Правила безопасного пользования интернетом

Интернет прочно вошел в нашу жизнь. Он помогает нам общаться с друзьями, знакомиться с новыми людьми, учиться, слушать любимую музыку и смотреть фильмы. Возможности Глобальной сети с каждым годом возрастают. Но, как оказывается, интернет может приносить не только пользу, но и вред.

Как же предотвратить его вредоносное воздействие? Предлагаем вашему вниманию ряд практических рекомендаций, используя которые вы сможете избежать многих интернет — угроз. Они помогут обезопасить не только общение с людьми во всемирной паутине, а также снизят нежелательные риски при использовании онлайн — игр и мобильного телефона.

1. Для защиты своего компьютера необходимо регулярное обновление программного обеспечения, использование надежных антивирусных и антишпионских программ.

2. В интернете не стоит переходить по ссылкам и нажимай кнопки во всплывающих сообщениях, которые кажутся подозрительными. Даже если вас будут уверять, что там находится нечто очень важное лично для вас.

3. Для защиты личной информации придумайте надежный пароль и никому его не сообщайте. Для каждого ресурса стоит использовать уникальные логины и пароли.

4. Никогда не предоставляйте секретные сведения, например, номер счета или пароль в ответе на сообщение электронной почты или в социальных сетях.

5. Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка рядом с адресной строкой, который обозначает безопасное соединение.

6. Для безопасности общения в социальных сетях оставляйте как можно меньше данных о себе и избирательно подходите к предложениям о дружбе.

7. Откройте пункт «Настройки» или «Параметры» в таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно заблокировать некоторых пользователей.

8. Перед просмотром входящих писем на электронном ящике, проверьте адрес отправителя. Подозрительные письма смело отправляйте в спам, особенно если в таких письмах содержатся прикрепленные файлы.

9. В чатах и системах мгновенного обмена сообщениями вы никогда не можете быть уверенными, кто с вами общается. Постарайтесь избегать общения с незнакомцами и ни в коем случае не соглашайтесь с ним на встречу в реальной жизни.

10. Для скачивания картинки или мелодии вам предлагают отправить смс? Не спешите! Сначала проверьте этот номер в интернете — безопасен ли он и не обманут ли вас.

Есть сайты, которые лучше не посещать, и технологии, которыми лучше не пользоваться. Но можно рискнуть! И все же сперва узнайте, чем вы рискуете. Вдруг передумаете?

Торренты

С помощью торрентов легко занести на компьютер вирус или вредоносную программу. Особенность технологии в том, что часто вы даже не знаете, что именно скачиваете.

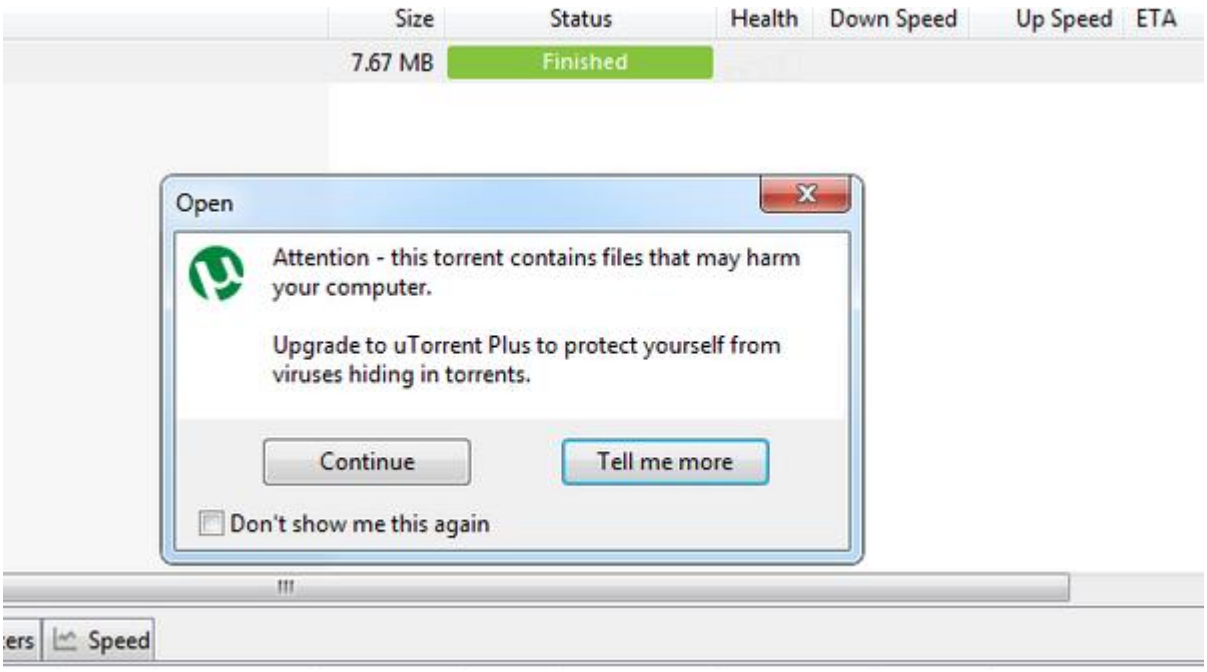
Программа показывает, что загрузится лишь папка с файлами (например, аудиокнига), но среди них вполне может быть вирус. Мы же не проверяем каждый файл, когда их сотни. Терпения не хватает.

Конечно, не все торренты — зло. Есть множество ответственных сервисов, которые распространяют контент, но при этом блокируют зараженные вирусами раздачи.

Что делать?

Пользуйтесь только знакомыми торрент-трекерами. Если сайт не знаком, поизучайте его — чем больше раздач и пользователей на нем, тем лучше. Посмотрите количество отзывов в топиках. На некоторых трекерах рядом с раздачей даже стоят отметки, что файлы проверены антивирусом.

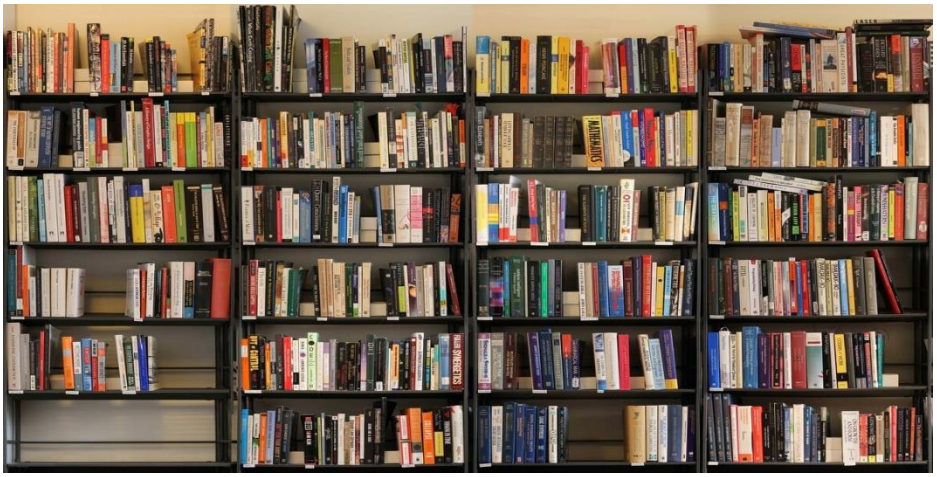
Если вы искали что-то редкое и попали на неизвестный трекер, лучше обойдите стороной или сперва узнайте, как безопасно качать торренты.



Некоторые торрент-клиенты предупреждают, что скачиваемые файлы могут повредить компьютеру. И предлагают купить платную версию клиента со встроенным антивирусом.

Книжные библиотеки

Пиратские библиотеки часто вместо книжек высылают архивы с вирусами. При этом отличить «честных» пиратов от «нечестных» трудно — сайты оформлены примерно одинаково, предлагают скачать файлы напрямую.



Есть и другая опасность. Многие библиотеки якобы проверяют пользователей перед скачиванием файла — просят отправить СМС, чтобы в ответ пришел код, который нужно ввести на сайте. Естественно, никто вас не предупредит, что сообщение платное, — оно просто снимет с вашего счета деньги.

Что делать?

Не качайте книги из неизвестных источников. Если не хотите платить, попросите ссылки у друга.

Файлообменники

Большая часть файлообменников — нерегулируемые хранилища, куда люди заливают что попало. Это удобно, когда ты хочешь скинуть другу большой файл. Проблема, как обычно, в людях. Злоумышленники заливают на такие сервисы файлы с вирусами, чтобы заражать чужие компьютеры. Например, якобы взломанный Adobe Photoshop. Если обменник не проверит его антивирусом, вы можете скачать программу и словить вирус. Так уж вышло, что свобода интернета распространяется на всех, даже на мошенников. И они этим пользуются.

Гораздо хуже, когда файлообменник подсовывает вам чужой софт, который якобы нужно установить на компьютер, чтобы качать файлы быстро.

Сайты знакомств

Тут все просто: если вас просят выслать деньги, не высылайте. Схем мошенничества предостаточно:

- девушка горит желанием переехать к вам в другой город, но ей нужны деньги на билет;
- заграничный жених готов перевезти вас в Испанию на ПМЖ, но сначала вышлите ему деньги, чтобы подтвердить серьезность намерений;
- ваш новый знакомый попал в беду, ему срочно нужны деньги;
- у вашего собеседника кончился интернет на телефоне, нужно пополнить ему счет.

Работа онлайн

В ней нет ничего плохого, но во время поиска легко наткнуться на мошенников. Существует несколько распространенных способов увести деньги у соискателя:

- выманить залог за что-то ценное (например, оборудование или программу), обещая много работы в будущем;
- уговорить оплатить закрытый доступ или премиум-аккаунт на сайт с хорошей работой;
- заплатить за обучение, после которого вас «точно возьмут в одну хорошую контору».

Если «повезет», вы не потеряете деньги, но поработаете бесплатно. Недельку порассылаете спам, будете по сто раз в день вводить капчу, прокликаете тысячу объявлений, напишете пять-десять текстов для тестового задания, обзвоните с холодными звонками сотню-другую компаний. На оплату даже не надейтесь.

Наконец, самый коварный способ — вам предложат скачать бесплатно программу, которая поможет зарабатывать до $ 2000 в неделю. Например, «Взломщик Яндекс. Денег» или «Генератор Webmoney». Заработают в итоге на вас, когда программа сворует все данные с вашего компьютера и передаст злоумышленникам или просто заблокирует его и потребует выкуп.

Что делать?

Не верьте в легкий и быстрый заработок в интернете. Увы, его не бывает.

Сервисы для «ВКонтакте»

Иногда хочется узнать, кто заходил на вашу страницу, кто добавил ваш профиль в закладки, кому ставят лайки ваши друзья и с кем переписывается ваш партнер. И, конечно, бывает позарез нужно скачать музыку или видео «ВКонтакте». И вообще супер, если можно будет получить платные стикеры бесплатно.

Для всего этого существуют сторонние сервисы. Они могут сделать все что угодно, нужно только ввести логин и пароль от аккаунта.

Почти все эти сервисы воруют учетные записи. В некоторых случаях внаглую «угоняют» и меняют пароль, в других действуют тоньше — время от времени под вашим аккаунтом незаметно заходит бот и вступает в разные группы.

Что делать?

Не верить сторонним сервисам и не оставлять им свои данные. Использовать двухфакторную авторизацию.