Безопасный тренд

Что происходит, когда мы читаем новости, постим фото в Инстаграмм, общаемся во Вконтакте или на Фейсбуке? Что скрывается за простым нажатием клавиш на нашем компьютере? Будучи модной тенденцией, социальные медиа подвергают нас риску потери конфиденциальности персональных данных. Как сохранить свою безопасность, не прекращая использовать социальные сети?

За ответом на данные вопросы мы обратились к куратору научного студенческого общества физико-технического факультета АлтГУ Рустаму Сахатову, который провел экскурсию по лаборатории «Безопасность информационных сетей».
Войдя в лабораторию, Рустам начал:

– Знаете, мне всегда нравилось работать с техникой, в том числе компьютерами, – и правда, в Лаборатории как в штаб-квартире ЦРУ – большие мониторы, много компьютеров и разного оборудования. – На первом курсе меня заинтересовала тема шифровки информации, – продолжает Рустам. Например, шифр Цезаря – это один из самых простых и известных методов шифрования. Каждая буква в этом шифре заменяется другой буквой, отстающей от первой на определенное расстояние. Эта процедура была необходима для того, чтобы обезопасить информацию от «перехвата» врагами во время войны. А уже в век информационных технологий вся информация хранится и распространяется посредством сети Интернет.
По словам Рустама, нужно оказаться по разные стороны баррикад: в лаборатории можно попробовать свои силы в организации различных сетевых атак и взломов, а также научиться противодействовать этим атакам. Все же видели, как в кино умело орудуют хакеры, так почему бы самому этого не попробовать?
Конечно, процесс обучения – это сложная процедура, но всегда можно освоить это постепенно.

–А вот и Павел, – Рустам показывает на задумчивого и погруженного в работу парня, студента физико-технического факультета.
– Я занимаюсь написанием программы по защите от прослушивания беспроводной Wi-Fi сети с открытым доступом. Суть проекта в следующем: когда люди пользуются открытым Wi-Fi, на это можно посмотреть с помощью различных программных средств. Моя разработка «вытаскивает» из всего картинки, HTML-документы, файлы и др., но если они не зашифрованы. При этом программу невозможно обнаружить.
Первая мысль, которая приходит к нам в голову: неужели мы настолько уязвимы в интернет-среде? Но Павел нас быстро успокаивает:

–- Важно пользоваться закрытым Wi-Fi, который требует введение пароля. Данный способ поможет обезопасить пребывание в Интернете, – посоветовал нашим читателям Павел.
Это возможно, если следовать ряду правил, а именно:
1. Не стоит нажимать на заманчивые картинки и рекламу, иначе можно «влететь на деньги».
2. Быть бдительным, когда браузер или плагин требует обновления. По статистике, Adobe больше всего подвергается нападению: в серьезных компаниях за это выписывают

штрафы.
3. Проверять скачанный файл на наличие вирусов, ведь компьютеры так уязвимы.
4. Не сохранять пароли и прочие конфиденциальные данные в браузере, потому что так вы облегчаете труд взломщикам, оставляя свои данные.
Создавая такие проекты, молодые специалисты вносят значительный вклад в развитие информационной среды и на практике занимаются анализом корпоративных сетей. Похоже, теперь научную лабораторию «Безопасность информационных сетей» можно отнести к основной учебной площадке для реализации своих творческих и научных амбиций.