Статья: По секрету - всему Интернету, или Как не попасться web-паукам (Антропова Т.Ю.) ("Руководитель автономного учреждения", 2021, N 9)

"Руководитель автономного учреждения", 2021, N 9

ПО СЕКРЕТУ - ВСЕМУ ИНТЕРНЕТУ, ИЛИ КАК НЕ ПОПАСТЬСЯ WEB-ПАУКАМ

В Интернете трудно сохранить приватность. Каждый шаг в Сети оставляет след. В эпоху компьютерных технологий любой человек может связаться с любым человеком или собрать на него неплохое досье. Хорошо, если это делается с мирными намерениями. А если действует злоумышленник, цель которого - отъем денег?

Есть ли способы защиты? Есть. И мы их обсудим.

Да, компьютер может быть заражен вирусом. И плохо то, что иногда сам пользователь как бы предлагает хакерам взломать его устройство, сам приглашает супостатов в свое интернет-пространство, разве что красную дорожку не стелет.

Способов виртуального мошенничества достаточно много, и каждый день список пополняется. Большинство этих способов основано на трех человеческих слабостях: жадность, любопытство и сверхдоверчивость. Враждебные действия могут быть направлены **против "железа"** или **против его хозяина**. В первом случае недоброжелатель заражает компьютер вирусом, во втором - выуживает нужную ему информацию при помощи методов социальной инженерии.

Когда безопасность в опасности

Мы понимаем, что охранять свою виртуальную территорию надо. Но знаем, что абсолютно защищенных доступов не бывает, как и не бывает невскрываемых дверей.

И тут возникает вопрос: если хакеры взломали даже такой суперресурс, как сервер NASA, стоит ли простому пользователю пытаться обеспечить себе интернет-приватность? Не проще ли пойти по пути садовода, по завершении сезона оставляющего дом открытым и вешающего табличку "Здесь брать нечего"?

Не проще. Потому что, в отличие от садовода, который все ценное имущество либо вывез в город, либо спрятал в надежном месте, нашему пользователю есть что терять. Практически каждый гражданин имеет банковскую карту, а бесконтактные платежи становятся все популярнее, и соблазн получить доступ к чужим онлайн-счетам у нечистых на руку субъектов все больше. Карты нет? А может, есть опасный секрет? Его тоже можно дистанционно обнаружить - вот вам и повод для вымогания денег. Да мало ли причин для сбора чужой информации.

Однако любой взлом - это время, нервы и деньги. Преступники стремятся использовать свои ресурсы рационально. Многие из них понимают: за сутки возни с защищенным компьютером можно вскрыть три-четыре незащищенных. Помните эпизод из фильма "Джентльмены удачи" с перетаскиванием батарей в детском саду? Работали бы Хмырь, Косой и Василий Алибабаевич с таким энтузиазмом, зная, какая именно сумма лежит в тумбочке? Ситуация с защитой аналогична: хозяин компьютера должен **усложнить работу непрошеному гостю до такой степени, чтобы он не захотел заниматься этой работой**.

Зачем же лезть в чужой компьютер?

Поколение хакеров - умненьких шалунов, внедряющих вредителей в чужие интернет-системы забавы ради, постепенно уходит в историю. Это те юмористы, которые в 2014 году на дорожном табло в Сан-Франциско, предупреждающем о пробках и ремонтных работах, разместили светящуюся надпись "Годзилла атакует! Поворачивай!"; годом раньше - в аккаунте Burger King заменили его логотип на символ главного конкурента, компании McDonald's...

Современные взломщики более меркантильны, но их методы не менее креативны.

Как отнимают деньги?

Представим, что хакер уже проник в чужой компьютер и начинает там свою деятельность. Каковы могут быть его коварные планы?

Уводят средства с онлайн-счета

Компьютер - это лишь машина. Умная, быстрая, незаменимая, но всего лишь машина. Он не может самостоятельно отличить хозяина от чужака. Если нет установленного запрета, все равно, кто нажимает на кнопки, кто открывает файлы и кто на какие сайты заходит. "Железо" выполняет команды человека. Того человека, в чьих руках "бразды правления".

Цель хакера - завладеть управлением. И тогда ваши возможности - это его возможности. Захочет - посетит онлайн-банк и переведет куда надо ваши сбережения. Пожелает - приобретет себе что-то нужное и расплатится от вашего имени. Возможности поистине безграничны, хватило бы средств на их реализацию. Ваших средств. Впустили на свою территорию чужака - расплачивайтесь. В буквальном смысле этого слова.

"Купите ваши же секреты!"

Остап Бендер смог получить миллион от Корейко, используя добытую информацию против него. Компромат аферист собирал тщательно и с большим трудом. В век Интернета все было бы проще.

Безупречных людей нет. Кто-то что-то кому-то сообщил в личной беседе, кто-то что-то сделал, не подозревая, что камера включена дистанционно, кто-то сохранил приватное видео. Вот и материал для шантажа.

За примером ходить далеко не надо - возьмем хотя бы звездные скандалы. Памела Андерсен в первый раз судилась со взломщиками в начале 1990-х - они выложили в открытый доступ ее домашнее видео с мужем, Томми Ли, не предназначенное для посторонних глаз. Через 10 лет история повторилась. Видеодива отсудила у наглецов, посмевших вторгнуться в ее частную жизнь, более 90 млн долл. Но компромат-то в Сети остался. Аналогичная история произошла в 2006 году с Ким Кардашьян.

Свои "скелеты в компьютере" есть у многих. Задача взломщика - найти эти "скелеты" и продать подороже.

Существует и другой вид вымогательства, опасный даже для людей с безупречной репутацией. Представьте темный экран монитора, внезапно "сдохшую" компьютерную мышь и

системный блок, работающий бессистемно. Это постарался вирус-разрушитель, внедренный из присланного файла или подхваченный с какого-то сайта.

И вот, когда уже у пользователя опустились руки, когда он понял, что важные записи утеряны навсегда, а любимый ноутбук годен лишь в качестве подставки под горшок с фиалкой, на экране появляется надпись: переведите по указанному счету энную сумму, и будет вам счастье - все оживет и заработает. Ничего личного, это бизнес.

Может быть, все действительно начнет работать после совершения транзакции (хотя такое очень редко случается). Но деньги-то уйдут. И уйдут безвозвратно, поскольку подобные преступления раскрывать трудно.

Делаем вывод: чтобы вымогатели и грабители не считали работу с вами подарком судьбы, **не распаковываем сомнительные файлы, не ходим по сомнительным ссылкам**. А если очень хочется это сделать, активно "обеззараживаем" все антивирусной программой.

Зачем выуживают информацию?

Про деньги все понятно. Их надо охранять. Но зачем нужна информация - простые подробности жизни, которые и скрывать-то нет смысла?

На первый взгляд, в обычной информации нет ничего особенного. Какая разница, знает ли посторонний кличку вашего питомца, дату рождения ребенка или девичью фамилию матери? Разберемся.

"Информация - власть!" - говаривал доктор Хаус из известного сериала. Представьте ситуацию, когда вдруг на телефон заботливой мамы или любящего папы поступает звонок от "следователя по особо важным делам", который, обращаясь к собеседнику по имени-отчеству, сообщает, что чадо такого-то возраста по такому-то имени совершило преступление, что ребенка срочно нужно спасать, что спасение дорогое, но оно того стоит! И вот уже родитель в панике продает соседу фамильные драгоценности, чтобы как можно быстрее передать сумму нужному человеку "из компетентных органов". А после передачи и заверений "Теперь все будет хорошо, но вы впредь за ребеночком приглядывайте", после исчезновения "благодетеля" с деньгами заспанный отпрыск вдруг выплывает из своей комнаты с удивленным видом: "Да, я сегодня поздно явился и тихонько лег в постель, дабы вас, уже спящих, не тревожить".

Тут родители - они же наивные пользователи, не принявшие меры интернет-безопасности, - понимают, что звонил им злоумышленник, и недоумевают, где же он взял нужные сведения. Потерпевшие не подозревают, что сами преподнесли все "на блюдечке", выложив в Интернет информацию и не позаботившись о ее защите. В соцсетях есть имена, фамилии, полнейшие отчеты о передвижениях, сведения о недвижимости и движимости и т.д. В переписке и комментариях - факты из личной жизни, какие-то интересные подробности.

Описанный случай показательный, но не единственный пример использования краденой информации в корыстных целях. Зачастую последствия взлома могут быть серьезнее, чем передача неизвестному половины вашего месячного оклада.

К сведению. Одна популярная телепрограмма, основанная на демонстрации чудесных возможностей людей с якобы паранормальными способностями, долгие годы делает себе рейтинг путем тщательной подготовки каждого "испытания". Команда профессионалов

выуживает информацию о каждом человеке, обратившемся к "чудо-людям" за помощью. Основным источником сведений, разумеется, выступает Всемирная паутина. А потом та же команда удивляет телезрителей подробностями "видений" участников шоу.

Обратившиеся за помощью даже не подозревают, сколько информации о них можно найти в Сети, и искренне восторгаются: "Этого никто о нас не знает!".

Как защитить свой компьютер?

Страшные рассказы об интернет-вымогателях и интернет-взломщиках могут дать повод думать, что современному пользователю надо денно и нощно проявлять бдительность. Но это не так.

Правила компьютерной безопасности для обычного человека существуют. И они не сложнее, чем нормы этикета или требования гигиены.

Антивирус: всегда обновлен и всегда в деле

Антивирусная защита должна быть на каждом компьютере - это не обсуждается. Вторая аксиома - на вирусы следует проверять не только то, что нужно открывать или распаковывать (флешки, диски, файлы и т.д.), но и (периодически) все содержимое компьютера. Третье железное правило - ваш антивирус должен обновляться. Создатели вредоносных программ регулярно "радуют" пользователей своими новыми достижениями. Разработчики интернет-защиты тоже не отстают: регулярно изобретают способы противодействия, "вшивают" их в очередную версию существующей программы и предлагают клиентам.

Как и когда обновлять программу? Обычно компьютер сам напоминает "Пора!" и выдает алгоритм действий.

Правило обновления действует и для обычных программ, новые версии которых более устойчивы к интернет-атакам. А само программное обеспечение безопаснее скачивать с проверенных сайтов.

Пароли: не надо бояться сложностей

Лет десять назад, в эпоху расцвета компьютерных клубов, чуть ли не треть заведений называлась QWERTY. Знакомое сочетание, не так ли? Правильно, это первые шесть букв клавиатуры в английской раскладке - один из самых популярных паролей.

Правда, существует группа еще более ленивых пользователей, которые предпочитают, например, нажимать несколько раз подряд одну и ту же цифру или букву для входа в систему.

Те, кто похитрее, используют в качестве кода доступа кличку питомца, девичью фамилию (свою или мамы), значимую дату, не подозревая, что и эта информация есть во Всемирной паутине (соцсети, переписки, форумы, сайты).

Еще более ушлые набирают на английской раскладке какую-либо фразу без пробелов, например vjqgfhjkm, хотя у взломщиков есть специальные программы, которые быстро вычислят "мойпароль", зашифрованный столь примитивно.

При подборе пароля надо применять **следующие правила**:

- сочетание не только букв, но и цифр, а также символов обязательно;

- сочетание бессистемно - это случайный набор;

- буквы не только прописные, но и строчные;

- длина кода - минимум шесть знаков.

Если фантазии для создания пароля не хватает, воспользуйтесь услугами генератора, благо в Интернете их предостаточно (Password, Avast Passwords, Norton Password Manager и т.д.).

Еще одно правило парольной безопасности: **коды нужно периодически менять**.

Да, сложный пароль труден не только для взломщика, но и для того, кто им пользуется, - попробуй запомнить последовательность всех этих знаков хотя бы для одного секретного сочетания! Тут, как ни крути, не обойдешься без записи. Но какому носителю можно доверить столь важную информацию? Компьютер взломают, в блокнот подсмотрят.

Попробуйте сделать так.

1. Сгенерируйте, например, шестизначное сочетание, запишите его или запомните.

2. В дальнейшем используйте это сочетание при создании паролей, вставляя его в любое место наряду с другими символами.

3. Заведите тетрадь или создайте файл для хранения паролей и записывайте туда всю информацию в зашифрованном виде, заменяя шестизначное сочетание звездочкой или другим значком, понятным только вам. Вы будете знать, что именно скрывается за такой цифрой, буквой, символом, а посторонний - нет.

А если информация, хранящаяся в вашем компьютере или на другом устройстве, очень ценная, используйте еще и биометрическую аутентификацию - например, вход по отпечатку пальца, скану радужной оболочки глаза.

Слово не воробей, но Сетью ловится

Интровертам проще - информацию из них приходится выуживать. Экстраверты готовы рассказать все о себе первому встречному. Поэтому экстраверты чаще страдают от интернет-мошенников. Однако любой сможет хранить секреты, если осознает последствия, которые могут наступить при их разглашении.

Защита в этом направлении одна - **не болтать**. Помните: все, что вы выложите во всеобщий доступ, может быть использовано против вас. Например, многие перед путешествием любят публиковать на страничке в соцсети фото билетов. Почему это плохая идея? Да хотя бы потому, что злоумышленник поймет, когда вас не будет дома. В посадочных документах имеются и другие важные сведения. Кто-то может позвонить перевозчику от вашего имени и, указав необходимые данные, отменить поездку и попросить вернуть деньги. А уж шестизначный код бронирования - временный пароль, известный также как PNR (запись имени пассажира), вообще

подарок для злоумышленников. Человек, знающий этот код и фамилию владельца билета, может получить доступ к его багажу или улететь его рейсом.

С билетами на концерт - та же история. В 2016 году некий москвич пожаловался в Instagram, что не смог попасть на концерт любимой группы Black Sabbath, поскольку некто скопировал штрих-код с фото билета, выложенного в профиле, и проник на площадку раньше.

Но если информация не идет к вымогателю, **вымогатель идет к информации**: создает очень привлекательные сайты, делает предложения, от которых трудно отказаться. Кто-то поведется на сообщение о распродаже конфиската, при которой брендовая одежда уходит к счастливчикам за смешные деньги. Кого-то соблазнит приглашение на суперработу, например три часа в день собирать шариковые ручки за оклад директора мини-завода. Цель посулов одна - заставить потенциальную жертву зарегистрироваться, указав персональные данные (а иногда требуется еще и подтвердить серьезность намерений вступительным взносом). Обычно после регистрации связь с сайтовладельцами прекращается.

Стоит ли принимать подобные предложения, человек разумный решает самостоятельно. Для начала можно задуматься: а почему на такую привлекательную распродажу торговец не зовет своих знакомых, почему на суперработу не устраивает родственников? Если и после этого соблазн остается, посмотрите отзывы о предложении в Интернете. Но ищите не по названию компании или магазина (изменить его недолго), а по тексту сообщения - как правило, с вариациями на эту тему отправители не заморачиваются.

Компьютер, щетка и расческа должны быть личными

Жил-был ответственный пользователь. На сомнительные сайты не ходил. Файлы от незнакомцев не открывал. Уходя из своего офиса, оставлял охранника.

Все эти меры предосторожности оказались напрасными: устройство взломали, вирус внедрили. А все потому, что скучающий охранник развлекался на хозяйском компьютере - и на разные сайты заглядывал, и сомнительные вложенные файлы открывал.

Мораль этой правдоподобной истории проста: безопасность компьютера зависит от всех его пользователей. Такими пользователями могут быть и сослуживцы, и домочадцы, и просто знакомые.

Не хотите "случайных связей" - **поставьте пароль на вход**.

Скачок трафика - это опасно

Вирусы-шпионы незаметны, но производительны. Наряду с постоянным сканированием компьютера на предмет заражения нужно следить за своей интернет-активностью. Например, если трафик за день вырос до 1 Гб, а вы только пару раз открывали почту, что-то тут нечисто. Кто-то пользуется Интернетом от вашего имени - шлет спам, отправляет собранную информацию, а может, добывает криптовалюту за счет ресурсов вашего процессора.

Расходование трафика можно отследить, найдя в разделе "Параметры" подраздел "Сеть и Интернет". Там же можно этот трафик ограничить.

Поверим, не проверим?

Письма по-прежнему являются одним из самых действенных способов проникновения в чужой компьютер или получения заветной суммы. Письма могут маскироваться под следующую корреспонденцию.

1. **Весточка от друга.** Это письмо действительно отправлено с почтового ящика вашего знакомого, но не им, а хакером, взломавшим ящик. Чтобы распознать мошенника, обратите внимание на безличные предложения (скорее всего, рассылка веерная, злоумышленнику некогда разбираться с приветствиями) и изменение привычной лексики (чрезмерную фамильярность или официоз), просьбы перейти на сайт или как можно быстрее посмотреть присланные файлы ("а то обижусь"), мольбы о материальной помощи. Проигнорируйте такое письмо. А если боитесь обидеть отправителя, свяжитесь с ним по телефону или найдите другой способ уточнить информацию.

2. **Официальное послание.** Иногда мошенники поступают примитивно - выбирают любой адрес и отправляют провокационное сообщение типа "Списание с вашего счета 5 тыс. руб. одобрено банком", "Из-за грубых нарушений ваш аккаунт заблокирован", "А у вас молоко убежало". Далее обязательно следует ссылка, по которой надо пройти, чтобы во всем разобраться. Испуганный адресат переходит на нужную страницу, недоумевает: "Позвольте, какое молоко? У меня на плите нет молока!" А вредоносный вирус уже топчется в его компьютере.

Поэтому не торопитесь, вначале проанализируйте ситуацию.

Более старательные преступники маскируют письма под известные бренды: "Госуслуги", "Сбербанк", "Авито" и т.д. В этом случае обязательно смотрите на адрес отправителя. Буквы и цифры после "собаки" (@) должны совпадать с доменом официального сайта. Например, послание, пришедшее с Avito, будет заканчиваться так: @avito.ru. Если в конце стоят awito.ru, ovito.ru или avita.ru - сообщение отправлял злоумышленник. Корпоративная символика и другой официоз оформления вводить в заблуждение не должны.

3. **Ошиблись адресом.** Много ли мужчин устоит, получив, например, такое сообщение "от Анжелы": "Привет. Классно вчера посидели в баньке. Высылаю фотки. Но только для тебя"? Желание посмотреть, что же такого было в этой баньке, частенько пересиливает понимание, что отправитель ошибся адресом и что читать чужие письма, смотреть чужие фотографии - плохо. Заинтригованный получатель идет по ссылке или распаковывает файл. Возможно, он видит то, что хочет. Но в это время вирус идет к нему в компьютер и делает то, что может.

Совет: если любопытство пересиливает разумные доводы, проверьте ссылку на вирусы хотя бы на сайте vms.drweb.ru/online или просканируйте присланный файл антивирусной программой.

4. **Просьба о помощи.** Один из самых гнусных онлайн-обманов касается благотворительности. Прошли времена массового получения писем от умирающих миллионеров, которые наслышаны о филантропических качествах адресата и готовы перевести на его счет все свои деньги. Но когда на почту приходит просьба помочь в сборе средств на операцию для ребенка или приюту для животных, проверьте честность отправителя.

Например, автор этой статьи получил сообщение с мольбой о материальной помощи прооперированной собаке, которую готовы выбросить на улицу, поскольку не оплачен

стационар. В письме были фотографии документов и, конечно, снимок несчастного животного. Простое обращение в клинику, где работают "бессердечные ветеринары", показало, что сообщение не что иное, как вымогательство: никакой похожей собаки в клинике не было, там не было даже стационара. "Вы не первая, кто к нам обращается, про эту собаку постоянно спрашивают", - устало сообщил врач по телефону. Будьте бдительны! Благотворительность почетна, но ваши деньги должны действительно приносить пользу, а не обогащать мошенников. Сомневаетесь - введите в поисковик наиболее характерную фразу из письма или указанный телефон. Как правило, аналогичные письма не первый день гуляют по Интернету. Либо найдите контакты названного в письме заведения и проверьте все сведения лично.

Второй почтовый ящик - не роскошь

При регистрации на сайтах, при интернет-покупках и других действиях в Сети зачастую требуется вписать адрес электронной почты. Бывает, что база данных с этих сайтов попадает в руки мошенников. В лучшем случае адресата заваливают спамом, в худшем - при помощи полученных данных воруют деньги.

Поэтому желательно иметь два почтовых ящика. Один для важной переписки, а другой - для своей интернет-деятельности.

Чужой компьютер - свои правила

Отдельно рассмотрим ситуацию, когда приходится работать на стороннем компьютере. В этом случае желательно оповестить об этом машину, нажав соответствующую кнопку при входе. Тогда все "пароли, адреса, явки" не будут сохраняться автоматически, как это бывает на домашнем устройстве.

Дополнительными мерами безопасности станут очистка истории просмотров (кнопка находится справа, вверху страницы браузера) и удаление личных файлов, в том числе из "корзины" и из папки "Загрузки".

И не совершайте самую распространенную ошибку - по завершении работы обязательно выйдите из своей почты.

* * *

Компьютер надо защищать в любом случае - хорошая защита отобьет у хакеров желание тратить на вас нервы и время. Кроме того, следует заботиться об интернет-безопасности, выполняя не очень сложные, но важные правила:

1) доверять, но проверять;

2) не ходить, куда не надо;

3) пользоваться антивирусом;

4) применять сложные пароли и регулярно менять их;

5) систематически обновлять программное обеспечение.

Т.Ю. Антропова
Эксперт журнала
"Руководитель автономного учреждения"

Подписано в печать

24.08.2021