БЕЗОПАСНОСТЬ СОЦИАЛЬНЫХ СЕТЕЙ

- Социальные сети — это область интернета, в которой сегодня засиживается почти половина всех компьютерных пользователей. Неважно, кто это — ваш босс, ваш сосед, ваш друг или подружка — все они зарегистрированы хотя бы в одной социальной сети. Но поскольку эти места общения привлекают так много людей, большинство которых пребывают в счастливом неведении о необходимости защиты своего компьютера, здесь также охотятся киберпреступники, подстерегающие неосмотрительного пользователя и готовые к немедленному броску на свою жертву.

- Угрозы могут быть самыми разными — от простой спам-рекламы, которую мы временами обнаруживаем в своём электронном почтовом ящике, до более изощрённых видов интернет-мошенничества, созданных специально для кражи регистрационных данных пользователей социальных сетей или, например, для заражения компьютеров троянской программой-бэкдором. В результате пользователь не только теряет свою личную информацию и деньги, он подвергает угрозе компьютерного заражения окружающих. Важно понимать, что, став жертвой преступников, вы ставите под удар и себя, и людей, которые находятся рядом с вами. И в первую очередь — ваших друзей по социальным сетям. Обезопасьте себя! Вам нужно всего лишь самому выполнять основные требования безопасности и призывать к бдительности своих друзей.

- Одна из наименее технически опасных угроз, исходящих из мира социальных сетей, — это традиционная попытка заполучить регистрационные данные пользователей. Как и в случаях с интернет-мошенничеством в системах онлайн-банкинга или фальшивыми уведомлениями из налогового управления США, фишеры создают сайт, копирующий регистрационную страницу сайта социальной сети, выбранной мишенью, и затем рассылают фишинговую ссылку на него по электронной почте или в сообщениях, отправленных якобы от имени самой социальной сети.

- Безусловно, единственная функция этой страницы — перенаправить ничего не подозревающего пользователя на настоящий сайт социальной сети после того, как он введет свои регистрационные данные. Полученным логином и паролем фишер может распорядиться следующим образом:

- * продать на черном рынке;
- * использовать для сбора дополнительной информации о жертве, зайдя в ее профиль;
- * использовать взломанную учетную запись этой социальной сети для рассылки спама.


.com

- В большинстве сообщений, рассылаемых с использованием техники маскировки под законного пользователя, содержится компонент социальной инженерии, который пытается заманить жертву на определенный сайт или уговорить получателя сообщения загрузить программу на свой компьютер. Даже если вы не можете убедить своих друзей установить хорошее антивирусное решение, попросите их относится внимательнее к ссылкам, полученным от знакомых. Поскольку фишинговые атаки генерируются компьютером, будет невредно поинтересоваться у своих друзей, действительно ли они отправляли вам ссылку.

- Ещё один тип угроз, который мигрировал в социальные сети из систем интернет-банкинга — это программы для кражи паролей. Они внедряют части своего кода в ваш браузер (в основном, в Internet Explorer и иногда в Firefox) для того, чтобы похитить ваши регистрационные данные до того, как они будут отправлены на сервер.

правила

- 1)Никогда не открывайте спамы.
- 2)если вас взломали, передайте всем своим друзьям, потому что от вас будут или спамы или через вас взломают всех ваших друзей.
- 3)не открывайте сомнительные сайты
- 4)после того как выключили интернет проверьте компьютер на вирусы, просто может случится так , что вы поймаете вирус.
- 5)следуйте этим правилам и никогда не поймаете вирус.
- Это ещё не все правила для использования социальных сетей.

Конец