Пластун Я.И.

Основы безопасности в Интернете

16+

Яна Игоревна Пластун

Основы безопасности в Интернете

http://www.litres.ru/pages/biblio_book/?art=40315873
SelfPub; 2019

Аннотация

Для кого эта книга? Для всех, кто имеет возможность выходить в Интернет. И неважно, насколько часто это происходит: ваш гаджет постоянно онлайн, или же Вы проверяете почту раз в месяц. О чем эта книга?О том, сколько реальных опасностей таит в себе вроде бы виртуальная Всемирная паутина и как защититься от них.

Содержание

Предисловие

Сложно представить, что каких-то 20 лет назад люди обходились без мобильных телефонов и Интернета. А сейчас без них ни к врачу записаться, ни ЖКХ оплатить, ни с друзьями о встрече не договориться. Настолько они прочно вошли в нашу жизнь. И чем дальше, тем сильнее опутывает нас Интернет своей паутиной.

Я бы не сказала, что это плохо. Особенно, если пользоваться им с умом. Интернет принес в нашу жизнь удобства, о которых еще наши родители могли только мечтать, а может, даже и не смели подумать. Еще бы, можно не вставая с дивана:

- заказать себе запчасть на автомобиль/компьютер/строительный инструмент с другого конца света;
- пообщаться с друзьями из другой страны, да так, будто они рядом сидят;
- найти новых друзей, причем подробнейшая анкета человека позволяет сразу "отсеять" тех, кто не подходит нам по взглядам;
- найти практически любую необходимую литературу;
- обучиться чему-то новому напрямую у высококлассных мастеров;
- работать в любом месте в любое время;
- и многое-многое другое, мир Интернета обширен и

разнопланен.

Но, к сожалению, не все знают, как обезопасить себя и своих близких во время серфинга в Интернете. Наверное, потому что считают, что раз ты не выходишь из дома, значит с тобой ничего не случится. Это не так. Да, кирпич на голову вряд ли Вам упадет, пока Вы сидите на диване, но вот получить психологическую травму, потерять солидную сумму денег, данные на своем носителе, доступ к своим устройствам и сервисам – запросто.

Чтобы максимально обезопасить себя в Интернете, нужно соблюдать некоторые правила, а также вовсю пользоваться здравым смыслом, потому что ситуации бывают разные. Приведу простой пример. Все мы знаем, что нужно мыть руки перед едой. Но допустим такую ситуацию, при которой чистой воды нет вовсе (т.е. есть в наличии только такая вода, в которой плавает вся таблица Менделеева и использованный носок в придачу). Что безопаснее: поесть с немытыми руками или рискнуть помыть? В данной задаче еще много нюансов: насколько грязны руки, как далеко до относительно чистой воды, сможет ли человек протянуть, если сейчас не поест и так далее. Поэтому всегда нужно действовать по ситуации, а за основу брать базовые (на то они и базовые) правила. Так же и при выходе в Интернет – знание базовых правил обязательно для комфортного серфинга.

В данной книге я хочу привести основные правила, которыми стоит руководствоваться при путешествии по Все-

мирной паутине, а также привести примеры мошеннических действий, которые возможны в Интернете.

Книга не претендует на истину в первой инстанции, потому что, повторюсь, нужно не слепо следовать правилам, а думать головой.

Некоторые термины, применяемые автором, могут быть непонятны читателям. Для разъяснения в конце книги имеется глоссарий, куда вынесены определения наиболее «страшных» слов.

Также в конце есть ссылки на упоминаемые в книге программы и сервисы.

Рекомендуется к прочтению лицам старше 16 лет.

Все имена, фамилии и ситуации являются порождением фантазии автора. Любые совпадения с реальными людьми или историями случайны.

Подготовка к выходу в Интернет

Начнем мы с самых азов. Чтобы выйти в Интернет, Вам потребуется:

- рабочий исправный гаджет (телефон, планшет, к примеру) или ПК,
- браузер на этом устройстве,
- подключение к интернету,
- установленный и активный антивирус.

Вот про последний пункт почему-то многие забывают или не предают ему значение.

Антивирус

Антивирус – это программа, созданная для обнаружения и обезвреживания вирусов.

Антивирус необходимо устанавливать на все компьютеры, планшеты и смартфоны, даже если они не имеют выхода в Интернет.

Почему? Для защиты от вирусов (а также прочих неприятных программ, направленных на извлечение прибыли для чужого человека за Ваш счет), разумеется. Даже если Ваше устройство не подключено к Интернету, оно может получить вредоносный код через съемные носители информации (флешки) или при передаче файлов через альтернативные способы связи между устройствами (Bluetooth, ИК-порт, проводное соединение). Вирусы бывают разные:

- одни заражают Ваше устройство и начинают с него рассылку спама другим людям;
- другие закрывают доступ к Вашим файлам и требуют за них выкуп (и с большой вероятностью получится так, что заплатив указанную сумму, Вы все равно данные назад не получите);
- третьи следят за Вашими действиями и перехватывают Ваши пароли от всевозможных сервисов (от социальных сетей до банковских карт);
- четвертые пытаются подменить адреса сайтов, которые

Вы посещаете, чтобы выманить у нас пароли и явки;

• и еще пятые, шестые, восьмые и пятнадцатые. И все хотят прибыли за Ваш счет (прямым или косвенным образом).

И чтобы минимизировать риск заражения вредоносной программой, нужно обезопасить себя, установив антивирус.

Антивирусы тоже бывают разные:

• Есть такие, которые находят вирусы в оперативной памяти, на внутренних и (или) внешних носителях. Это сканеры.

• Есть такие, которые загружаются при старте системы и постоянно ее сканируют на вирусы. Это программы-мониторы.

• Есть такие, которые выполняют вакцинацию системы от определенных вирусов (известных данной программе). Они изменяют файлы и каталоги так, что это не влияет на их работу. После этого вирус, от которого производилась вакцинация, воспринимает этот файл уже зараженным и не внедряется в него. Это иммунизаторы.

• Есть такие, которые обнаруживают вирусы на ранней стадии заражения и не дают ему размножаться дальше. Это программы-фильтры.

• Самым надежным средством защиты ПК признаны программы-ревизоры. В отличие от остальных программ, они запоминают все изначальные параметры файлов, каталогов и системы в целом, а затем проводят сравнительный анализ.

• Есть универсальные программы, которые и сканируют систему, и блокируют проникновение новых вирусов, а также лечат зараженные файлы. Это программы-доктора. Скорее всего, Вы о них слышали, самые известные из них: Norton AntiVirus, Doctor Web, Kaspersky Antivirus. Именно такого типа программы следует установить в первую очередь на свое устройство для защиты от вирусов.

Универсальная программа, или программа-доктор, поможет Вам защититься от вредоносных программ, даже если Вы не частый гость в Интернете (поверьте, для заражения достаточно зайти 1 раз на зараженный сайт). Она постоянно будет следить за тем, какие файлы пытаются проникнуть в Вашу систему и вовремя забьет тревогу.

Вообще полное сканирование системы на вирусы необходимо проводить раз в месяц, а если Вы активно пользуетесь Интернет, скачиваете оттуда не всегда проверенные файлы, то и того чаще.

Сейчас на рынке много предложений от компаний, занимающихся разработкой антивирусных программ. Они отличаются по комплектации, универсальности, а также цене. Есть и бесплатные версии, полностью бесплатные антивирусы, которые хоть и защищают Вашу систему, но делают это не всегда полноценно (все зависит от разработчика). Поэтому прежде чем озаботиться установкой антивируса, нужно изучить предложения от хотя бы ведущих антивирусных компаний и, взвесив все плюсы и минусы, определиться.

В книге приводить предложения компаний нет смысла, потому что вирусы пишутся каждый день, следовательно, антивирусные базы обновляются также ежедневно, и чуть реже, чем ежедневно, обновляются предложения компаний-разработчиков антивирусного программного обеспечения.

Но тут возникает коллапс, подумаете Вы. Как мне выйти в интернет, чтобы определиться с антивирусом, не подхватив вирус, если у меня еще не установлен антивирус?

Действительно, как? А очень просто. Запоминайте рецепт (актуально на 2018 год, для ПК):

- Запускаем браузер.
- Набираем в адресной строке адрес https://ya.ru (это аскетичная версия Яндекса, без примочек).
- В поисковой строке вводим “антивирус Аваст”.
- Переходим на сайт https://www.avast.ru/.
- Скачиваем оттуда бесплатную актуальную версию антивируса.
- Устанавливаем его (установка и сам антивирус на русском языке, всё интуитивно понятно).
- Антивирус установлен, проверяем, чтобы он был запущен (в правом нижнем углу, в трее, возле часов, появится иконка).
- Запускаем браузер, и идем сравнивать антивирусные продукты.

В более краткой версии, можно опустить п.2 и п.3, и сразу

набирать в адресной строке адрес сайта Аваста.

Антивирус Аваст дает базовую защиту от вирусов, и если Вы будете пользоваться Интернетом с умом, риск подхватить заразу минимален. По идее, Вы можете вообще остановится на пользовании именно этим антивирусом, но в бесплатной версии есть не все функции, да и база антивирусная обновляется не так часто, как у того же Доктора Веба. И еще очень часто Вам будут приходить всякие рекламные сообщения с предложением купить полную версию продукта, а это некоторых раздражает.

Если вы все же решили остаться на бесплатном антивирусе, крайне рекомендую хотя бы время от времени проверять свой ПК бесплатными лечащими утилитами от Доктора Веба или Касперского. Вирусные базы, как уже было сказано, у них обновляются чаще, поэтому вероятность обнаружить заразу выше.

И еще пару слов о мобильных антивирусах. Как правило, у большинства крупных антивирусных разработчиков есть продукты для защиты мобильных устройств. И некоторые стоят денег. Опять же, Вам нужно будет сделать Выбор самим, руководствуясь своими предпочтениями. Но тут есть небольшой плюс: большинство производителей планшетов и смартфонов на Android встраивают в устройство антивирус McAfee, который вполне может обеспечивать защиту Вашего устройства. Для операционной системы iOS также есть ряд антивирусов, которые могут обеспечить защиту устрой-

ства.

Конец ознакомительного фрагмента.