

30.10.2017 г. в ГБОУ Школа №920 прошёл Единый урок по безопасности в сети «Интернет»

Единый урок представляет собой цикл мероприятий для школьников, направленных на повышение уровня кибербезопасности и цифровой грамотности, а также на привлечение внимания родительской и педагогической общественности к проблеме обеспечения безопасности и развития детей в информационном пространстве.

В ходе Единого урока участники узнали, как защитить свои персональные данные, совершать безопасные покупки в интернет-магазинах, научились анализировать правдивость и достоверность информации в сети Интернет и многое другое.



ЕДИНЫЙ УРОК ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ



Для того, чтобы обезопасить свой игровой аккаунт, достаточно придерживаться простых правил:

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков, и к тебе перестанут доходить от него сообщения;
- Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скриншотов;
- Не указывай личную информацию в профайле игры и не привязывай карты для оплаты к аккаунту;
- Не устанавливай неофициальные патчи и моды;
- Используй сложные и разные пароли;
- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Чтобы спокойно пользоваться подобными сервисами и другими онлайн-магазинами нужно знать базовые вещи при оплате онлайн:

- Лучше не хранить мобильный телефон или гаджет для генерации паролей в одной сумке с кошельком;
- Не стоит хранить в кошельке и платежную карту, и карту с набором одноразовых паролей;
- Большинство российских банков присылают временные пароли по смс;
- Если вы боитесь публиковать в интернете данные вашей основной банковской карты, можно завести специальную виртуальную карту для покупок в сети.

Простые правила использования Wi-Fi в общественных местах:



- Для начала нужно удостовериться, что вы подключаетесь к официальной сети Wi-Fi заведения, в котором вы находитесь. Обычно такие сети или имеют пароль, или требуют минимальную авторизацию.
- Старайтесь не посещать требующие авторизации сайты. Проверить почту или оставить комментарий на форуме можно, но только если вы уверены в безопасности подключения.
- Не проводите через публичную сеть никаких финансовых операций на сайтах или приложениях.
- Используйте двухфакторную аутентификацию — это сведёт к нулю вероятность взлома аккаунта, если ваши данные всё же перехватят и смогут расшифровать. Сейчас двухфакторную аутентификацию поддерживают практически все социальные сети и крупные сервисы.

Самые распространенные пути заражения:



- Переход по ссылкам или открытие файлов из писем и сообщений с незнакомых адресов;
- Посещение сомнительных и зараженных сайтов;
- Клики на баннеры сомнительного содержания;
- Скачивание и установка программ и файлов с непроверенных ресурсов;
- Неосторожное использование чужих зараженных флешек.

Чтобы обезопасить себя в социальных сетях нужно придерживаться нескольких правил:



- Указывайте меньше личной информации;
- Не указывать места, где вы были, при помощи геолокации;
- Не стоит афишировать свое финансовое благосостояние;
- Не указывайте номер своей кредитной банковской карты;
- Не каждый вложенный файл в сообщении следует открывать, точно также как и в электронной почте;
- Конфиденциальность.

Давайте повторим основные правила:



- Надо выбрать правильный почтовый сервис;
- Не указывай в личной почте личную информацию;
- Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS или на другую почту;
- Выбери сложный пароль;
- Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей;
- Используйте несколько почтовых ящиков. Один для переписки, а второй для регистрации на сайтах, форумах, социальных сетях и играх.