Правила поведения для учащихся в современной информационной среде

Вы должны это знать:

- Не желательно размещать персональную информацию в Интернете. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей. Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
- Не отвечайте на Спам (нежелательную электронную почту).
- Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
- Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)

Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

- Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
- Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!

Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Рекомендации Абонентам

Убедитесь в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.

Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученных посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию.

Не спешите звонить или отправлять SMS на короткий номер, который обещает разблокировку компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора. Уточняйте у оператора стоимость платных номеров, предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.

Не торопитесь давать телефон на «1 звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.

Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения - то и от известных. С развитием функциональности мобильных телефонов, КПК и коммуникаторов хакеры стали уделять больше внимания созданию вредоносного ПО для этих устройств. По возможности, установите на мобильное устройство одну из многих антивирусных программ, которые вы можете найти на сайтах известных производителей антивирусного ПО.

Для разблокировки компьютера от вирусов используйте антивирусное ПО известных разработчиков, в том числе, бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям, гарантирующим избавление от вируса или исчезновение интернет-баннера при отправке смс на короткий номер.