Как не попасть в сети социальных сетей

В настоящее время порядка 1,8 млрд человек пользуются социальными сетями, при этом пользователями различных онлайн-ресурсов социальных сетей являются более 64% всех интернет-пользователей. Самой популярной по количеству активных пользователей в месяц уже на протяжении многих лет подряд остаётся Facebook, пользователями которой в 2015 были более 1,3 млрд человек. И это несмотря на то, что широкое распространение социальные сети получили сравнительно недавно, в 2003-2004 гг.

Поэтому излишне говорить, что сегодня социальные сети прочно вошли в ежедневный «рацион» большинства интернет-пользователей, особенно молодёжи до 30 лет, а потому многие продолжают пользоваться ими и на работе. По данным опросов, проведённых в Европе и США, посещение не связанных с работой интернет-сайтов (включая социальные сети) является второй «статьёй» нецелевого расходования рабочего времени (этим заняты 34% сотрудников компаний, на первом месте – общение с коллегами на нерабочие темы, чем регулярно занимаются 43% сотрудников). Причём на сайты социальных сетей заходят как с рабочих компьютеров, так и с личных, как правило, мобильных устройств, часто также используемых и для выполнения некоторых служебных функций (например, смартфоны с доступом к рабочему почтовому ящику).

В то же время и злоумышленники активно используют социальные сети для сбора конфиденциальной информации и/или персональных данных. Арсенал их методов достаточно широк:

1. Фишинг. Жертву заманивают на сайт, выдающий себя за настоящий, где предлагают сообщить конфиденциальную информацию, которая направляется злоумышленникам.

   Недавно пользователи социальной сети Facebook подверглись очередной атаке мошенников. Используемая схема была не нова, как и преследуемые злоумышленниками цели: жертву обманным путём побуждают установить расширение для браузера, с помощью которого злоумышленники в дальнейшем смогут украсть персональные данные жертвы.

   От имени скомпрометированного Facebook-аккаунта злоумышленники публикуют в социальной сети пост со ссылкой на некое видео для взрослых, якобы размещённое на популярном сервисе YouTube. Для привлечения внимания потенциальных жертв в посте с данным видео отмечаются пользователи из списка друзей скомпрометированного аккаунта. Расчёт ведётся как на любопытство пользователя, так и на любопытство его друзей, которым захочется посмотреть загадочное видео с пометкой «18+». При переходе по ссылке открывается страница, оформленная в стиле популярного видеосервиса YouTube. Однако, достаточно одного взгляда на адресную строку, и становится понятно, что страница не имеет никакого отношения к указанному сервису. При попытке запустить видео возникает баннер с предложением установить расширение для браузера. Злоумышленники рассчитывают на то, что жертва не станет вдаваться в подробности и даст разрешение на установку. После установки расширению даются права на чтение всех данных в браузере, что позволяет мошенникам заполучить введённые пароли, логины, данные банковских карт и другую конфиденциальную информацию пользователя. Кроме того, в дальнейшем расширение может продолжить распространять ссылки на себя в Facebook, но уже от имени самого пользователя среди его друзей.
2. Внедрение зловредного ПО. Подобное ПО размещают на взломанных сайтах, засылают на недостаточно защищённые системы или отправляют ссылки на него в сообщениях электронной почты.
3. Использование методов социальной инженерии. Существует целый класс методов, целью которых является управления действиями пользователя-жертвы без применения технических средств. При этом злоумышленники стараются создать условия, в которых жертва сама сообщает необходимую им конфиденциальную информацию. Такие атаки характеризуют нестандартный подход, достаточно высокая сложность и степень организации.

   В социальных сетях злоумышленники знакомятся с потенциальной жертвой и входят к ней в доверие для склонения жертвы к совершению нужных действий, например, открытия определённой ссылки. Наиболее распространённый сценарий следующий:

   - сбор доступной в социальной сети информации о пользователе, его интересах, предпочтениях и контактах;
   - создание аккаунта с учётом интересов и биографических данных жертвы (год и место рождения, школа, институт и т.п.);
   - добавление в «друзья» к тем, кто есть в списке контактов жертвы;
   - используя созданное «прикрытием», установление контакта с жертвой.

   Велика вероятность, что, получив ссылку с подготовленного таким образом аккаунта, потенциальная жертва нажмёт на неё. В противном случае злоумышленник может попробовать

© 2016 UBS, www.ubs.ru

более изощрённый способ – взломать аккаунт пользователя, которому доверяет жертва, и отправить ссылку от его имени.

Нажав на присланную злоумышленником ссылку, жертва попадает на сайт со зловредным ПО, позволяющим преступникам получить доступ к компьютеру. Таким образом, неосторожное пользование социальными сетями может способствовать проникновению хакеров как на личные устройства, так и в корпоративную сеть компании, если используется рабочий компьютер.

4. Подбор паролей. Обладая информацией о пользователе, которую легко найти в социальных сетях, можно попробовать угадать пароль к его аккаунту. Также можно с помощью специального ПО перебрать огромное количество вариантов, воспользовавшись ассоциативной базой данных или техникой словарной атаки, когда несловесные комбинации исключаются, а словесные модифицируются в соответствии с определёнными правилами.

Как же не попасть в сети злоумышленников при пользовании социальными сетями? Что может простой пользователь противопоставить хитрости и изобретательности злоумышленников?

Рецепты защиты просты, основная сложность, как это обычно бывает – постоянно им следовать:

1. Не следует принимать приглашения и иные запросы от незнакомых адресатов. А если приглашение прислал знакомый вам человек, нелишне убедиться, что он его действительно отправлял.
2. Как и в случае с электронной почтой, опрометчиво открывать незнакомые и подозрительные ссылки, загружать и устанавливать неизвестные плагины и расширения браузеров и иное ПО.
3. Третья рекомендация представляется наиболее важной. Сегодня у пользователей социальных сетей сформировалась довольно устойчивая тенденция выставлять свою жизнь «напоказ», публикуя массу личной (вплоть до интимной) информации о себе и своей жизни. Причём зачастую наряду с личной информацией огласке придаётся и служебная.

   Публикуемая информация может быть совершенно, на первый взгляд, невинной, однако усердному и целеустремлённому злоумышленнику не составит особого труда «нацедить» из разрозненных публикаций «объекта наблюдений» достаточно сведений, чтобы провести успешную атаку против коллег «объекта» или его самого.

   Поэтому всегда необходимо понимать, оценивать последствия и, в абсолютном большинстве случаев, воздерживаться от размещения в интернете личной и служебной информации, будь то пост в социальной сети, неправильно «расшаренный» файл в Dropbox или Google Drive, или даже фотография маркерной доски из переговорной.

Подготовлено по материалам СМИ

© 2016 UBS, www.ubs.ru