|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Хайрутдинова Венера

МОБУООШ с. Николаевка

Благовещенский район

**«Иформационная безопасность в сети ИНТЕРНЕТ»**

10/30/2017

Общая безопасность в интернете

Интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать их. Какие опасности могут поджидать в интернете В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут использовать самые разные инструменты и методы — например, вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах.

Вирусы

Вирусы могут распространяться с помощью вложенных файлов, ссылок в электронных письмах или в соцсетях, на съемных носителях, через зараженные сайты. Сообщение с вирусом может прислать как посторонний человек, так и знакомый, но уже зараженный участник социальной сети или почтовой переписки. Зараженными могут быть сайты, специально созданные в целях мошенничества, или обычные ресурсы, но имеющие уязвимости информационной безопасности. Рекомендации

• Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур. • Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус. • Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, [www.yadndex.ru](http://www.yadndex.ru)).

• Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требование перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Мошеннические письма

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма по определенному сценарию.

**В современном мире интернет-среда стала неотъемлемой составляющей повседневной жизни. Подрастающее поколение активно ведет существование в режиме on-line. Безопасность детей в интернете – актуальная проблем**

Хайрутдинова Венера

МОБУООШ с. Николаевка