Автор: Юрий Ревич © Новая газета ИНТЕРНЕТ И ИТ, РОССИЯ 2493 02.06.2009, 16:59 238

На ваш пароль найдется отзыв

Каждый, кто пользуется Интернетом, оставляет множество следов. Выявить эти следы, обобщить их и составить представление о человеке — задача чисто техническая

Одно из самых удивительных свойств Интернета как коммуникационной среды заключается в том, что при формальной анонимности пользователей человек в этой среде парадоксальным образом оказывается даже более уязвим к разного рода злоупотреблениям, чем в реальной жизни.

Сейчас все больше стали говорить о нарушениях приватности, касающихся в основном (но не только) многочисленных участников различных социальных сетей…

Почти каждый интернетчик состоит в какой-нибудь социальной сети, а чаще и не в одной — суммарная аудитория только двух крупнейших российских ресурсов такого рода, «Вконтакте» и «Одноклассники», превышает общую численность пользователей Интернета в нашей стране. Кроме социальных сетей есть блогосфера и многочисленные форумы, поисковые ресурсы — в общем, каждый, кто активно пользуется Интернетом, даже только как справочником по кулинарным рецептам и сборником рефератов, оставляет множество следов. Выявить эти следы, обобщить их и составить более-менее полное представление о человеке — задача чисто техническая. И даже если вы тщательно следите за тем, чтобы не оставлять своего реального адреса, номера телефона и не разглашать деталей биографии, тем не менее можно узнать довольно много о ваших склонностях, привычках и предпочтениях, и даже прогнозировать ваше поведение.

А такая информация ценится на вес золота. Владимир Коровкин в своей статье (см. на этой же полосе) объяснил, почему сейчас буквально все — от гигантов вроде Google или Wal-Mart до мелких торговых и рекламных фирм — заняты сбором подобной информации. Она позволяет осуществлять адресную рекламу — такую, которая естественным образом вписывается в круг ваших личных интересов и потому не вызывает отторжения и раздражения, как обезличенная медийная реклама. И в такой постановке вопроса это действительно выгодно всем сторонам: и рекламодателям, которые получают значительно больший отклик, и пользователям, которых обычная реклама уже достала, и самим социальным сетям, которые наконец получают шанс монетизироваться и начать окупать свою деятельность.

Но пользователям почему-то в массе своей не нравится, что их тихо «посчитали», и они выступают против сбора персональной информации. Так, член Законодательного собрания Нью-Йорка Ричард Бродский выдвинул законопроект, запрещающий не только собственно сбор персональной информации, но и демонстрацию им адресной рекламы без предварительного согласия пользователей. Любопытно, что в то время как интернет-гиганты, живущие за счет рекламы (Google, Yahoo, AOL), разумеется, против законопроекта, Microsoft его поддержала, лишь попросив доработать так, чтобы он охватывал все компании, живущие за счет рекламы в Сети (а не только те, что демонстрируют адресную рекламу). Аналогичный проект был выдвинут в штате Коннектикут.

В Европе подобные настроения еще более распространены. Так, «отец Интернета» сэр Тим Бернерс-Ли возмущается сбором данных о пользователях: «Почтальон не вскрывает мои письма, телефонная компания не прослушивает мои разговоры. А ведь при использовании Интернета я сообщаю о себе намного более личные данные». Использование таких данных без разрешения, по его мнению, возмутительно. Эти настроения нашли поддержку на уровне Еврокомиссии, которая категорически запрещает сбор личных данных без согласия пользователей и сейчас ведет судебный процесс против ряда британских интернет-провайдеров, уличенных в сборе персональных данных.

Можно ли эту реакцию отнести только к разряду массовых фобий-«страшилок», как это квалифицирует Коровкин? Конечно, иррациональный протест против сбора обезличенной статистики ни на каких внятных аргументах не основан. Беда в том, что методы сбора такой информации позволяют не ограничиться статистикой, эти методы легким движением мышки дают возможность предельно детализировать и индивидуализировать получаемые данные.

А раз такая возможность есть, значит, ею кто-нибудь обязательно воспользуется, и не исключено, в каких-нибудь неблаговидных целях (см. «под текст»). И будем откровенны: ранее, до появления коммуникационных сетей, такой сбор персональной информации всегда квалифицировался как шпионаж, персональная слежка, и не совсем понятно, почему нужно менять свое отношение к предмету с появлением цифровых технологий.

Причем в этих возможностях есть, конечно, и свои плюсы, и в них даже существует некая объективная необходимость, что трудно оспорить — смотря кто и зачем этим пользуется (об этом далее). Обратим также внимание на одно существенное отличие современных систем онлайновой слежки от традиционных способов — первые намного дешевле и проще в употреблении и хотя бы в теории доступны каждому, а не только спецслужбам или частным сыскным агентствам со специально обученными кадрами.

Чтобы не быть голословным, я связался с разработчиками одной из самых совершенных систем такого рода — компанией VS Lab. Ее подход отличается некоей глобальностью и универсальностью: разработанная там система под названием SkyPetr, основанная на передовых математических методах, одинаково годится для рекламщиков (для упомянутого выше анализа аудитории социальных сетей), государственных органов (например, для выявления и предупреждения экстремизма), для фильтрации «опасных связей» (например, для ограждения детей от нежелательных контактов) и многих других подобных вещей.

О перспективах, положительных и отрицательных сторонах системы SkyPetr я поговорил с**Екатериной Должиковой**, директором по развитию VS Lab.

— Какие реальные применения ваш проект уже находит?

— Увы, конкретных заказчиков я назвать не могу, скажу лишь, что это были коммерческие структуры, которым требовалась информация для проведения маркетинговых компаний. Сейчас к нам обратились специалисты (подразумеваются «специалисты» из спецслужб. — Ю.Р.), которым необходим анализ нескольких социальных ресурсов с точки зрения их безопасности и, скажем так, привлекательности для пользователей с «незаконными интересами и наклонностями», вроде детской порнографии и педофилии. Мы не стараемся ориентироваться на какой-то один сегмент рынка: считаем, что наши разработки могут найти применение в самых разных областях...

— Вы, наверное, понимаете, что ваши технологии могут также использоваться в качестве отличного инструмента для шпионажа за пользователями, в том числе со стороны не только спецслужб, но и криминальных элементов. В частности, декларированная вами защита детей от нежелательных контактов точно так же может использоваться в обратную сторону: скажем, для выявления подростков, склонных к определенного рода контактам. Ваши технологии легко использовать для выявления потенциальных объектов для шантажа и т.д.

— Вопрос, с одной стороны, вроде бы совершенно логичный, с другой — мне кажется, это старая, как мир, попытка переложить ответственность с человека на инструмент. Да, безусловно, любая технология, позволяющая так или иначе моделировать социальную структуру общества, прогнозировать поведение его членов и составлять их социальный и психологический портрет, может быть использована как во благо, так и во зло, и мы прекрасно осознаем свою ответственность.

Мы в своих выступлениях на «Инфофоруме» (конференция по информационной безопасности) в конце января 2009 года подняли целый пласт проблем, связанных как раз с отсутствием на сегодняшний день инструментов определения «опасных связей» и прогнозирования возможности незаконных действий пользователя. Это и повсеместно встречающийся, особенно среди молодежи и школьников, моббинг (травля), и виктимизация (процесс превращения лица в жертву преступления. — Ю.Р.) интернет-пользователей, и, кстати, шантаж, и распространение нелегального контента. А рассуждая в духе «...ваша технология позволяет собирать сведения для шантажа», следует признать вредным и сам Интернет, и обезболивающие препараты, поскольку фактически все они могут служить и наркотиками.

Надо очень четко понимать, что наступает момент, когда НЕпоявление какого-либо средства или технологии куда опаснее, чем возможные последствия от его появления. Я думаю, ни для кого не секрет, что уже давно в Интернете используются разные виды информационного оружия, проводятся четко спланированные атаки. Отсутствие средств анализа и распространения контента и влияния Интернета на человека в целом приводит к тому, что Интернет с каждым днем становится все более опасным, что в нем применяются откровенно аморальные методы продвижения продуктов и услуг, разного рода пропаганда и проч. И если с этим ничего не делать, то ситуация будет только ухудшаться.

— Как вы относитесь к общим опасениям по поводу сбора данных о пользователях и сведении их в единые базы: понятно, что де-факто это уже не остановить, но многие возражают, квалифицируя это как нарушение приватности и высказывая опасения в связи с возможной утечкой таких баз и попадании их в «плохие» руки?

— Во-первых, базы существуют на каждом ресурсе, где пользователь регистрируется, при этом большинство ресурсов никак не озабочены системой безопасности хранения этих баз. Данные пользователей лежат едва ли не в открытом доступе. Во-вторых, нельзя перекладывать всю ответственность на ресурсы. Люди должны наконец осознать, что понятие «виртуальная реальность» устарело. Вы же не оставляете, к примеру, свой кошелек на прилавке магазина, отходя в соседний отдел, и не диктуете номер своей кредитки по телефону, стоя посреди людной площади? Пора привыкать к тому, что и в Сети надо соблюдать те же правила безопасности. 80% пользователей имеют одинаковые логины и пароли на всех своих профилях и аккаунтах: электронной почты, социальных сетей, форумов и т.д. Киберпреступники, получив логин и пароль с незащищенного форума про «вышивание крестиком», совершенно спокойно получают доступ к почте и другим ресурсам, у которых как раз очень надежная защита данных.

Протестовать против создания баз, мне кажется, могут только ну уж совсем малообразованные люди. Весь Интернет, да что там Интернет — все общество строится на создании объединяющих баз. Никто же не возмущается по поводу обязательной регистрации по месту жительства, например (да ладно, еще как возмущаются. — Ю.Р.). А насчет утечек — опять же это вопрос не только к разработчикам. Пришло время, когда пользователям надо начинать задумываться о том, где и какую информацию о себе оставлять и, самое главное, какие действия совершать.

Конечно, Екатерина Должикова права: системы, подобные SkyPetr, есть всего лишь инструмент. Но о том, что он может быть использован и в преступных целях, не нужно забывать: классическим примером целой процветающей преступной отрасли, основанной на сборе данных о пользователях (как минимум об их адресах электронной почты), является рассылка незапрошенной корреспонденции — спама.

И зачем-то информацию о пользователях ведь собирают подпольно: так, в Великобритании зафиксирован сайт, собирающий резюме уволенных сотрудников. Оказалось, что за вполне законной на первый взгляд деятельностью стоит вымышленное кадровое агентство. И эксперты говорят, что большинство посланных резюме содержат по крайней мере восемь позиций персональных данных, которые могут быть теоретически использованы для «кражи личности». Аналогичная история случилась летом прошлого года и в России, где хакерская группировка Phreak предлагала спамерам на подпольных форумах за 600 долларов базу данных, содержащую тысячи резюме, собранных в автоматическом режиме с крупнейших сайтов по поиску работы. Такие базы могут использоваться, например, для адресных фишинговых атак — если клиенту поступает письмо якобы от банка, где он действительно имеет счет, вероятность успеха мошеннической операции резко возрастает.

Будем объективны: наверное, тенденцию к сбору персональных данных, как в маркетинговых целях, так и в интересах служб охраны порядка, уже не переломить. Но это не значит, что следует забывать о возможных негативных последствиях такой тенденции и пускать дело на самотек. Впрочем, сами пользователи тут могут себе помочь больше других, если действительно, как говорит Екатерина, начнут «задумываться о том, где и какую информацию о себе оставлять».

Под текст
Не сообщайте пароли, явки и PIN-коды

Есть такое понятие — «кража идентификационной информации, удостоверяющей личность». В США «кража личности» уже давно является преступлением номер один. Типовой пример: злоумышленник узнает номер социального страхования какого-нибудь человека, заводит себе дюжину кредитных карточек на его имя, в результате платить по счетам приходится этому человеку.

Подоспела и свежая российская история. 20 мая сотрудники Управления «К» МВД России задержали в Москве семейную пару, обманувшую более 10 тыс абонентов сотовой связи примерно на 100 млн рублей. При помощи специальной программы мошенники отправляли SMS в платежную систему с номера, который идентифицировался как номер потенциальной жертвы. Система, в свою очередь, отправляла абоненту 4-значный ПИН-код для доступа в систему управления счетом. Чтобы его узнать, мошенники звонили абоненту, представлялись устроителями лотерей и предлагали получить денежный приз, который якобы выиграл абонент. Узнав PIN-код и паспортные данные абонента, мошенники получали полный доступ к его счету, переводили деньги через другие «электронные кошельки» на пластиковые карты, а затем обналичивали их.

Сотрудники Управления «К» полагают, что сейчас они задержали организаторов обширной сети аферистов; исполнителей предстоит установить. Против задержанных возбуждено уголовное дело по ст. 272 УК РФ (неправомерный доступ к компьютерной информации) и ст. 159 УК РФ (мошенничество).

Это преступление — типичный пример «кражи личности», полный аналог того, что в Интернете носит название фишинга — рассылки подложных писем от лица реальных организаций.

Автор: Юрий Ревич © Новая газета ИНТЕРНЕТ И ИТ, РОССИЯ 2493 02.06.2009, 16:59 238
URL: https://babr24.com/?ADE=78142 Bytes: 13853 / 13809 Версия для печати

эл.почта: babrmarket@gmail.com