МЕРЫ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

Многие из нас, более 2,5 млрд. человек планеты, хотя бы раз выходил в интернет. Зайдя в Сеть мы с вами оставляем свои «цифровые отпечатки». Те, кто читает новости – в меньшей степени, те, кто ищет какую-либо информацию через поисковики – в большей степени.
Хотим вам напомнить ряд мер, которые вы не должны забывать, а должны выполнять, чтобы обеспечить себе безопасность работы в интернете.

Как защитить ваш компьютер?

☛ Необходимо периодически обновлять все программное обеспечение вашего компьютера.

☛ Обязательно установить антивирусную и антишпионскую защиту на компьютер.

☛ Желательно чтобы брандмауэр был включен.

☛ На домашнем беспроводном Wi-Fi-устройстве (маршрутизатор) установите защиту с помощью пароля.

☛ Не вставляйте в ваш компьютер чужие флешки или различные накопители, они могут быть заражены вирусом, который заразит ваш компьютер.

☛ Перед тем как вы будете переходить по ссылкам или будете открывать вложение пришедшее на вашу электронную почту, удостоверьтесь, что вам действительно отправлялось сообщение.

☛ Не переходите по подозрительным ссылкам и не нажимайте на кнопки всплывающих подсказок, которые так же выглядят подозрительно.

Как обеспечить защиту личной информации?

• Прежде чем вы будете вводить личные данные в веб-форму или на веб-странице, обязательно обратите внимание на адрес веб-страницы, она должна начинаться с префикса https и значка в виде закрытого замка ( ) рядом с адресной строкой. Это обозначает, что соединение безопасно.

• Никогда не давайте свои персональные сведения (такие как номер счета или пароль) если их запрашивает по электронной почте неизвестный вам адресат. А так же если они запрашиваются в социальной сети.

• Ни в коем случае не отвечайте на любые просьбы прислать деньги от «членов семьи» или «друзей», «родственников», на сомнительные предложения о сделке, на всевозможные сообщения о лотерейных розыгрышах, в которых вы не принимали участия, или на различные всевозможные мошеннические сообщения.

Какими должны быть пароли?

Пароли должны быть из длинных фраз или предложений и состоять из сочетаний строчных, прописных букв, цифр и символов. Обязательно используйте везде разные пароли, особенно там, где хранится ценная информация.

Как заботится о своей безопасности и репутации в Интернете?
Обязательно посмотрите, какая информация о вас имеется в Интернете. Делайте эту процедуру периодически. Всегда анализируйте и оценивайте нашедшую информацию. Постоянно заботьтесь о своей репутации и положительном имидже.

Как безопасно использовать социальные сети?
⇒ Обязательно настройте ваши аккаунты социальных сетей, так чтобы ваш **профиль** могли просматривать только пользователи, которые допущены к просмотру вашего профиля или фотографии.
⇒ Контролируйте добавленные комментарии о вас.
⇒ Научитесь блокировать пользователей пишущих нежелательные комментарии о вас.
⇒ Ни в коем случае не публикуйте информацию, которую вы не хотели бы видеть на доске объявлений.
⇒ Подходите очень избирательно к предложениям дружбы.
⇒ Постоянно анализируйте, кто из пользователей имеет доступ к вашим страницам, а также периодически просматривайте информацию, которую эти пользователи публикуют о вас.