Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Конфиденциальность
- Безопасность

Безопасность в социальных сетях

ОБ АВТОРЕ

Автор этого выпуска – Тэд Демопулос. Тэд – консультант в сфере информационной безопасности с многолетним стажем. Он также преподает в институте SANS более 10 лет такие курсы, как SEC401/501 и MGT414/512. Больше информации о Тэде вы можете узнать на его сайте http://demop.com.

ОБЗОР

Социальные сети, такие, как Facebook, Twitter, Google+, ВКонтакте, Одноклассники и LinkedIn являются мощным инструментом. Они позволяют находить людей по всему миру, общаться и обмениваться информацией. Однако все эти возможности таят в себе и ряд опасностей не только для вас, но и для членов вашей семьи, друзей и работодателей. В этой статье мы поговорим о возможных рисках и способах безопасного использования этих сайтов.

КОНФИДЕНЦИАЛЬНОСТЬ

Прежде всего, в социальных сетях не следует размещать личные данные и конфиденциальную информацию. Чем это грозит:

- **Негативным влиянием в будущем:** Во многих компаниях просмотр страницы в социальных сетях является частью проверки кандидата. Компрометирующие факты или фото, не важно, какой давности, могут помешать найму или продвижению по службе. Кроме того, многие университеты подобным образом проверяют потенциальных студентов. Настройки конфиденциальности не всегда помогают, так как сотрудники компании могут посмотреть вашу страницу до того, как наймут вас.
- **Атаками на вас:** Киберпреступники могут собрать конфиденциальную информацию о вас и атаковать вас с помощью ваших же личных данных. Например, некоторая информация подскажет ответ на секретный вопрос для получения пароля, поможет написать правдоподобное письмо по электронной почте или получить кредитную карту на ваше имя. Кроме этого, эти атаки могут представлять опасность и в реальной жизни, если преступники получат ваш адрес проживания или работы.
- **Причинением вреда работодателю:** Преступники или конкуренты могут использовать против вас то, что вы опубликуете о своём работодателе. Эта информация может навредить не только вам, но и испортить репутацию вашей компании. Прежде чем размещать какую-либо информацию о вашем работодателе, убедитесь, что это не противоречит политикам компании.

Безопасность в социальных сетях

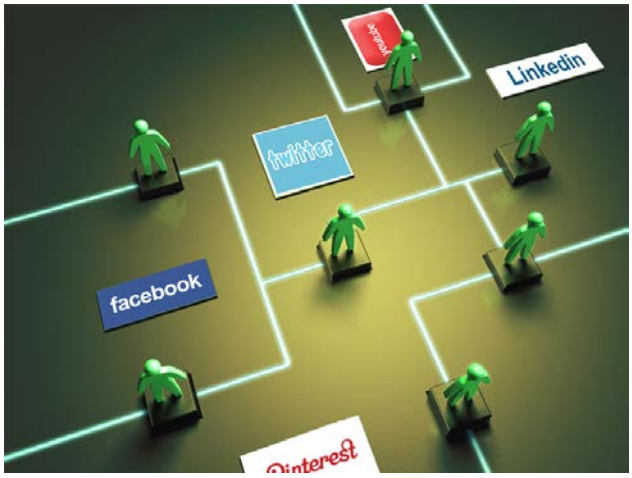
Ограничьте публикуемую информацию – это лучшая защита. Безусловно, настройки конфиденциальности обеспечивают некоторую защиту, но помните, что эти настройки часто неочевидны и могут меняться без вашего согласия. Всё, что вы считаете скрытым, в один момент может стать доступным для всех по ряду причин. Безопасность конфиденциальной информации может зависеть и от людей, с которыми вы ей делились. Чем больше количество контактов или друзей, с которыми вы обменивались личной информацией, тем выше риск того, что информация станет доступной общественности. Существует единственный способ защиты конфиденциальной информации: если вы не хотите, чтобы ваша мать или ваш начальник увидели ваши записи, не следует их размещать в сетях.

Помните, что ваши друзья тоже могут разместить в сети информацию о вас. Вам может навредить доступность персональных данных или компрометирующих фотографий. Убедитесь, что друзья это понимают и не публикуют то, что не следует. Если они все-таки разместили что-то, что вы не хотите афишировать, попросите это удалить. Со своей стороны тоже не размещайте информацию о друзьях без их согласия.

БЕЗОПАСНОСТЬ

Злоумышленники используют сайты социальных сетей не только для поиска компромата, но и для атаки на вас или ваши мобильные устройства. Вот некоторые шаги, которые помогут вам защитить себя:

- **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.



Социальные сети интересны и полезны, но будьте осторожны с тем, что публикуете и кому доверяете.

- **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 веб сайта.

Безопасность в социальных сетях

- **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.

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.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

11 советов 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 информационной безопасности:
http://preview.tinyurl.com/6wkpae5
Ежедневные советы по информационной безопасности Института SANS:
http://preview.tinyurl.com/6s2wrkp

УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт: http://www.securingthehuman.org.

Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.
Перевод: Александр Котков