В интернете есть праздник — День безопасного Интернета. Он отмечается с 2004 года. Каждый человек может сделать свой интернет безопаснее, а помогут в этом правила, которые откроют дорогу в безопасный интернет.

1. ХОРОШИЙ КАЧЕСТВЕННЫЙ АНТИВИРУС.

Перед тем, как начать пользоваться компьютером, обязательно позаботьтесь об установке качественного и проверенного временем антивируса. Когда вы подключаете какое-либо внешнее устройство к вашему компьютеру, например, флешку, то всегда проверяйте антивирусом, чтобы не заразить свой компьютер. Периодически проверяйте и ваш компьютер – запускайте сканирование.

2. НЕ ЗАБЫВАЙТЕ ПРО ОБНОВЛЕНИЯ ВАШИХ ПРОГРАММ.

Активный человек всегда пользуется множеством программ и приложений. Каждый раз хакеры ищут «дыры и уязвимости», через которые можно взломать программу. Но, есть выход из этой ситуации. **У программ есть обновления, про которые не следует забывать. С помощью обновлений исправляются уязвимости старых версий.** Это займёт не много времени, но защитит ваш компьютер от вирусов и вредоносных программ.

3. ЭТИ ОПАСНЫЕ ССЫЛКИ.

Ссылки придумали, чтобы нам жилось легче в интернет жизни. Это те дороги, по которым ссылки, как трамвайчики доставляют нас к нужному месту. Это происходит мгновенно. И тут только от вашей осторожности будет зависеть, где именно вы окажетесь – после такого мгновенного проезда – в нужном месте или в ловушке?

Как быть если вдруг по почте, в сообщении из социальной сети к вам пришла ссылка – не следует сразу же нажимать на неё, даже если вас просят. Опасные ссылки бывают с привлечением баннеров (картинок с заманчивым текстом): Вы выиграли приз!! Вы 100 счастливчик – возьмите приз!!! Или: Ваш компьютер заражён – проверьте его на вирусы!!! Не забывайте, что кликнув по ссылке, вложенной в письмо, вы можете спокойно заразить свой компьютер вирусами, троянами и другими опасными шпионскими программами.

4. У ВАС ЕСТЬ СМАРТФОН? НЕ ЗАБЫВАЙТЕ — ЭТО ТОЖЕ КОМПЬЮТЕР!

У него есть операционная система, его тоже нужно оберегать. С ним тоже надо соблюдать правила безопасности выхода в интернет. И антивирус хороший ему не помешает. **Не устанавливайте приложения сомнительного вида, скачивайте только с официальных источников и читайте отзывы.** И всегда смотрите, какое право и куда имеет доступ приложение. Иногда там чётко бывает написано, что приложение имеет доступ к отправке платных смс.

5. ЗАВЕДИТЕ ХРАНИТЕЛЬ ПАРОЛЕЙ. ПО ТЕХНИЧЕСКОМУ — МЕНЕДЖЕР ПАРОЛЕЙ.

Если вы обладаете отличной памятью на цифры и набор букв, то храните все пароли в своей голове. Или записывайте их в тетрадь, к которой доступ закрыт для остальных людей. Как сделать доступ тетради закрытым для других? Просто спрячьте её в сейфе или напишите пароли тоже при помощи шифра, придуманного вами. Например, напишите пароль, но запишите его в тетради в обратном порядке. Это правило шифровки можно применить для всех паролей. Об этом будете знать только вы и поэтому смело оставляйте тетрадь на виду.

6. НАУЧИТЕСЬ СЕБЯ ЗАЩИЩАТЬ.

Если вдруг вас в социальной сети начинают забрасывать спамом, или заваливать комментариями или сообщениями такого характера, которые вам не по душе – то просто найдите кнопку «заблокировать пользователя»

Вам могут угрожать, вас могут шантажировать, над вами могут просто издеваться, вызывая вас на ответную агрессию. Это дело рук интернет троллей.

Поэтому, не забывайте про эти волшебные кнопки, которые есть везде: «Пожаловаться на спам» «Заблокировать пользователя»

Подготовил библиограф Сладкевич С.В.

Велижская районная библиотека
Информационный центр для подростков «Войди в мир закона»

ВЕЛИЖ 2017