**ПАМЯТКА ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ**

Интернет – это самая обширная в мире библиотека знаний, развлечений, общения и других полезных вещей, Интернет может быть средством для обучения, отдыха или общения с друзьями, но в тоже время Интернет-источник угроз, представляющих опасность для жизни, физического, психического, нравственного здоровья и полноценного развития человека. Поэтому необходимо научиться правильно пользоваться этим неисчерпаемым источником информации.

**Наиболее часто встречающиеся угрозы при работе в Интернет:**

* + *угроза заражения вредоносным программным обеспечением.* Для распространения вредоносного программного обеспечения и проникновения в компьютеры используется почта, компакт-диски, дискеты и прочие сменные носители, или скачанные из сети Интернет файлы;
	+ *доступ к нежелательному содержимому.* Это насилие, наркотики, страницы, подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической идеологией. Независимо от желания пользователя, на многих сайтах отображаются всплывающие окна, содержащие подобную информацию;
	+ *контакты с незнакомыми людьми* с помощью чатов или электронной почты. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. Выдавая себя за сверстника, они могут выведывать личную информацию и искать личной встречи;
	+ *поиск развлечений* (например, игр) в Интернете. Иногда при поиске нового игрового сайта можно попасть на карточный сервер и проиграть большую сумму денег;
	+ *неконтролируемые покупки.*

 **Компьютерные вирусы**

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. Вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев вирусы распространяются через Интернет.

**Методы защиты от вредоносных программ:**

* используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
* работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
* используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
* ограничь физический доступ к компьютеру для посторонних лиц;
* используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;
* не открывай компьютерные файлы, полученные из ненадёжных источников (даже те файлы, которые прислал твой знакомый).

**Социальные сети**

Социальные сети активно входят в нашу жизнь, многие люди работают и

живут там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

**Основные советы по безопасности в социальных сетях:**

* ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
* защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
* защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
* если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
* избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
* при регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее восьми.

**Online игры**

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

**Основные советы по безопасности игрового аккаунта:**

* если другой игрок ведет себя некорректно и создает тебе неприятности, заблокируй его в списке игроков;
* пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скриншотов;
* не указывай личную информацию в профайле игры; используй сложные и разные пароли;
* уважай других участников по игре;
* даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

**Электронные деньги**

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

**Основные советы по безопасной работе с электронными деньгами:**

* привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
* используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
* выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее восьми знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п.
* перед тем, как воспользоваться развлекательными услугами Интернета (скачать игру, музыку, фильм и т.д.), проверь, что после этого тебя не попросят заплатить деньги.