

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

Виктория Парфенова

*Студентка Елабужского Института Казанского Федерального
Университета*

*Научный руководитель: кандидат физико-математических наук,
доцент кафедры математики и информатики ЕИ КФУ
Миронова Юлия Николаевна*

Вирусы

Компьютерный вирус - это вид компьютерной программы, которая может копировать себя и нанести вред файлам и данным.

Как защитить свой ПК от вредоносных программ:

1. Необходимо использовать современные операционные системы;
2. Как можно чаще устанавливайте проверенные обновления драйверов и приложений;
3. Регулярно устанавливайте антивирусные программы;
4. Нельзя открывать файлы из непроверенных источников.
5. Устанавливайте программы только от проверенных издателей и источников;

WI-FI и беспроводные общедоступные сети

Благодаря беспроводным сетям WI-FI вы можете получить доступ в интернет. Однако, вышеупомянутые сети чаще всего являются небезопасными.

Как обезопасить себя при работе с публичными сетями Wi-fi:

1. Не вводите свои логины или пароли от личных кабинетов при работе с публичными беспроводными сетями;
2. Нужно использовать антивирусные программы при работе с WI-FI;

3. Нельзя при работе с публичным WI-FI передавать личные данные и информацию о себе;

4. Запретите своему смартфону подключаться к сетям WI-FI автоматически;

Мессенджеры и социальные сети

Социальная сеть - это сайт, на котором люди могут общаться. Зачастую, там для каждого человека существует личная страница, на которой он присутствует личная информация.

Как обезопасить себя в социальных сетях:

1. В списке ваших друзей должны быть только те люди, которых вы хорошо знаете;

2. Не указывайте слишком подробную информацию о себе;

3. Раздумывайте над каждой новой публикацией;

4. Не передавайте незнакомым людям информацию о себе;

5. Не загружайте фотографии в местности, по которой можно понять, где вы живете;

6. Используйте только сложные пароли;

7. Для различных социальных сетей используйте различные пароли.

Интернет-валюта

Электронные деньги — виртуальный эквивалент денежных купюр, которыми можно расплачиваться в интернете.

Как обезопасить себя при работе с электронными деньгами:

1. Необходимо привязать к счету мобильный телефон;

2. Используйте только одноразовые пароли, которые вам сообщает система при регистрации;

3. Придумывайте сложные пароли для электронных кошельков;

4. Не вводите данные своих банковских карт на непроверенных сайтах.
- 5.

Фишинг или кража личных данных

Целью фишинга является получение логина и пароля пользователя от той или иной социальной сети, личного кабинета или виртуального кошелька.

Как обезопасить себя от фишинга:

1. Если вашу страницу взломали, нужно как можно скорее обратиться к администраторам;
2. Работайте только с проверенными и безопасными сайтами;
3. Для разных социальных сетей используйте разные и сложные пароли;
4. Важно отключить сохранение паролей в своем браузере;

Список литературы:

1. БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ [Электронный ресурс] URL: <http://school385.ru/bezopinternet/>