Правила безопасности
при пользовании Интернет-сервисами и соцсетями.

Официально администрация США давно разместила информацию – когда и на какие средства «поддержала стартапы» по созданию международных соцсетей и сервисов, но особо не афиширует эти факты. В настоящее время более 10 комитетов при Госдепе, развед.ведомствах и частных «фондах» работают по управлению «процессами» в соцсетях, облачных и других сервисах сети Интернет. Во всех последовавших за этими событиями «цветных» революциях «отметились» эти комитеты и ведомства, которые потратили на свои программы массу средств «на развитие демократии» за рубежом США.

Два маленьких примера. Никто не задавался вопросом, - а зачем собственно, на самом деле, затасканный по судам в США «Microsoft» за связь со своими национальными спецслужбами, себе в убыток приобрел пять лет назад видеосервис «Skype»? с его оригинальной системой шифрования трафика, которая раньше была «головной болью» спецслужб? Теперь к «Скайпу» нет претензий у американских развед.ведомств и спецслужб безопасности.

Проект «безопасного» браузера «Tor» (значок - полуразрезанная луковка) финансируется Госдепом и Минобороны США. Ясно, какую приватность он обеспечивает на свои деньги. Но криминальные злоумышленники «не спят», - используют сайты социальных сетей не только для поиска компромата, но и для атаки на вас или ваши мобильные устройства.

Зададимся одним простым вопросом: когда у вас что-то не получается, или вы не знаете ответа, куда вы прежде всего обращаетесь за помощью? Уверены, что большая часть пользователей современных смартфонов и компьютеров ищет ответы в Google или Яндексе. Вы никогда не замечали одну особенность, - если, предположим, вы искали новую летнюю резину для своей любимой машины, или более хорошую видеокарту для домашнего компьютера, то даже если вы приобрели заветную вещь, еще очень долго самые разные сайты будут показывать вам «релевантную»[1] рекламу в надежде на то, что вы сделаете эту покупку еще раз и именно у них.

Есть несколько способов избежать этого и сохранить свои предпочтения в тайне. Самый простой способ - использовать поисковые системы, не собирающие персональные данные. Подобные поисковые системы обычно работают с более крупными поисковиками, такими как Google, Yahoo!, Bing и т. д., что, в свою очередь, гарантирует качество и

[1] **Релева́нтность** (лат. Relevo «поднимать, облегчать») в информационном поиске - семантическое соответствие поисковому запросу полученного документа. В более общем смысле, одно из наиболее близких понятию качества «релевантности» — «адекватность», то есть не только оценка степени соответствия, но и степени практической применимости результата, а также степени социальной применимости варианта решения задачи (Википедия).

«релевантность» результатов поиска на должном уровне. Однако, в отличие от крупных поисковиков, они заботятся о вашей приватности, в частности они не раскрывают ваш адрес, данные о вашей системе, программном обеспечении, местонахождении и многом другом. Исходя из опыта, можно порекомендовать следующие сервисы: - disconnect.me; - duckduckgo.com; - startpage.com.

Следующий момент, которого хотелось бы коснуться, — безопасные браузеры. Сразу же оговоримся, что мы не рекомендуем устанавливать такие браузеры всем. ИБ всегда балансирует между максимальной защищенностью и удобством работы. Есть два основных типа браузеров — созданные с целью сохранения приватности и использующие различные надстройки для обеспечения безопасности пользователя.

В качестве примера первого типа браузера можно привести Epic privacy browser. Он был создан на основе Chromium — браузера с отрытым исходным кодом, разработанного компанией Google. Его основная задача — защита вашей приватности. Все куки уничтожаются после каждой сессии, трафик проходит через серверы разработчиков, позволяя скрыть ваш IP-адрес, а соединение с веб-сайтами осуществляется преимущественно через SSL.

Примером браузера, который использует различные надстройки для обеспечения приватности, может служить Comodo dragon на основе Chromium или Comodo icedragon на основе Mozilla Firefox.

Одной из особенностей данного браузера, на наш взгляд, и очень важной — является использование им своих собственных DNS-серверов. А это, в свою очередь, позволяет защититься от фишинговых атак и от возможности попадания вредоносных программ на вашу рабочую станцию.

Еще одна интересная вещь — это виртуальная среда, в которой браузер запускается в изолированном от остальной системы режиме, но, к сожалению, данная опция доступна только обладателям продукта Comodo Internet Security.

Имеются и другие браузеры, нацеленные на сохранение вашей приватности, — Brave, Dooble, Avira Scout и т. д.

В ключе разговора о браузерах мы хотели бы рассмотреть одно любопытное дополнение - AdNauseam. В отличие от других расширений, оно не только прячет нежелательные рекламные объявления, но еще и имитирует проходы по ним. Что приводит к тому, что собирающие о вас информацию системы начинают предполагать, что вас интересует все, начиная от похудения и заканчивая проблемами миграции кенгуру в брачный период. Естественно, что в этом огромном объеме данных ваши настоящие интересы просто затеряются. Так почему же Google не позволяет своим пользователям устанавливать это расширение?

Во-первых, это связанно с тем, что эта компания является одним из лидеров по сбору и обработке персональных данных.

Вторая причина — бизнес-модель. Пользователи рекламной сети Google не платят за показы рекламы, а только за переходы по объявлениям.

Использование данного плагина ведет к убыткам, поскольку клик по ссылке был и деньги за него были списаны, а реального перехода не произошло. AdNauseam, как бы издеваясь над всей отраслью контекстной рекламы, показывает примерную сумму, на которую она уже «накликала».

Раз уж зашел разговор о ПО, созданном для защиты вашей приватности, было бы огромным упущением с нашей стороны не рассказать об ОС, созданных с той же целью.

Большая часть из них представляет собой модификации Debian или Ubuntu. Операционные системы данного класса можно запускать с внешних носителей, таких как DVD. Преимущество такого подхода в том, что даже если во время работы на вашу рабочую станцию проникло вредоносное ПО, после перезагрузки вы опять получите чистую и нетронутую ОС.

К тому же такие ОС уже сконфигурированы для использования сети «Tor», что безусловно помогает вам обеспечить свою приватность и даже посещать закрытые сайты, но помните, кто платит за проект «Tor»! Если цель – защита не от них –можете смело пользоваться. Как правило, такие ОС не ограничиваются одним лишь использованием «Tor», они поставляются с большим количеством предустановленного и настроенного ПО, в том числе для:

- шифрования и дешифровки носителей, электронной почты и другой информации;
- безопасного пользования Интернетом (про браузеры такого типа мы говорили чуть выше);
- использования генераторов и менеджеров паролей;
- обеспечения удобной и безопасной работы с сетью.

На взгляд специалиста по безопасности, среди огромного множества таких систем наибольшего внимания заслуживают:

- Tails — одна из самых бурно развивающихся. Известна тем, что эту ОС использовал Эдвард Сноуден;
- Whonix — предназначена для использования в качестве гостевой изолированной ОС, работающей в VirtualBox и использующей сеть «Tor»;
- IprediaOS — в отличие от других проектов, вместо «Tor» использует L2P и построена на основе Fedora Linux;
- Discreete Linux — обеспечивает высокий уровень защиты и предназначена для людей, не имеющих глубоких знаний в области ИТ.

Безусловно, мы не рассмотрели множество прочих аспектов обеспечения индивидуальной безопасности отдельных хостов сети, но мы надеемся, что квалифицированный пользователь не забывает о регулярном обновлении ПО, установке антивируса, шифровании диска, использовании шифрования и блокировки телефона, создании безопасных паролей и о многом другом, что составляет основу личной информационной безопасности.

Вот еще некоторые простые советы по использованию соцсетей, которые помогут вам повысить свою безопасность:

- Думайте перед тем как сообщать информацию о себе, своих взглядах, планах и оценках, фотографиях и видеороликах, - как это можно использовать против вас?;

- Логин. Используйте для защиты аккаунта только надёжный пароль и никому его не сообщайте или не используйте повторно для других сайтов. Кроме того, многие сайты поддерживают более надёжную аутентификацию, например двухступенчатую проверку. По возможности, пользуйтесь ей. © The SANS Institute 2013 http://www.securingthehuman.org;

- Шифрование. Большинство сайтов социальных сетей используют сетевой протокол HTTPS для безопасного соединения. HTTPS обеспечивает шифрование данных при передаче по компьютерным сетям. Некоторые сайты, такие, как Twitter, Google+ используют этот протокол по умолчанию, на других нужно сконфигурировать соединение HTTPS. Используйте безопасный протокол HTTPS, если это возможно;

- Электронная почта. С осторожностью относитесь к письмам, которые приходят от имени социальных сетей; злоумышленники легко могут подделать их для атаки. Самый безопасный способ ответа на такие письма непосредственно с самого сайта социальных сетей, например, из закладок; проверяйте сообщения или уведомления только с Web-сайта.

- Вредоносные ссылки/Обман. Будьте осторожны с подозрительными ссылками или ложными публикациями на сайтах социальных сетей. Киберпреступники могут размещать вредоносные ссылки. Если вы щелкните по ним, то попадёте на вредоносные сайты, которые попытаются заразить ваш компьютер. Внимание, если пришло сообщение от друга, это не значит, что он его отправлял - его аккаунт могли взломать. Поэтому если вы получили подозрительное сообщение от члена семьи или друга (например, что его ограбили и ему нужны деньги), свяжитесь с ним по телефону, чтобы развеять сомнения;

- Приложения. Некоторые социальные сети предоставляют возможность установить программы, созданные сторонними разработчиками, например, игры. Помните, эти программы подвергаются минимальной проверке или вовсе не проверяются на предмет наличия недекларированных функций и зловредного кода, через них можно получить контроль над вашим аккаунтом или доступ к персональным данным. Устанавливайте только те приложения, которые вам действительно нужны, загружайте их с известных, проверенных сайтов и сразу же удаляйте после использования;

- Советы по безопасному использованию социальных сетей: http://preview.tinyurl.com/b28a525;

- Информация по безопасности Facebook: http://ru-ru.facebook.com/help/security Facebook;

– Настройки безопасности: http://preview.tinyurl.com/a67munp;

- Безопасность социальной сети ВКонтакте: http://vk.com/security;

- Microsoft: Правила безопасности при использовании социальных сетей: http://preview.tinyurl.com/anqnbp5;

- Термины ИБ: http://preview.tinyurl.com/6wkpae5;

- Ежедневные советы по информационной безопасности Института SANS: http://preview.tinyurl.com/6s2wrkp.

Социальные сети представляют собой мощный и удобный способ общения с миром. Если вы будете следовать нашим рекомендациям, то ваше онлайн общение станет безопасней. Вы можете ознакомиться с дополнительными правилами безопасности на сайте веб сервиса, который вы используете. В случаях несанкционированной активности сообщайте в службу поддержки пользователей.

Основным препятствием на пути выстраивания системы современной защиты от навязывания мнений через соцсети может стать «псевдо-патриотизм» с постановкой заведомо «ложных целей», навязыванием борьбы с «мифическим врагом» и «мнимыми победами» в интересах заочно заработать политические бонусы на патриотизме, проблемах, войне и горе. В этих условиях может сложиться ситуация, когда активно обсуждаются насущные вроде проблемы, но виноваты во всем - власти, социальные группы, национальности, богачи и т.п. Типичными для такого рода «обработки» будут: - присвоение права на «абсолютную» истину, безапелляционное навязывание догм и только своего «правильного» мнения, героизация борцов за «правое» дело, образ «врага» и «разчеловечивание» приверженцев «стана врага», мир делится для таких «проповедников» на тек кто с ними, а остальные - враги, - выбора нет. Эти черты характерны для обработки и вовлечения в экстремистские и террористические сообщества. Будьте осторожны и бдительны при таких признаках в опосредованном общении в соцсетях.

Кроме того, современные средства массовой коммуникации - Интернет, мобильные сервисы, радио и телевизионные СМИ, - используют разработанные изначально военными ведомствами Западных стран особые виды так называемых «ментальных вирусов». Новые виды их разрабатываются сейчас и далее, - как в коммерческих целях, так и в «боевых» геополитических, когда ставится задача манипулирования массовым мнением и поведением конкретных целевых групп.

Этому можно противостоять и рецепт здесь один – это защита тех форм идентичности, которые исторически сложились у народов бывшего СССР. При посещении информационных ресурсов (сервисов), через которые транслируются нереальные, виртуальные смыслы типа – «все же знают, что..; всем известно авторитетное мнение, что…» противостоять этому якобы «общепринятому мнению» может только критическое отношение к любому общему, или авторитетному мнению, не подкрепленному доказательствами компетентных и не заинтересованных специалистов. Любое «задевшее» вас мнение кого бы то ни было – проверяйте, перепроверяйте и, при попытках склонить вас к какому либо образу мыслей, мнению, - никому не доверяйте на слово, без убедительных проверенных вами доказательств. Если ваш опосредованный оппонент, собеседник, высказывает мнение, вызывающее у вас сомнение, - задайте последовательно всего три вопроса ему:

- на основании каких источников собеседник так именно считает?;

- эти источники где (из чего, откуда) взяли эту информацию?;

- первичный источник информации - как и где ее получил, чем она подтверждается?

Обычно при попытках умышленной или неумышленной манипуляции вашим мнением, общение на этих очевидных вопросах прерывается, или собеседник переходит на оскорбления. Это как раз и свидетельствует о бездоказательном навязывании нужного собеседнику мнения.