Интернет-конкурс, посвященный безопасному использованию Интернета
http://www.edu.yar.ru/safety/internet_konkurs/o_konkurse.html
Тема «Что бы я посоветовал другу при встрече с опасностью в Интернет»
номинация учащиеся 6-8 классов школ

Иванов Василий
г. Уфа
Республика Башкортостан

Привет, Вова.

Как у тебя дела? Какая у вас погода? Ты не поверишь, что со мной случилось: я случайно кликнул на баннер, и пришлось заново ставить Windows. Чтобы ты не попал в такую ситуацию вот тебе правила безопасности в интернете

- Будь аккуратен со ссылками, содержащимися в электронных посланиях. Они могут вести совсем не туда, куда указывает текстовая информация.
- Не отправляй конфиденциальную личную или финансовую информацию, если только она не зашифрована (при работе на защищенном веб-сайте). Обычные письма по электронной почте не шифруются.
- Будь внимателен! Фальшивые, похожие на сайты крупных компаний веб-сайты, предназначены для обмана клиентов и сбора их личной информации. Убедись, что веб-сайты, с которыми ты работаешь, содержат заявления о соблюдении конфиденциальности и безопасности, и внимательно их изучи. Убедись, что необходимый вам URL появляется в поле «адрес» или «узел» вашего браузера. Некоторые веб-сайты могут казаться похожими на необходимый тебе, но в действительности быть фальсифицированными. Потрать несколько лишних секунд и напечатайте URL лично.
- При передаче конфиденциальной информации ищи символ замка в правом нижнем углу веб-страницы. Этот символ указывает на то, что сайт работает в защищенном режиме. Ты должны увидеть его ПРЕЖДЕ, чем ты введешь конфиденциальную информацию.
- Используй надежные пароли или ПИНы для твоих счетов в Интернете. Выбирай слова, которые другим будет трудно угадать, и используй разный пароль для каждого твоего счета. Используй буквы и цифры, а также сочетание заглавных и строчных букв, если пароли или ПИНы различают строчные и заглавные буквы.
- При выходе из программы делай это в соответствии с установленными процедурами. Не закрывай браузер просто так! Выполняй инструкции по выходу из безопасной зоны для обеспечения Вашей безопасности.
- Избегай осуществления любых банковских операций в местах, где услуги Интернет являются общедоступными, например в Интернет-кафе. Очень трудно определить, отсутствуют ли на таких компьютерах хакерские программы, которые фиксируют твою личную информацию и сведения о счете. Если тебе необходимо осуществить операцию с компьютера общего пользования, измените свой ПИН со своего компьютера после того, как ты пользовался компьютером общего доступа. Это имеет большое значение, так как существует риск фиксирования нажатий клавиш (включая номера банковской карты и кредитной карты, а также ПИНа) при помощи специальных программ, встроенных в компьютер общего доступа, без твоего ведома.

Запомни эти правила и используй их. Вот собственно и всё. Пока.

С уважением, Вася.