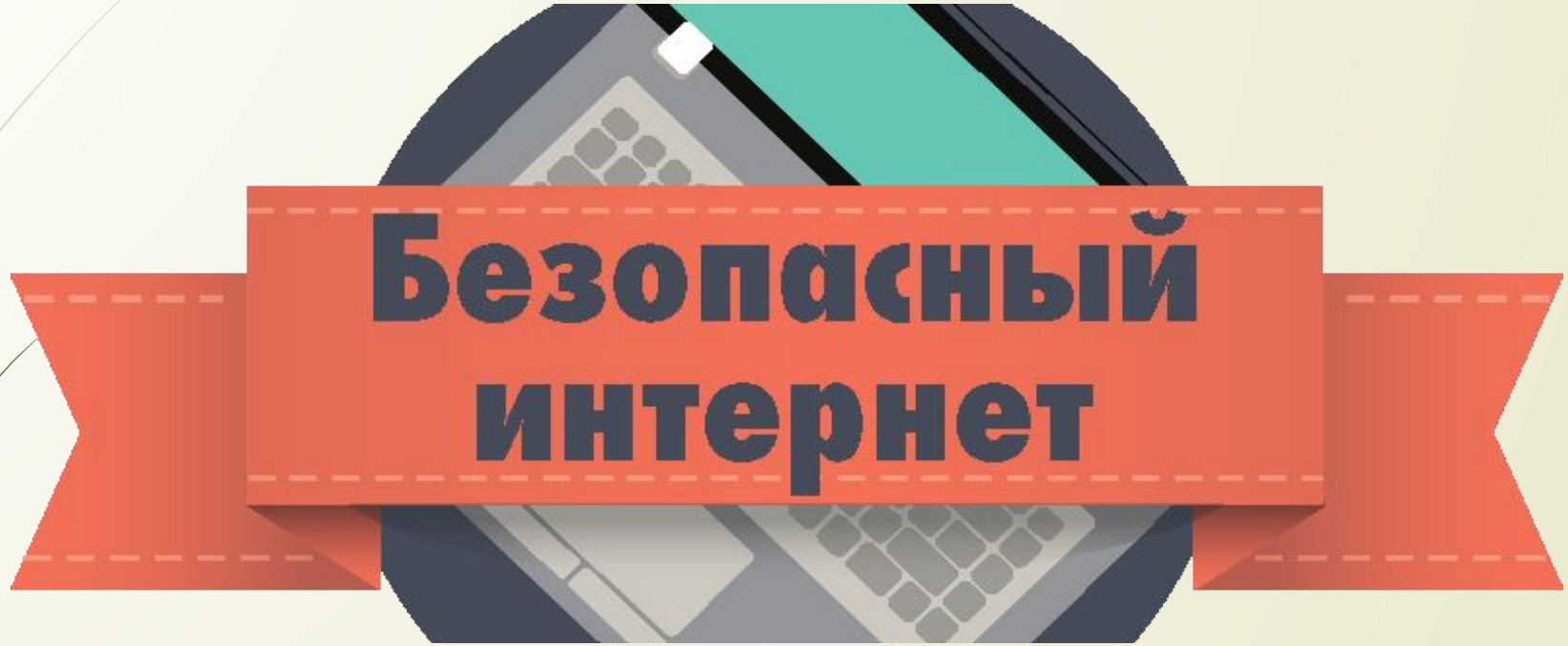

Безопасный интернет

Выполнил обучающийся 1 курса группы 108/3 Лютов Сергей

Руководитель группы Олимова Н.Н.

Содержание:

1. Что такое интернет безопасность?
2. Угрозы при работе с интернетом и как их избежать.
3. Советы по безопасности при работе в интернете.

Что такое интернет безопасность?

Интернет-безопасность — это отрасль компьютерной безопасности, связанная специальным образом не только с интернетом, но и с сетевой безопасностью, поскольку она применяется к другим приложениям или операционным системам в целом. Её цель — установить правила и принять меры для предотвращения атак через Интернет. Интернет представляет собой небезопасный канал для обмена информацией, который приводит к высокому риску вторжения или мошенничества, таких как фишинг, компьютерные вирусы, трояны и многое другое.

Угрозы при работе с интернетом и как их избежать.

Вирусная атака

Самая распространённая интернет-угроза — это атака вирусов. Из-за неё можно потерять информацию, которую вы годами собирали на компьютере.

Чтобы избежать проникновения вирусов на устройство:

1. Следите за регулярным обновлением операционной системы. Если этого не происходит, вирусам легче найти уязвимые места и проникнуть в компьютер.

2. Пользуйтесь антивирусными программами. Они устранят многие угрозы, подскажут, можно ли посещать неизвестный вам сайт, проверят файлы, скачиваемые из интернета.

3. Старайтесь не сообщать даже близким друзьям пароли от личного кабинета, банковских карт, социальных сетей, от рабочей и личной почты.

Угрозы при работе с интернетом и как их избежать.

Спам и фишинг

Ваш электронный ящик напоминает мусорную корзину, в которую сваливают всё подряд? Значит, вы давно попали в базы спамеров. В потоке спама невозможно разобраться. Кроме того, просматривать вложения, прикрепленные к таким письмам, опасно, многие из них содержат вредоносный код.

Во время фишинговых атак на вашу почту приходит рассылка от ресурсов, маскирующихся под популярные сервисы (например, банковские). Мошенники от имени знакомых вам компаний запрашивают конфиденциальную информацию (номера и пин-коды кредитных карт, пароли от почты, сервисов, предоставляющих государственные услуги). Текст письма обычно провокационный и призывает пользователя к мгновенному ответу. Даже если информация кажется вам надёжной, лучше всего позвонить в официальную службу поддержки организации, от имени которой пришло письмо.

Чтобы избежать спама и фишинговых атак:

1.Старайтесь не оставлять адрес почты на сайтах общего доступа (соцсети, форумы, в комментариях).

2.Используйте несколько почтовых ящиков для разных целей.

3.Никогда не отвечайте на спам. После вашего отказа от рассылки письма могут пойти с новой силой.

Угрозы при работе с интернетом и как их избежать.

Раздражающая и потенциально опасная реклама

Назойливая реклама преследует нас повсюду. Каждый сталкивался с ситуацией, когда перед видео на YouTube необходимо просматривать 30-секундный рекламный ролик. Это не только отвлекает от работы, мешает просматривать сайты, вести переписку: загрузка рекламного сообщения на вашем экране (будь то преролл или баннер) съедает часть вашего интернет-трафика. Получается, что за эту рекламу вы еще и платите. Часто из-за большого веса рекламных сообщений, сайты грузятся дольше. От этого у смартфонов значительно сокращается заряд батареи. Кроме того, реклама может содержать вредоносный код или вести на сайты с таким кодом.

Угрозы при работе с интернетом и как их избежать.

Кибершпионаж

Программы-шпионы проникают в компьютер вместе с подозрительным контентом, который вы скачиваете из сети. Шпионы собирают личные данные, анализируют ваши действия, составляют список часто посещаемых сайтов, просматривают поисковые запросы, а затем отправляют эту информацию поставщикам интернет-услуг. Такие программы работают в фоновом режиме и, как правило, не заметны для обычных пользователей.

Вам может показаться, что шпионы безвредны, но это не так. Они способны отключить антивирус, а также передать ваши данные злоумышленникам.

Чтобы избежать знакомства с программами-шпионами:

Старайтесь не устанавливать на компьютер условно-бесплатные программы и не нажимайте на рекламные ссылки, которые открываются во всплывающих окнах.

Угрозы при работе с интернетом и как их избежать.

Мошенничество с банковскими картами

Покупать и продавать через интернет удобно. Но при этом — опасно.

Вы разместили объявление на популярном сайте? Не спешите радоваться, если вам позвонит покупатель, готовый немедленно приобрести ваш товар.
Он сообщит, что хочет прямо сейчас перевести на вашу карту необходимую сумму. Всё, что от вас требуется — это реквизиты и несколько кодов, которые придут на ваш телефон. Псевдопокупатель исчезнет сразу же, как вы отправите ему кодовое слово или пароль, пришедшие по смс. Такая история закончится обнулением счёта вашей карточки.

Чтобы обезопасить себя от мошенничества с банковскими картами**,** помните**:**

1.Нельзя сообщать посторонним людям секретную информацию, размещённую на обороте вашей дебетовой или кредитной карты.

2.Для совершения операции по оплате достаточно фамилии, имени и отчества держателя карты, а также номера карты.

3.Если у вас возникает хотя бы малейшее сомнение в добросовестности продавца или покупателя, требуйте личной встречи и не передавайте деньги заранее.

Угрозы при работе с интернетом и как их избежать.

Браузерный эксплоит

Вы открываете браузер, и вместо привычной домашней страницы вас ожидает сюрприз — сайт с сомнительным контентом. А при ошибке ввода данных в адресной строке автоматически происходит переадресация на неизвестный сайт. Если вам знакомы эти ситуации, то, скорее всего, вы столкнулись с браузерным эксплойтом, т.е. ваш браузер был атакован.

Чтобы избежать изменения работы браузера:

1.Не забывайте его регулярно обновлять.

2.Проверяйте, работает ли на вашем компьютере брандмауэр — специальная программа, которая сканирует данные из интернета и регулирует их передачу на устройство.

3.Не скачивайте условно-бесплатное рекламное программное обеспечение.

Советы по безопасности при работе в интернете:

1. Постоянно обновляйте своё программное обеспечение.
2. Используйте двухэтапную аутентификацию.
3. Не отключайте антивирус.
4. Используйте одну электронную почту с надежным паролем
5. Файлы рекомендуется скачивать исключительно из проверенных источников.
6. Не сохраняйте в браузере свои пароли.
7. Не открывайте письма без темы и из неизвестных эмеил адресов.
8. Для того чтобы обезопасить свою личную информацию время от времени рекомендуется менять пароли на часто используемых ресурсов.

Спасибо за внимание!