Любители соцсетей - находка для хакеров

Подумайте дважды, прежде чем публиковать в социальных сетях селфи в офисе своей компании или групповые снимки вместе с коллегами по работе. Хакеры рыщут по интернету в поисках фото, видео и другой информации, чтобы с ее помощью лучше спланировать атаку на вашу фирму. Об этом предупреждает Стефани Каррутерс (Stephanie Carruthers), известная в киберсообществе под псевдонимом Snow. Вместе с другими коллегами по "хакерскому цеху" она входит в команду X-Force Red подразделения IBM Security, специализирующегося на вопросах информационной безопасности. По заказу других компаний они ищут пробелы в киберзащите организаций до того, как их обнаружат и используют настоящие злоумышленники.



Каррутерс собирает в интернете данные, выложенные сотрудниками компаний в открытый доступ, звонит персоналу по телефону и с помощью приемов социальной инженерии выуживает у них различные сведения, в том числе и те, что позволяют проникнуть в офис организации.

Социальные сети и опубликованные в них фотографии - настоящая "золотая жила" для получения такой информации. Чего только не рассмотришь на заднем фоне снимков, сделанных в компаниях - от пропусков сотрудников в офис до незаблокированных экранов ноутбуков и приклеенных листочков-напоминалок с записанными на них паролями к Wi-Fi.

В статье для онлайн-журнала Fast Company, Каррутерс рассказала, как на первый взгляд безобидные публикации в соцсетях делают компанию уязвимее и облегчают работу хакерам.

Не секрет, что самое слабое звено в системе кибербезопасности организаций - это сотрудники. За технической или программной уязвимостью нередко стоит человеческий фактор. Особенно это касается молодых специалистов и новичков, проходящих в компании стажировку или недавно занявших должность. По словам Каррутерс, в 75 процентах случаев нужную ей информацию она получает именно от таких сотрудников.



Молодые люди, приходящие сегодня в компании, выросли на соцсетях и привыкли выкладывать в интернет буквально все. А уж стажировка или новая работа - такая замечательная новость, чтобы ею поделиться. Ситуацию усугубляет то, что компании нередко проводят тренинги по кибербезопасности с новым персоналом лишь недели, а то и месяцы спустя после приема на работу. Вот вам и готовый рецепт уязвимости.

Зная это слабое место и несколько расхожих хэштегов, таких как #firstday, #newjob или #intern + [#companyname] (#первыйденьнаработе, #новаяработа, #стажировка + [#названиекомпании]), Каррутерс всего за несколько часов может найти в соцсетях массу полезной для хакера информации.

Многие не задумываются, что публикуя собственные и коллективные фотографии на рабочем месте, во время перерыва и какого-то корпоративного мероприятия, они раскрывают о себе больше информации, чем планировали. На фото могут случайно попасть различные детали, например, постеры и офисные доски с записями, которые хакер может использовать в своих интересах. Например, заметив на снимке постер с объявлением о скором проведении командного турнира по софтболу, киберзлоумышленник может отправить сотруднику электронное письмо со ссылкой якобы на расписание игр. Скорее всего, сотрудник не заподозрит ничего плохого и кликнет по линку... на самом деле вредоносному.

Также Каррутерс множество раз находила в соцсетях снимки, на которых крупном планом видны бейджи сотрудников, служащие пропуском в офис. Такие фото чаще всего публикуют новички и стажеры, когда выкладывают свои селфи в первый рабочий день. Зная, как выглядит бейдж, нетрудно изготовить дубликат и с его помощью проникнуть в офис.



"Всего за несколько минут я могу скопировать бейдж изготовить дубликат, заменив на нем фото сотрудника на свое. Да, электронную систему таким пропуском не обмануть, но вы не представляете, как просто пристроиться за кем-то в хвост на проходной и зайти в компанию, просто помахав бейджем в воздухе перед охранником. Главное при этом уверенно улыбаться", - рассказала Стефани Каррутерс о своем опыте.

Но настоящая находка для хакеров - это сотрудник-видеоблогер, решивший опубликовать ролик на тему "день в офисе". По записи можно узнать и планировку здания, и места, где действует пропускная система. По схемам на офисных досках, которые случайно окажутся в кадре, можно изучить и планы компании. В общем, попадись такой ролик злоумышленнику - и считай, он сам побывал в офисе.

Кроме того, по изображениям на экранах офисных компьютеров можно понять, какой антивирус и другое программное обеспечение используются в компании. Зная это, хакер может изготовить персонализированное вредоносное ПО, замаскированное под обновление для одного из офисных приложений.

Киберпреступники также могут воспользоваться информацией об имеющихся в компании проблемах. Выяснить, чем недовольны сотрудники, позволяют такие онлайн ресурсы, как Glassdoor, сайты поиска работы и, конечно, обсуждения в соцсетях.



Каррутерс с помощью таких сведений однажды устроила успешную фишинговую рассылку. В одной из компаний, киберзащиту которой тестировала команда X-Force Red, многие работники жаловались онлайн на нехватку парковочных мест. Каррутерс написала электронное письмо, в котором компания якобы разъясняла новую политику паркинга и предупреждала, что автомобили, оставленные не на своих местах, будут эвакуироваться. Метод социальной инженерии сработал на ура: взволнованные новостью о выделении мест для стоянки и напуганные тем, что машину может забрать эвакуатор, многие сотрудники открывали вредоносное вложение к письму, выполненное в виде схемы парковки.

"В следующий раз, прежде чем делиться чем-то в соцсетях, подумайте, не пригодится ли эта информация хакерам", - посоветовала в заключении Стефани Каррутерс.