Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Приватность
- Безопасность

Социальные сети

Обзор

Социальные сети, например, сайты Facebook, Twitter, Instagram и LinkedIn – отличные ресурсы, позволяющие встречаться, общаться и обмениваться информацией с людьми по всему миру. Но кроме возможностей, они приносят и риски, не только для вас, но и для вашей семьи, друзей и работодателей. В этом выпуске мы поговорим о возможных опасностях и способах безопасного посещения этих сайтов.

Об авторе

Таня Бэккем – консультант по безопасности с большим опытом. Более десяти лет она является автором и инструктором SANS, читает курсы SEC502, SEC542, SEC401, MGT414, AUD507 и многие другие. Ведет записи в Twitter **@tbaccam**.

Приватность

Самая главная задача при посещении социальных сетей – сохранение персональных данных. Потенциальная опасность заключается в следующем:

- **Влияние на будущее**: В некоторых компаниях просмотр страниц социальных сетей является частью проверки кандидатов. Неприличные или компрометирующие фотографии или записи, вне зависимости от срока давности, могут помешать получить работу или повышение. Такие проверки проводят и многие университеты для своих студентов. Настройки безопасности не всегда могут защитить страницу от просмотра, например, вас могут попросить «лайкнуть» их страничку, подписаться на новости или посмотреть ваши записи через другие сайты.
- **Атаки**: Кибер мошенники, проанализировав ваши записи, могут получить доступ к вашей личной или служебной информации. Например, подобрать ответы на «секретные вопросы» и сбросить пароль, подготовить целенаправленную атаку на вас, так называемую фишинг атаку или позвонить кому-нибудь из коллег от вашего имени. Помните, что такие атаки могут быть не только виртуальными, но и перейти в реальную жизнь, например, выяснить ваш адрес или место работы.
- **Непреднамеренный вред работодателю**: Преступники или конкуренты могут воспользоваться конфиденциальной информацией, которую вы публикуете о своей компании, и причинить ей вред. Также, ваши записи могут испортить репутацию вашей организации. Убедитесь, что вы ознакомились с политикой компании перед тем, как публиковать информацию о своей работе, так как некоторые записи в социальных сетях могут контролироваться.

Лучший способ защиты – сократить публикации в сетях. Конечно, настройки конфиденциальности обеспечивают некоторую защиту, но они сложные и часто меняются без уведомления. Все, что находилось в закрытом доступе, в один момент становится достоянием общественности. Кроме того, конфиденциальность ваших сообщений

Социальные сети

сохраняется до тех пор, пока вы не поделитесь ими с друзьями. Чем большему количеству друзей вы их отправите, тем выше вероятность того, что информация станет доступна всем. Прежде, чем что-то размещать, представьте, что это будет доступно всем и сохранится в Интернете навсегда.

Наконец, следите за тем, что ваши друзья публикуют о вас. Если что-то вас смущает, попросите это удалить. Если они не соглашаются или игнорируют просьбу, обратитесь в службу поддержки сайта. Со своей стороны, тоже не размещайте лишнего и компрометирующего о других.



сайты социальных сетей приносят удовольствие общения и предоставляют много возможностей, но будьте осторожны с тем, чем делитесь и с кем делитесь.

Безопасность.

Поговорим о некоторых шагах, которые помогут обеспечить безопасность аккаунтов и онлайн активности.

- **Логины**: защитите каждый свой аккаунт сильным и уникальным паролем и не делитесь им ни с кем. Большинство сайтов социальных сетей поддерживают усиленную защиту, например, двухступенчатую верификацию. Используйте эту функцию, по возможности. Наконец, никогда не заходите с аккаунта социальных сетей на другие сайты, в случае взлома вы подвергнете опасности все свои аккаунты.
- **Настройки конфиденциальности**: Если вы используете настройки конфиденциальности, регулярно их проверяйте и тестируйте. Сайты социальных сетей часто их меняют и можно легко ошибиться. Многие приложения и сервисы позволяют вам отмечать свое местоположение в публикациях (так называемые геотеги). Регулярно проверяйте их настройки, если не хотите афишировать свое местоположение.
- **Шифрование**: Сайты социальных сетей используют шифрование, так называемое HTTPS соединение. Некоторые сайты, например, Twitter и Google+ используют такое соединение по умолчанию, другие требуют ручной настройки. Проверьте настройки аккаунта социальных сетей и, по возможности, установите эту функцию по умолчанию.
- **Электронная почта**: С осторожностью относитесь к письмам от имени сайтов социальных сетей, злоумышленники часто подделывают такие письма и используют для атаки. Самый безопасный способ ответа на такие письма непосредственно из аккаунта этой сети, лучше из закладок, только потом следует открывать письма и отвечать на запросы.
- **Вредоносные ссылки/мошенничество**: Будьте осторожны со ссылками или информацией, публикуемой в социальных сетях. Плохие парни часто используют такие сайты для атак. Если сообщение приходит от вашего друга, это не значит, что он его действительно отправлял, его аккаунт могли взломать. Если члены семьи или друзья присылают подозрительное сообщение (например, что

Социальные сети

их ограбили или им нужны деньги), перезвоните им на мобильный, или другим способом проверьте правдивость информации.

- **Мобильные приложения**: большинство сайтов социальных сетей предоставляют мобильные приложения для входа в аккаунт. Убедитесь, что загружаете приложения из надёжных источников и ваш смартфон защищен надёжным паролем. Помните, если ваш смартфон взломают, или вы его потеряете, любой сможет войти в ваш аккаунт и вести записи от вашего имени.

Сайты социальных сетей предоставляют отличную возможность общаться и оставаться на связи по всему миру. Следуя несложным правилам, приведенным в этой статье, вы сможете общаться онлайн безопасней. Чтобы узнать больше о способах безопасного использования сайта или сообщить о подозрительной активности, изучите страничку описания безопасности сайта.

Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом. Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

Паролевые фразы: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_ru.pdf

Двухступенчатая верификация: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_ru.pdf

Безопасное использование мобильных приложений:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_ru.pdf

Правила компьютерной безопасности для детей:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201506_ru.pdf

Центр безопасности Facebook: https://www.facebook.com/safety

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова