

Здравствуй, Данил!

При последней встрече мы договорились с тобой, что я буду учить тебя как безопасно пользоваться интернет ресурсами. Конечно, я тоже не все пока знаю, но мы на уроках информатики и на классных часах много говорим на эту тему. И мне самому интересна эта тема, поэтому я и изучаю самостоятельно.

Сегодня я бы хотел поговорить о безопасности в интернете. Так как есть много мошенников, которые хотят получить наши данные и завладеть нашим устройством, хотелось бы начать о вирусах, от безопасных до самых опасных.

Winlocker - один из самых не очень опасных вирусов, когда придется переустановить windows, но с компьютером останется все в полном порядке.

А сейчас вирус поопаснее и имя ему Storm. Суть действия была в том, что приходила новостная ссылка о том, что погибли 230 человек от бури в Европе, и переходя на сайт вирус уже загружался на компьютер и воровал данные. Этот вирус все еще находится в действии.

Nimda - это опасный вирус, который полностью поражал интернет, просто переходя по ссылке. Он поражал компьютеры, но он не смог поразить всю инфраструктуру сетей.

И последний на сегодня вирус – Wannacry. Этот вирус как Winlocker, но больше известен в Америке. В самом начале она была программой военных Америки, как поражающая вражеские компьютеры, но был украден и переделан хакерской группировкой. Чтобы избавиться от вируса, надо было заплатить 300 долларов, потом уже 600 долларов, а если за 7 дней деньги не приходили, то вирус начинал удалять все данные жесткого диска. Вот какие опасности ждут нас. Попутно хочу разъяснить: изначально **хакерами** называли программистов, которые быстро и по-умному исправляли ошибки в программном обеспечении. Но сейчас хакерами называют злоумышленников, которые взламывают компьютеры, пишут и распространяют те самые компьютерные вирусы.

Ну, мы подошли к завершению разговора о вирусах и хочу предупредить, не надо скачивать файлы, игры, музыку и т.д. со сторонних сайтов!

Данил, хочу сказать, что вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям называется **фишинг**. Это письмо я тебе отправляю по электронной почте. Но случается и массовые рассылки электронных писем от имени популярных брендов, а также от имени банков или внутри социальных сетей. Поэтому, прежде чем открыть письмо, подумай, ты знаешь отправителя, ты ждешь это письмо?

Жду от тебя письмо, напиши, что ты знаешь о вирусах, какой антивирус у вас на компьютере.

В следующем письме я расскажу о контактах с незнакомыми людьми в социальных сетях.

Пока, Данил!

Твой брат Эмиль
20 марта 2022 г