Бойся меня! Ловушки в интернете, о которых вы не знали

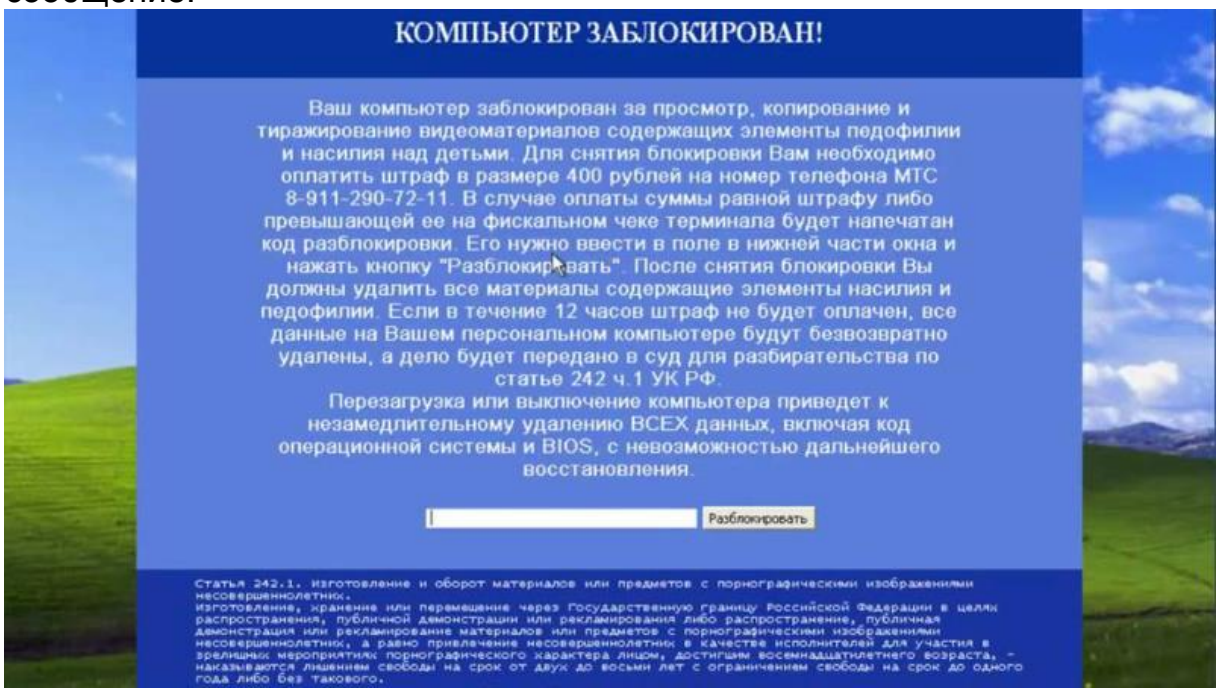
Источник: https://hi-tech.mail.ru/review/danger-in-the-web/

Интернет часто называют не только всемирной паутиной, но и всемирной помойкой. Кроме полезных и нужных вещей здесь на каждом углу нас норовят тем или иным образом обмануть. Неопытных пользователей ловушки подстерегают тут и там. Рассказываем, как их распознать, и что делать, если все же попались на крючок.

Вымогатели и попрошайки

Количество различных вредоносных программ для ПК исчисляется миллионами. Причем если еще каких-то 10 лет назад они создавались в первую очередь из хулиганских побуждений (например, знаменитый «Чернобыль» выводил из строя компьютеры так, что они после этого не включались), то теперь их главная цель – ваш кошелек.

Самый примитивный вариант – это «попрошайки», которые блокируют работу на компьютере, требуя ввести пароль для разблокировки. Для пущего устрашения на экран выводится сообщение о том, что вам нужно заплатить штраф за просмотр запрещенного порно или чего-то по добного, иначе компьютер будет заблокирован навсегда, а файлы удалены. Вернее так: «удолены навсигда» — грамотность авторов оставляет желать лучшего, ведь создают такие программы, как правило, школьники, пользуясь готовыми конструкторами, куда нужно только вписать свое сообщение.



Классический троян-вымогатель блокирует работу компьютера

Гораздо хуже более серьезные «попрошайки», которые шифруют содержимое жесткого диска, делая ваши файлы недоступными: это уже настоящее похищение с целью выкупа и суммы тут требуют большие: до нескольких тысяч рублей. Если от обычного блокиратора можно избавиться, в крайнем случае, переустановкой ОС, то здесь есть шанс навсегда лишиться плодов многолетнего труда: они останутся на диске, но расшифровать их будет невозможно.

Если в предыдущих двух случаях вы можете сами принять решение, платить или не платить, то так называемые «банковские трояны» крадут деньги с вашей карты без вашего ведома, перехватывая логины и пароли от интернет-банка. Не спасает даже двухфакторная авторизация через SMS: современные трояны умеют устанавливать одну из своих частей и на ваш смартфон, когда вы подключаете его к USB-порту для зарядки или копирования фотографий. После этого SMS от банка вы не видите; они отправляются прямиком к злоумышленникам и те спокойно опустошают ваш счет.

Методы защиты

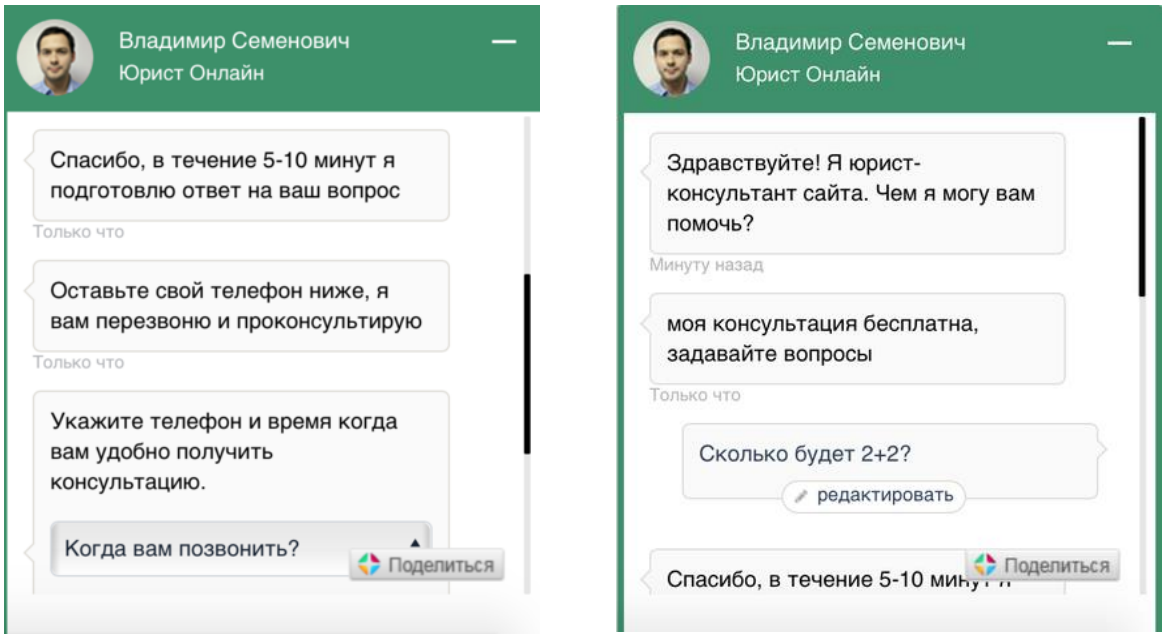
Поскольку вирусы используют «дырки» в безопасности операционных систем, необходимо, во-первых, постоянно устанавливать все обновления и не отключать встроенную систему безопасности. Для Windows 10 этого зачастую достаточно, однако неопытным пользователям дополнительный антивирус не помешает – главное, чтобы он тоже постоянно обновлялся. «Трояны» всегда устанавливаются вручную. Поэтому никаких «бесплатных танков», скачанных с форумов, никаких «кряков для фотошопа» и «активаторов офиса», скачанных с форумов, файлообменников и прочих сомнительных ресурсов.

Да, мы понимаем, что бесплатный софт очень притягателен и не будем убеждать вас в том, что все программы надо обязательно покупать, даже если она нужна вам один раз на пять минут. Но, во-первых, есть триальные версии, во-вторых, есть торрент-трекеры с системой «кармы» для авторов раздач (качайте то, что выкладывают «гуру»), в-третьих, все скачанное обязательно нужно проверять антивирусом.

Чтобы справиться с трояном, понадобятся стальные нервы

Фейки и подписки

Фейки тоже подстерегают вас, когда вы пытаетесь что-то скачать. По всем популярным запросам выдача Яндекс и Google замусорена поисковым спамом, поэтому, введя что-то типа «Игра престолов смотреть онлайн бесплатно» или «Скачать torrent», на первых пяти страницах вы получите ссылки на так называемые «дорвеи», соответствующие вашему поисковому запросу.



Это бот, собирающий базу телефонов потенциальных жертв массового обзвона

Переход на такой дорвей заканчивается одинаково: вам предлагают скачать то, что вы искали, но при этом под каким-нибудь надуманным предлогом (например, «защита от спама», или «докажите, что вы не робот» ввести свой номер мобильного телефона. На него отправляется SMS с кодом, который нужно ввести на сайте – казалось бы, привычная двухфакторная авторизация.

На самом деле (и это написано двумя экранами ниже мелким шрифтом светло-серым по белому) вы согласились подписаться на платный сервис с оплатой с вашего мобильного счета, абонентская плата рублей эдак 20 в день.

К этой же категории относятся фейковые сервисы: например, «анализ родословной», «поиск человека», «подбор диеты» и даже «местоположение любого абонента по спутнику»: здесь с вас тоже возьмут деньги в виде подписки или однократно за SMS, но в ответ вы получите вовсе не то, что ожидали, а копипасту из Википедии или справку о том, что +7921 – это Северо-Западный филиал «МегаФона».

Методы защиты

Что-то действительно бесплатно скачать реально только на специализированных закрытых форумах (если вы их не знаете, то сначала проконсультируйтесь со знающими людьми), либо на крупных торрент-трекерах (самый крупный трекер заблокирован на территории России, поэтому вам придется заходить на него не из России, например, с помощью VPN). Однако, где бы вы ни нашли ссылку для скачивания, не вводите номер телефона и не отправляйте SMS на короткие номера. Вас разводят!

Проверить тот или иной сервис на «фейковость» можно, введя заведомо несуществующие данные. Если человек по имени *Цйййй* и фамилии *Ьббббб* из города *Жжжжж* «успешно найден в базе данных» и осталось только «пройти проверку», закрывайте окно браузера. Фейковые сервисы всегда сначала создают иллюзию «одного шага от результата».

Фейковый сервис поиска абонентов по их номеру

3

Adware, Spyware и Bloatware

Так называют не совсем вредоносное, но все равно неприятное программное обеспечение.

Adware – это программы, поселяющиеся у вас в компьютере и то и дело подсовывающие рекламу, в основном при работе в Интернете. Они могут подставлять «свои» баннеры вместо размещенных на сайте и добавлять новые, подменять поисковую систему, установленную по умолчанию, открывать новые вкладки с сайтами, которые «могут вас заинтересовать», замусоривают закладки и т.п.

Spyware еще и следит за тем, что вы делаете на компьютере и на основании этого стараются показывать таргетированную рекламу – и, конечно, продают ваши персональные данные.

Получить такое на компьютер проще всего при попытке скачать какое-то заведомо бесплатное ПО, самое распространенное – это драйверы, на втором месте – «кряки». То есть, по конкретным запросам вроде «Geforce driver Windows 10» выдача замусорена дорвеями, с которых у вас скачивается… не драйвер, а «программа для обновления драйверов». С функцией обновления драйверов такое добро справляется не намного лучше, чем сама Windows, то есть, пользы почти не несет (редких драйверов, которые вам нужны, там обычно нет, а остальные ОС и сама обновит), зато исправно прописывается в реестре и сует свои баннеры куда только можно. То же самое делают и «Базы кряков».

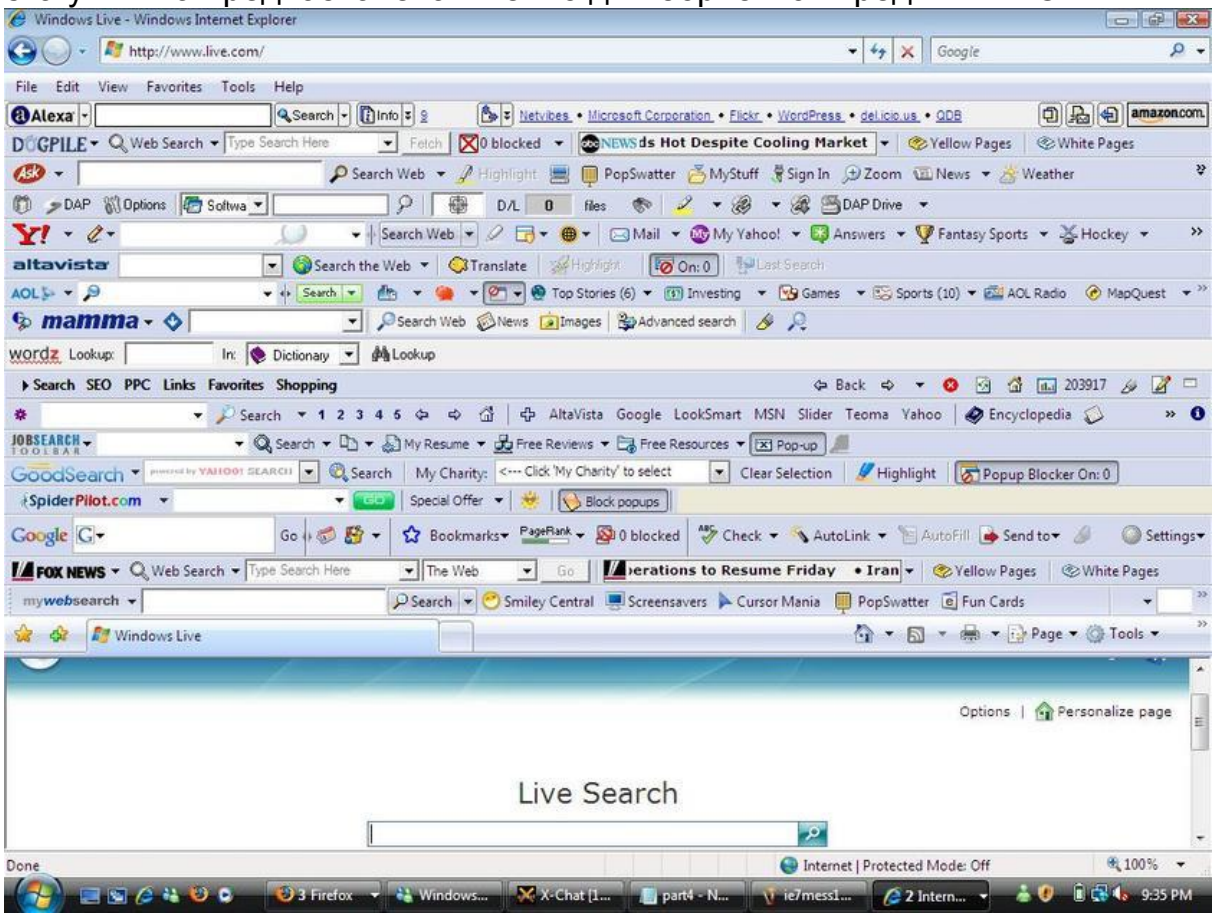
Bloatware – еще один вид вредного ПО. Стоит вам попытаться скачать популярную бесплатную программу, например, uTorrent, как вся выдача будет пестреть ссылками на exe-файл. Скачав его, вы действительно получите нужную программу. Но вместе с ней автоматически установится

еще миллиард «Ускорителей интернета», «Оптимизаторов памяти» и прочего бесполезного барахла, тормозящего работу.

Когда ваш номер попадет в базу данных, от назойливых звонков отделаться не получится

Методы защиты

Драйвера лучше всего качать с сайта производителя, а кряки к варезу брать там же, где вы этот варез скачали. Определить «подставу» довольно просто: попробуйте на сайте с «драйверами» или «кряками» скачать два-три совершенно разных, только не открывайте после скачивания. Если это фейк, то у вас в папке «Загрузки» окажутся три файла одного размера, но с разными именами. Если же вы уже нахватали гадостей – качайте Ad-Aware, эта утилита предназначена именно для борьбы с «вредным» ПО.



Вот что бывает, если бесконтрольно ставить всякие дополнения для браузера

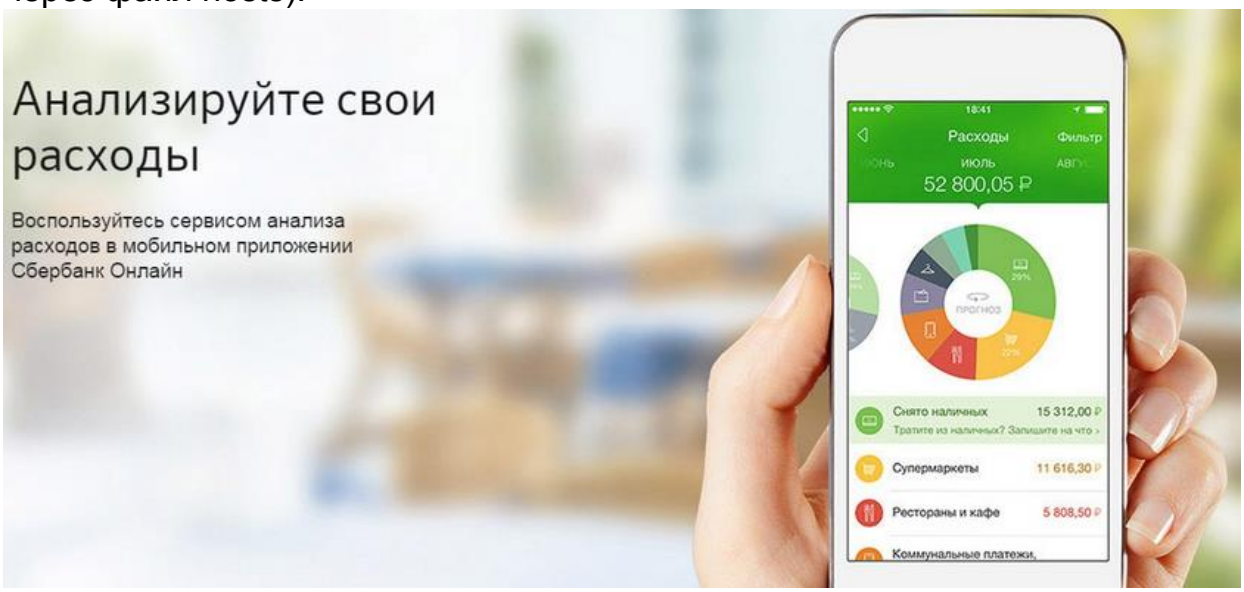
4

Фишинг

Фишинг (от англ. *phishing*) – это попытка сбора тех или иных данных на подставных сайтах, которые выглядят так же, как настоящие. Чаще всего злоумышленников интересуют логины и пароли от почтовых сервисов и соцсетей, а также банковских сервисов. Очень любят они и данные кредитных карт: собрав их, можно впоследствии неожиданно для жертвы организовать списание средств.

Раньше мошенники просто регистрировали домены, визуально не отличающиеся от привычных, например, vkontatke.ru или mai1.ru – многие до сих пор «клюют» на подобные фокусы. Однако с помощью вирусов и троянов, и даже более серьезной атаки, скажем, на роутер можно подменить DNS-записи и сделать так, чтобы при наборе правильного

адреса открывался подставной сайт с другим IP (чаще всего это делается через файл hosts).



«Сбербанк-Онлайн» подделывают чаще всего, на файлообменниках полно патченных версий, ворующих данные

Также в последнее время распространился сбор персональных данных через «чат-ботов». Стоит вам зайти из поиска на медицинский или юридический сайт, как в углу появляется окно чата, и «специалист» пишет вам: «Чем я могу вам помочь? Моя консультация бесплатна».

Что бы вы ни ввели в ответ, получите сообщение: «Спасибо, я подготовлю ответ в течение 5-10 минут», а затем: «Чтобы не ждать, оставьте свое имя и номер, я перезвоню с ответом». Стоит вам так сделать, и на ваш номер обрушится шквал звонков от продажников и втюхивателей всех мастей, знающих, что вас можно брать тепленьким. Естественно, ваш вопрос никто не прочитает: ваши данные просто продадут юридическим фирмам да торговцам БАДами,косметическими процедурами и чудо-фильтрами для воды. Впрочем, это уже совсем оффлайновая история…

Методы защиты

Внимательно следите за адресами в строке браузера. Не оставляйте свои контактные данные где попало. «Специалистов» сразу спрашивайте: «Сколько будет дважды два?», бот все равно уйдет думать и попросит телефончик.

Предупредите друзей о самых распространенных ловушках в интернете — помогите им избежать обмана