Обеспечение безопасности при работе в режиме онлайн: меры предосторожности

Бюро по вопросам образования и культуры Государственного департамента США весьма серьезно относится к мерам по обеспечению безопасности при работе в режиме онлайн. Когда вы открываете странички социальных сетей, электронной почты либо интернет сайтов, помните, пожалуйста, о следующих мерах предосторожности:

1. Никогда не сообщайте свою контактную информацию частного характера. Никогда не выставляйте адрес своей электронной почты или номер своего телефона на страницах публичного доступа, таких как ваша страница публичного профиля, блог, форум либо подпись к изображению.

2. Если вы являетесь членом социальной сети, то тщательно следите за своими настройками защиты частной информации, которые дают вам возможность самому определять кому и сколько информации о себе вы хотите сообщить.

3. Тщательно продумайте то, что вы собираетесь написать на страницах социальных сетей. Прежде, чем выставить фотографии, видеоролик или текст, задумайтесь, не окажетесь ли вы в неловком положении, если это увидят члены вашей семьи или же ваш работодатель?

4. Прежде чем вы добавите к своей странице публичного профиля виджет (микроприложение, доступ к которому могут получить другие лица), подумайте, хотите ли вы, чтобы создатели виджета имели доступ к вашей странице публичного профиля и к информации о вашей активности в социальной сети? Помните, что социальные сети обычно не контролируют такого рода мини-приложения, поэтому при использовании этих виджетов действуйте осмотрительно.

5. Сообщайте администраторам сайта о любых злоупотреблениях правилами пользования сайта. Любой уважаемый сайт или социальная сеть обеспечит пользователям возможность сообщать о злоупотреблениях.

6. Электронная почта может применяться в целях распространения вредоносного программного обеспечения либо для получения ваших личных данных с целью мошенничества. Чтобы защитить себя и компьютеры, которыми вы пользуетесь, следуйте следующим руководящим принципам:

- Будьте настороже, когда вам посылают непредусмотренные электронные послания либо звонят люди, запрашивающие информацию личного характера. Если неизвестный представляется как представитель легитимной организации, попытайтесь обратиться в эту организацию и поинтересуйтесь: работает ли у них такой человек?

- Не делитесь ни вашей финансовой, ни личной информацией (номера кредитных карт, личный идентификатор) с лицами, которые по собственной инициативе запросили такого рода информацию либо по телефону, либо по электронной почте.

- Не посылайте информации личного или финансового характера по интернету не проверив безопасность сайта. (Адрес безопасных сайтов начинается с “https://”)

- Обращайте внимание на адреса сайтов, которые расположены в верхней части экрана. Вредоносные сайты могут выглядеть точно так же, как и легитимные, зачастую в адресе могут быть заменены одна или несколько букв, либо у них другой домен (например “.com”, вместо “.net”).

- Защищайте свой и другие компьютеры, которыми вы пользуетесь, путем проверки на вирусы посредством сканирования всех съемных носителей, таких как флэш-диски, CD и DVD, а также всех приложений, которые вы получаете по электронной почте перед их открытием.

- Не принимайте и не открывайте исполняемые файлы (название таких файлов заканчивается на “.exe”), которые вы получаете по электронной почте. Такие файлы могут представлять опасность.