УДК 004

РИСКИ ВОВЛЕЧЕНИЯ БИЗНЕСА В СОЦИАЛЬНЫЕ СЕТИ

Губенко Н.Е.[1)], Целуйко О.А.[2)]
Донецкий национальный технический университет
[1)] к.т.н., доцент; [2)] студент

Введение

По мере того как растет интерес к социальным сетям, растут и его ожидания относительно появления новых угроз. Последней тенденцией стало вовлечение бизнеса в социальную сеть. Так компании получают потенциальных клиентов, открывающиеся возможности для продвижения товаров и услуг, для поиска персонала или проведения рекламных акций, какой бы сферы они ни касались .Социальная сеть облегчает задачу поиска целевой аудитории. Анализируя данные профилей, можно сделать большое количество обоснованных предположений о пользователе. На подобные услуги растет спрос - появились компании, которые обучают маркетологов тому, как вести бизнес в социальной сети. В настоящее время одна из самых востребованных вакансий на рынке - это сотрудник по продвижению в социальных сетях. Новые возможности для бизнеса всегда сопровождаются новыми рисками.

Основные проблемы

Социальные сети хранят практически все, что интересует обычного пользователя: его личные данные, привычки, хобби, социальное положение, вкусы и пристрастия, поведение в интернете, даже распорядок дня и местоположение. Социальная сеть знает все о друзьях и интенсивности общения. Здесь размещено немалое количество информации о своих родных и близких, доступны публичные данные о связях между пользователями. Анализируя поведение людей в интернете, социальная сеть сохраняет все, что пользователи там оставили. Что же касается безопасности этой информации, то специалисты обеспокоены по поводу того, что парольная защита ослабевает с приходом в Интернет все большего количества людей. Это происходит, прежде всего, из-за использования простых паролей. Кроме применения простых паролей, пользователи зачастую используют одинаковые пароли на самых разных местах: на сайтах, личных кабинетах провайдера, электронной почте; для социальных сетей и так далее, что позволяет легко подобрать пароль. Не маловажным остается тот факт, что пользователи чаще всего используют один-единственный аккаунт у всех случаи. Почти на всех популярных сайтах, которые посещает большое количество людей, установлены специальные шлюзы для доступа в социальные сети. Через любой сайт, оснащенный подобным шлюзом, пользователь компании может общаться, хотя и ограниченно, с социальной сетью. JavaScript, загруженный из социальной сети, отслеживает DOM-событие on-Click- это позволяет узнать, по какой ссылке был покинут сайт .Если на том сайте, куда перешли, имеется кнопочка Like или connect, то будет известен маршрут движения. Таким образом, социальная сеть имеет возможность узнать, с какого сайта вы пришли, сколько времени там провели, когда покинули. Когда третьи лица становятся собственниками подобной информации неизбежны нарушения безопасности, начиная с использования профилей (взлом, клонирование ,сегодня можно приобрести пароль от какого угодно ящика или аккаунта в социальной сети), до потери денег на банковском счете. Некоторые сайты могут быть интегрированы с платежными системами, и как результат в сети может оказаться конфиденциальная пользовательская информация. Для бизнеса сложность в том, что очень часто нет возможности закрыть доступ к социальной сети всем. Кроме того, пытаясь ограничить пользование интернет-сообществами, они провоцируют сотрудников говорить за пределами организаций, что способствует обнародованию информации, которую компании не хотели бы публиковать.

За последние два года наблюдается тенденция к использованию сокращенных URL-адресов. Сервисы, подобные Twitter, где длина сообщений ограничена, часто используют сокращение URL. Переходя по ссылке, пользователь сначала попадает на сервис сокращенных URL, а затем автоматически перенаправляется по целевому адресу. А это значит, что о переходе становится

известно третьей компании. По сути, весь пользовательский трафик проходит через одну точку — t.co, что позволяет компании иметь мощные аналитические возможности для анализа поведения пользователей в Интернете. Другой аспект этого вопроса заключается в том, что большинство сервисов не имеют функции предварительного просмотра URL, на который они, в конечном счёте, указывают, поэтому хакеры могут легко замаскировать полу-доверенное имя под сокращение URL. Это приводит к дальнейшей эскалации атак.

Еще одной тенденцией начиная с 2011г, стало повсеместное использование федеративных средств аутентификациина основе социальных сетей или иных сервисов. К примеру, сайт газеты «Ведомости». Поняв, что все пользователи присутствуют в социальной сети, газета поступила просто: предложила своим посетителям сайта логиниться с помощью этой сети. И так происходит повсюду. Большинство сайтов не имеет желания накапливать собственную пользовательскую базу, потому что пользователи не любят и не хотят регистрироваться. Они предпочитают делать это централизованно — через «ВКонтакте», «Яндекс», Mail.ru, Facebook или что-то другое. Это удобно и для пользователей, так как избавляет их от необходимости лишний раз регистрироваться, и дает социальным сетям дополнительную информацию о действиях пользователя на внешних сайтах. Не остается без внимания специфическая особенность, связана с возможностью узнать о местопребывании человека. Сочетание мобильных устройств, сервисов и социальных сетей предоставляет значительные возможности для эффективной работы, но в то же время оставляет легкие в обнаружении следы личных данных пользователей в сети.

Социальная сеть — великолепный источник сбора аналитики о компании. Не менее серьезную проблему представляет угроза переманивания сотрудников. Социальная сеть дает широкие возможности для просмотра чужих профилей. Пользователь может указать свои интересы, сведения о работе, учебном заведении и т.п. По ключевым словам представители рекрутинговых агентств могут отыскать нужных им кандидатов и потом их перекупать. Существуют сети, специально созданные для личного продвижения профессионалов — например, linkedln. Еще одна возможность – размещение вакансий через социальную сеть. Рекрутинговые агентства проводят специальные мини-обучения, рассказывают, как правильно размещать и продвигать свое резюме[1].

Выводы

Поскольку запретить компаниям работать в Интернете и социальных сетях нельзя, такое поведение в сети будет процветать, однако это сильно мешает бизнесу. Дальше придется или смириться, или разумно контролировать, пока компании не поймут, что нужно тратить время на обучение сотрудников правильному поведению в социальных сетях. Сопротивляться социальным сетям нет смысла и возможности, они есть и никуда не уйдут. Это слишком удобная технология, чтобы ее не использовать. Например, создание корпоративных социальных сетей – это уже данность для ряда крупных компаний. Чем дальше, тем больше будет распространяться интеграция между мобильными терминалами, сервисами обмена данными, социальными сетями и другими аналогичными средствами. При дальнейшей работе в соц. сети лучше всего обращать внимание на риски и работать с ними – какую-то часть принимать, частью управлять. Пользователям социальных сетей будет несложно следовать ряду простых правил, которые сделают их жизнь более безопасной, не распространять: личные данные — имена, фамилии, телефоны, емейлы, данные icp и url, паспортные данные; фотографии, ссылки на Facebook, youtube, google; ссылки на новостные сайты и магазины. Это позволяет вычислить профиль интересов. Этим пользуются поисковики для рекламы.

Список использованных источников

1. Jet Info. Электронный ресурс. Режим доступа к статье: http://www.jet.msk.su/pres_center- Вы пользуетесь социальной сетью?
2. Securelise. Электронный ресурс. Режим доступа к статье: http://www.securelist.com/ru/analysis-Опасности на пути пользователей социальных сетей.
3. kaspersky. Электронный ресурс. Режим доступа к статье: http://www.kaspersky.ru/reading_room - «Лаборатория Касперского» публикует статью «Угрозы социальных сетей»
4. «Директор информационной службы». Электронный ресурс. Режим доступа к статье: http://www.osp.ru/cio/2011/12/13012286-Угрозы социальных сетей.