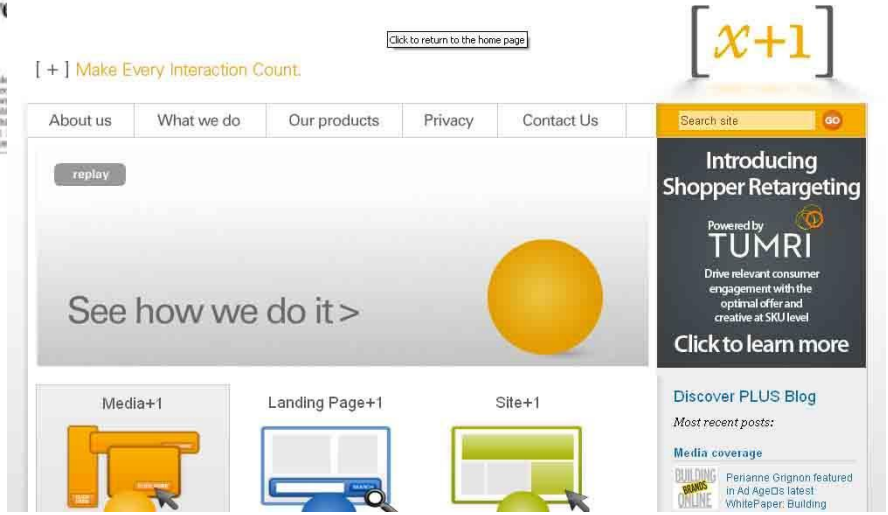
АНОНИМНОСТЬ – ПОСЛЕДНЯЯ ИЛЛЮЗИЯ ИНТЕРНЕТА

Автор презентации: Виталий Цопа

По данным Международного института электросвязи, к концу 2010 года Интернетом будет регулярно пользоваться каждый третий житель Земли. Надо учиться с этим жить.

«Зачем мне анонимность, ведь я не делаю ничего предосудительного, пусть хакеры об этом беспокоятся...», - скажет кто-то. А подумайте: если каждый встречный будет знать ваш домашний адрес, и, при желании, следить за вами? Понравится ли вам такое? Почему же мы так мало внимания обращаем на проблему анонимности в Интернете?



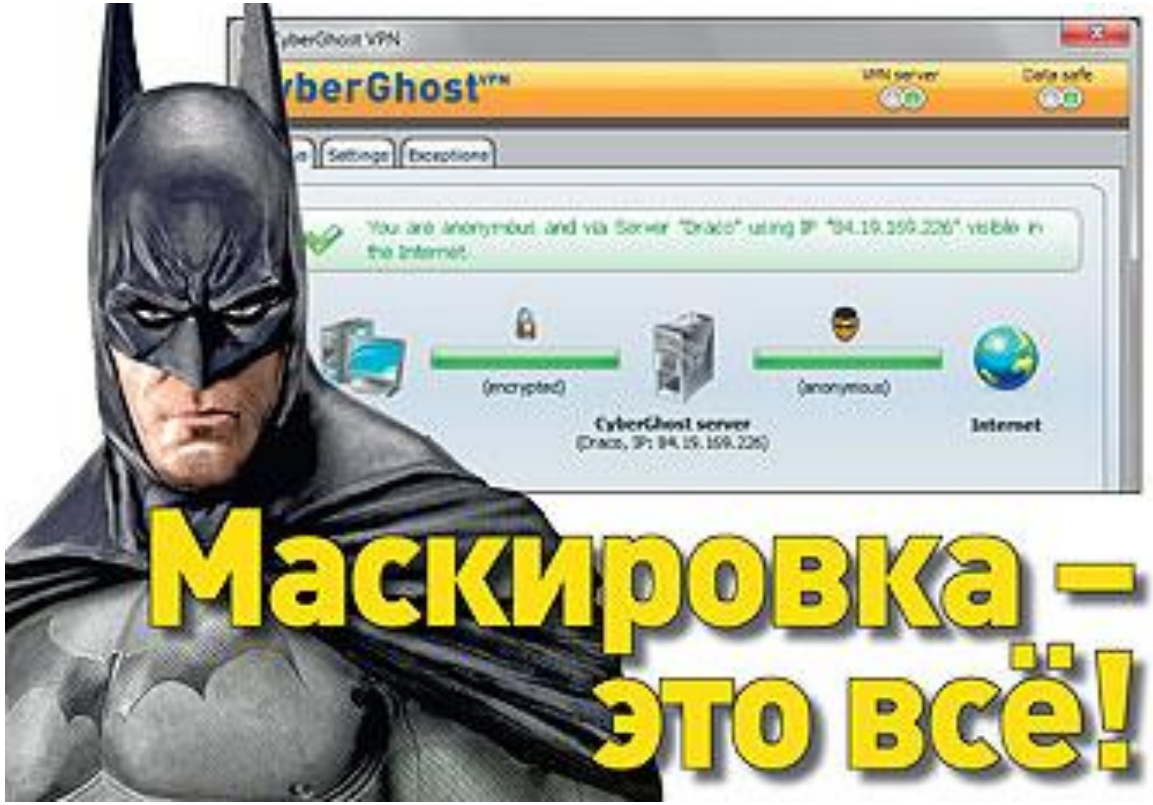
В августе 2010 года внимание «The Wall Street Journal» привлекла деятельность компании [x + 1]. «Вы можете ничего не знать об этой компании, но, вполне возможно, она очень многое знает о вас», - пишет авторитетное издание.

Как за нами следят?

По одному «клику» пользователя компания точно определяет его пол, возраст, семейное положение, годовой доход и другие «характеристики». Количество детей и любимая марка автомобилей, а также хобби и наличие высшего образования также не являются для нее секретом. Для этого вовсе не нужно отслеживать каждую деталь, просто технологии оценки и обработки информации дают достаточно точную характеристику отдельно взятого человека.

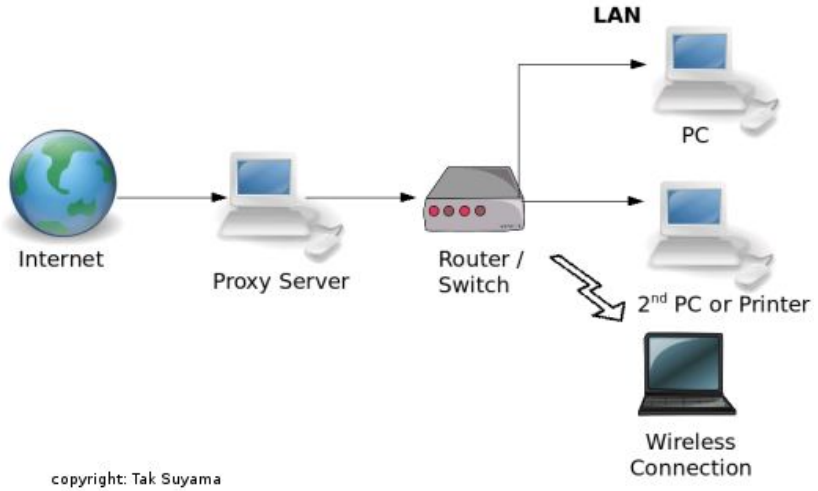
«Мы работаем с брендами, агентствами и медиа-компаниями, чтобы помочь им определить наиболее ценных клиентов», — говорится на сайте компании [x +1]. Там же сообщается, что благодаря новаторской запатентованной технологии Engine, любая рекламная информация или объявление будут доставлены определенному человеку в нужное время. Информацию, собранную [x + 1], различные компании используют для своих целей. Например, компания Capital One Financial, специализирующаяся на выпуске кредитных и дебетовых банковских карт, с помощью этих расчетов определяет, какую кредитную карточку отрекламировать первой определенному посетителю ее сайта.
Проще говоря, компания сначала оценивает, сможет ли конкретный посетитель ее сайта быть хорошим клиентом, а потом решает, стоит ли показывать ему определенную информацию. Такой подход практикует, в частности, популярный ресурс Amazon.com, который анализирует собственную базу данных посетителей, а затем показывает им те новые элементы, которые должны быть им интересны.

А нужно ли «прятаться»?



СПОСОБЫ МАСКИРОВКИ

Когда вы набираете в строке браузера какой-нибудь адрес, то сначала запрос отправляется на сервер DNS*, который преобразует строку символов в набор из 32 нулей и единиц — IP-адрес*, использующийся для маршрутизации. Зная этот адрес, злоумышленник может выведать о человеке очень многое. Например, его реальное местонахождение. Делается это с помощью сервиса whois, который по IP-адресу легко определяет провайдера пользователя. Как же можно себя защитить?



Для начала можно попробовать «спрятаться» с помощью прокси-сервера, который является как бы посредником между компьютером пользователя и серверами Сети. Мы уже выяснили, что главный «предатель» — это IP-адрес, от которого никак нельзя избавиться, потому что он необходим для маршрутизации данных. Но прокси-сервер отправляет запросы на веб-сервера как бы от себя. И он сам получает всю ответную информацию. Так что, на первый взгляд, использование прокси-сервера — гарантия анонимности. Но не так все просто. Оказывается, подавляющее большинство прокси-серверов в своих запросах передают в специальном поле (x-forwarded-for) IP-адрес конечного пользователя. Правда, есть и анонимные службы, вот только найти их не так уж и просто. Кстати, проверить любой прокси-сервер на анонимность можно на сайте www.proxylist.com.

Другой вариант сохранения анонимности в Интернете — использование анонимайзеров (anonymizer). Это, по сути, просто анонимные прокси-сервера, имеющие собственный веб-интерфейс. И работать с ними очень просто. Заходим на сайт, вводим в специальное поле адрес нужного нам сервера — и все. Загружается запрашиваемая страничка, причем вы можете быть уверены в собственной анонимности. Правда, при использовании анонимайзеров придется смириться с парой недостатков. Во-первых, скорость загрузки страниц может значительно уменьшиться. А во-вторых, на сегодняшний день уже практически невозможно найти бесплатный анонимайзер. Когда эти службы только появились, никому и в голову не могла прийти мысль о сборе денег за свои услуги. Теперь же пользователям приходится платить за «роскошь» остаться неузнанным.

А вообще - самой распространенной технологией «слежки» является **cookies** (переводится с английского как «пирожки» или «печенье»). Cookie — это строка символов размером до 4 кб, которую веб-сервер записывает в специальный файл на компьютере пользователя. Технология была разработана для удобства работы в сети. Например, для того, чтобы интернет-магазин мог «вспомнить» пользователя и предложить посмотреть новые поступления товара в зависимости от увлечений человека. А чтобы сохранять конфиденциальность данных, было введено специальное ограничение: считывать информацию из cookies может только тот сервер, который ее записал.

К сожалению, обойти это оказалось проще простого. Записать и считать данные из cookies может скрипт счетчика посещений, который расположен на многих сайтах. В результате система имеет возможность проследить ваш веб-маршрут, узнать ваши увлечения. А это уже, согласитесь, самая настоящая слежка.

Существует еще один способ обеспечения анонимности в Интернете – на сегодняшний день самый надежный. Речь идет о socks-протоколах. Принцип действия этой технологии похож на работу прокси-сервера. Socks-сервер принимает данные от компьютера пользователя, отправляет их на веб-сервера, а затем перенаправляет ответную информацию обратно. Правда, здесь есть и несколько серьезных различий. Во-первых, «общение» клиентского компьютера и socks-сервера происходит не по общепринятым, а по специальным протоколам (socks4, socks5 и т.д.). В результате передача IP-адреса пользователя невозможна в принципе. Кроме того, socks-сервер сам преобразовывает информацию от пользователя в запросы для общепринятых протоколов. А это значит, что ни один сервер «не догадается», что отправляет данные не конечному пользователю, а посреднику. Да и работать с технологией socks очень удобно. Достаточно скачать специальную утилиту SocksCap от компании NEC USA, Inc. Установив эту программу, запустите ее, выберите софт, для которого вы бы хотели получить анонимное соединение (например, Internet Explorer), введите адрес и порт socks-сервера. Все — теперь, запустив браузер из SocksCap, вы можете больше ни о чем не беспокоиться.

«В жизни нет гарантий,
существуют одни
вероятности».

Том Клэнси
(сценарист
компьютерных игр)