыть зараженную страницу, и вредоносная программа сама незаметно загрузится и запустится на вашем компьютере.

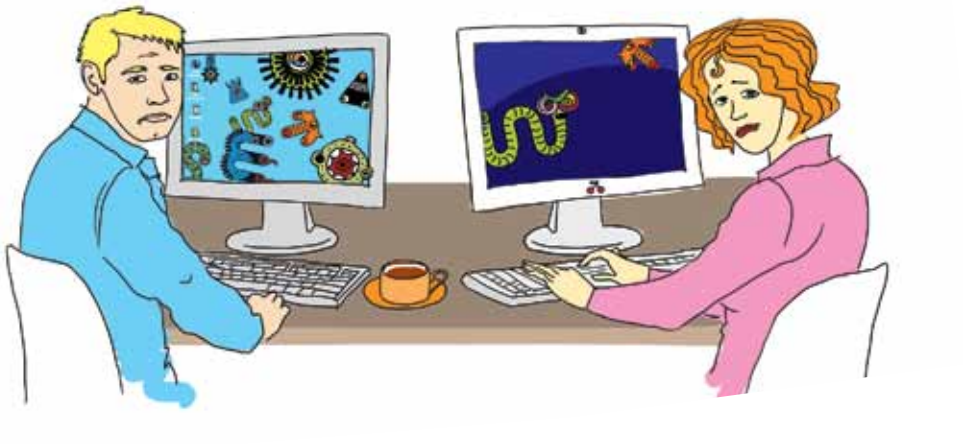
МИФ 8

Чем меньше распространено программное обеспечение (приложения, браузеры и т.п.), тем лучше оно защищено

Популярность программного обеспечения и его техническая реализация – слабо связанные вещи. Неизвестная программа может содержать гораздо больше уязвимостей, чем любая популярная программа. Однако злоумышленники действительно уделяют мало внимания нераспространенным программам и в этом смысле можно говорить, что использование такой программы безопаснее в данный момент.

МИФ 9

Операционные системы Linux, Android и MacOS обладают абсолютной защитой от вредоносных программ

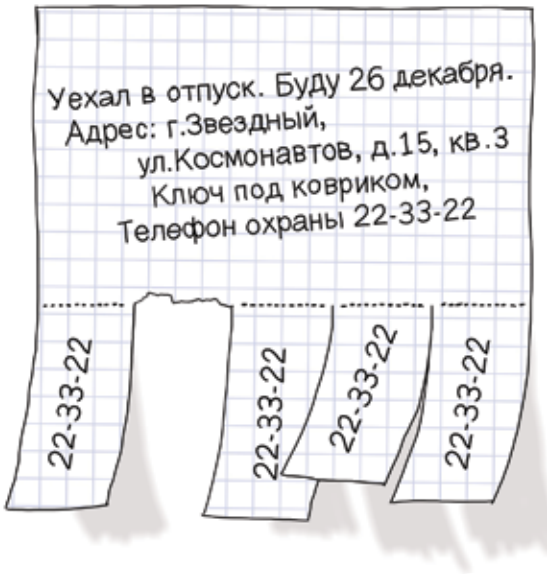


РАЗРУШЕНО

Как показывает статистика, число атак на операционную систему прямо пропорционально ее популярности среди пользователей. С развитием популярности «альтернативных» систем, появляются и вредоносные программы для них, о чем свидетельствуют данные антивирусных компаний: число вредоносных программ для MacOS, iOS и Android продолжает увеличиваться.

МИФ 10

Порядочному человеку приватность ни к чему: домашний адрес, телефон и прочие данные можно смело публиковать



РАЗРУШЕНО

Эти данные могут быть использованы злоумышленниками при «восстановлении» вашего пароля (а на самом деле для кражи его), для определения вашего приблизительного уровня доходов, территориального местоположения в конкретный момент времени. И это делает вас и ваше имущество уязвимыми для прицельного мошенничества и других преступлений.

МИФ 11

Сохранение паролей в браузерах, почтовых программах, ftp-клиентах и системах мгновенного обмена сообщениями — небезопасно

ПОДТВЕРЖДЕНО

Сохранение паролей в таких программах, как браузеры и почтовые клиенты, делает вас уязвимыми к широко распространенной категории вредоносных программ, занимающихся кражей сохраненных паролей в популярных программах и отправляющих их злоумышленнику.

МИФ 12

Администраторам сервиса может потребоваться ваш пароль для проведения какой-либо операции

РАЗРУШЕНО

Администраторы интернет-сервисов ни при каких обстоятельствах не будут спрашивать у вас пароль. Если вы получили письмо, отправитель которого представляется администратором сервиса и просит вас выслать пароль, это значит, что письмо прислано мошенниками, а вы оказались их мишенью. В этом случае вероятны дальнейшие попытки атаки на ваши учетные записи, поэтому будьте очень осторожны и внимательны при работе в интернете.

МИФ 13

Можно подделать любой адрес отправителя электронной почты и sms-сообщений

ПОДТВЕРЖДЕНО

Действительно, подделать адрес отправителя при отправке электронной почты не сложно, хотя многие почтовые фильтры обычно осуществляют специальную проверку и выявляют фальсифицированные адреса отправителя. В случае с sms специальные программы позволяют мошенникам указывать произвольный номер отправителя и даже текстовый идентификатор («Мама», «<Название компании сотового оператора>» и т.д.). Следует помнить о возможности подделки адреса/номера отправителя, особенно если в письме/сообщении вас просят ответить на другой адрес/номер.

МИФ 14

Чтобы ваш почтовый адрес не попал в списки спам-рассылок, нужно при публикации адреса на открытых ресурсах вместо символа «@» и точки надо использовать другие символы, например «[at]» и «[dot]»

ПОДТВЕРЖДЕНО

Списки для спам-рассылок обычно собираются специальными программами, которые исследуют информационные ресурсы на предмет наличия строк вида x@y.z

Публикация своего email-адреса в виде vasya_ivanov[at]mymail[dot]ru снижает вероятность попадания в списки спам-рассылок.

МИФ 15

Мой почтовый аккаунт никого не заинтересует — я общаюсь в Skype / icq / социальной сети и т.п.

РАЗРУШЕНО

Большинство учетных записей различных интернет-сервисов и систем мгновенного обмена сообщениями (Skype, icq и т.п.) при регистрации привязываются к электронному адресу и позволяют выслать на него забытый пароль. Получение злоумышленником пароля к вашей электронной почте может привести к взлому всех привязанных к ней аккаунтов.

МИФ 16

Все вредоносные программы портят информацию

РАЗРУШЕНО

Существуют семейства вредоносных программ, которые действительно портят данные, а затем злоумышленники требуют деньги за восстановление информации. Однако подавляющее большинство вредоносных программ нацелено на кражу данных, рассылку спама и организацию DDos-атак.

МИФ 17

Вредоносные программы попадают только к тем, кто заходит на порносайты

РАЗРУШЕНО

Возможность заражения не зависит от тематики сайта. Любой сайт может быть взломан и, как следствие, являться источником распространения вредоносных программ.

МИФ 18

Троянец-вымогатель всегда разблокирует компьютер и удалит сам себя, если перевести деньги по требованию вымогателей

РАЗРУШЕНО

Отправлять деньги злоумышленнику не следует ни при каких условиях. У многих антивирусных компаний есть специальные сервисы (деблокеры), которые позволяют бесплатно получить код для разблокировки системы.

МИФ 19

Стоимость платных sms на короткие номера всегда указана

РАЗРУШЕНО

С одной стороны, чтобы узнать точную стоимость sms на короткий номер следует обратиться к оператору сотовой связи. С другой стороны, одной sms на короткий номер вы можете, не подозревая об этом, дать согласие на платную подписку на какой-либо сервис. Возможен и другой вариант: вы вполне осознанно подписываетесь на какую-либо предлагаемую по короткому номеру услугу, но мошенники обычно указывают заниженную стоимость услуги, а реальная ее стоимость оказывается в несколько раз выше.

МИФ 20

Мобильные устройства не подвергаются атакам

РАЗРУШЕНО

Мобильные устройства прочно вошли в нашу повседневную жизнь и вызывают огромный интерес у злоумышленников. Управление электронной почтой, системами мгновенного обмена сообщениями, банковскими счетами может осуществляться с мобильных устройств, а это значит, что на них хранятся соответствующие логины и пароли и эти данные можно украсть. С каждым годом число вредоносных программ под различные мобильные платформы становится все больше.

Узнать больше об информационной безопасности
можно на сайте проекта «Академия Касперского»
www.kasperskyacademy.com

Kaspersky® **Academy**