Соцсети: как не стать жертвой киберпреступников. Инструкция по безопасности

Легкомыслие в социальных сетях может обернуться взломом аккаунта и заражением вашего компьютера вредоносными программами.

Всего за несколько лет социальные сети стали неотъемлемой частью жизни современного человека. Сегодня подавляющая часть пользователей имеет аккаунт на популярном ресурсе (зачастую — далеко не один) или имела в прошлом подобный опыт.

Несмотря на распространенность соцсетей, многие легкомысленно относятся к виртуальному общению и свободно размещают в сети личную информацию. В итоге она легко может оказаться в руках у злоумышленников. Уже 31% опрошенных россиян, как показывает исследование, проведенное для «Лаборатории Касперского» летом 2013 года, столкнулись хотя бы с одним инцидентом, в рамках которого один из их аккаунтов был взломан злоумышленниками. Правда, у большинства взлом аккаунта прошел без серьезных последствий: 56% респондентов удалось вовремя сбросить пароль и вернуть доступ к аккаунту, однако остальные жертвы взломщиков сталкивались с разнообразными негативными последствиями таких инцидентов. В 44% случаев от имени респондентов совершались публикации, а в 14% —онлайн-друзья, получив письмо, переходили по вредоносной ссылке.

«К любому аккаунту практически в любой соцсети можно получить доступ, причем даже без помощи специальных технических средств. В первую очередь, это связано с легкомыслием самих пользователей, которые не уделяют должного внимания безопасности персональных страничек, — утверждает **антивирусный эксперт «Лаборатории Касперского» Сергей Ложкин**. — Например, огромное количество пользователей применяют очень простые пароли, которые легко угадать. Это можно сделать с помощью специальных программ, которые перебирают комбинации. Также пароль можно вычислить по той информации, которую пользователь оставляет о себе в открытом доступе».

Информация, которую человек пишет в социальных сетях, фотографии, которые он выкладывает и места, в которых он отмечается, является своего рода «ключиком» для злоумышленников. С помощью него они и составляют психологический портрет своей жертвы и без проблемы втираются к ней в доверие. Самые популярные — методы социальной инженерии, при помощи которых злоумышленники получают несанкционированный доступ к аккаунтам пользователей без помощи специальных технических средств, основываясь только на особенностях человеческой психологии.

Как же работает социальная инженерия? Когда аккаунт взломан, злоумышленник получает доступ ко всем контактам пользователя. И друзьям начинают поступать сообщения с интригующими заголовками: «посмотри, что я о тебе увидел», «какая интересная ссылка» и другие. Получая такое письмо от своего друга или коллеги, человек чаще всего открывает сообщение и переходит по ссылке, так как он доверяет отправителю. В итоге, на его компьютер при наличии уязвимых версий программного обеспечения,

например, устаревшего браузера, автоматически можется загрузиться вредоносная программа. Либо пользователю будет предложено скачать фотографию или документ, при открытии которых может произойти заражение вредоносной программой.

Социальная инженерия может обернуться куда более серьезными и опасными вещами, вплоть до корпоративного шпионажа. К примеру, социальный инженер втирается к пользователю в доверие, добавляет его в друзья, собирает информацию о нем — место работы, должность, непосредственный руководитель, чем конкретно занимается человек. А потом преступник ненавязчиво попросит вас помочь с трудоустройством и скинет вам свое резюме, в котором, как вы догадываетесь, содержится вредоносная программа. Открыв ее на рабочем компьютере, вы предоставите злоумышленнику доступ к внутренним ресурсам компании.

«Соблюдайте элементарную осторожность, — советует **менеджер по технологическому позиционированию «Лаборатории Касперского» Денис Макрушин**. — Если Вам пришла ссылка от друга, который никогда ничего не присылает или присылает нехарактерное сообщение, то это должно вызвать подозрения. Как минимум, стоит переспросить друга лично и узнать, взломан ли его аккаунт.

Обращайте внимание и на сами ссылки — в доменном имени на первый взгляд популярного веб-ресурса могут содержаться непонятные знаки, отличаться буквы. Это первый признак того, что вы попадете на фишинговый сайт. Не надо добавлять друзей, которых вы не знаете, и не нужно, в принципе, заходить по незнакомым подозрительным ссылкам».

Так можно ли обезопасить себя при общении в соцсетях? Эксперты «Лаборатории Касперского» рекомендуют соблюдать несколько простых правил.

1. Обязательно используйте антивирусную защиту. Например, с помощью модуля «Анти-Фишинг» от «Лаборатории Касперского» в таких защитных решениях для домашнего использования как универсальный Kaspersky Internet Security для всех устройств, а также базовый Kaspersky Anti-Virus и пакет для максимальной безопасности Kaspersky CRYSTAL пользователь может отсечь потенциально вредоносные ссылки, которые приходят ему в письмах. Модуль «Анти-Спам» поможет справиться с проверкой почтовых сообщений, которые злоумышленник может отправить в том числе и через социальную сеть.

2. Регулярно обновляйте программное обеспечение. В 90% случаев вредоносные ссылки используют уязвимости в популярном ПО (Java, Adobe Flash, интернет-браузеры). Подобные программы стоят на большинстве компьютеров и киберпреступники ищут уязвимости, прежде всего, именно в них.

3. Используйте сложные пароли, не связанные с вашей жизнью. Пароль может быть набором символов с использованием цифр, больших и маленьких букв, спецсимволов. Его будет сложно запомнить, но это обеспечит вашу безопасность в сети.

Казалось бы, всех этих проблем можно было бы избежать, отказавшись от общения в социальных сетях. Но и в таком случае вы можете стать жертвой злоумышленников, которые могут зарегистрироваться в сети под вашим именем и будут выдавать этот аккаунт за ваш.

http://www.aif.ru/society/web/1013444