

Киберугрозы современности: главные принципы их распознавания и предотвращения



Учитель информатики

Леньшина Ю. А.

МБОУ «СОШ № 11»

Киберугроза - это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей. Атака, обычно, поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя.



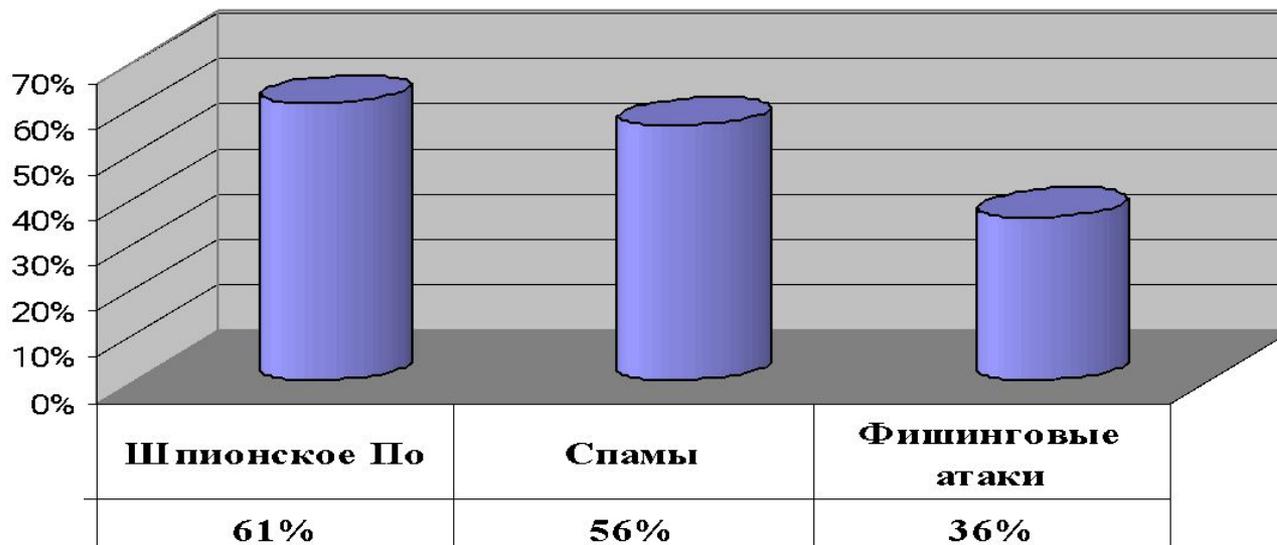
Исследования Лаборатории Касперского

В мире **91%** компаний подвергаются киберугрозам

В России этот показатель составляет **96 %**



Основные киберугрозы



Вирусы

Рекомендации:

- используй антивирусное ПО
- убедись, что файлы или ссылки, полученные по электронной почте, не содержат вирус



- не подключай к своему компьютеру непроверенные съемные носители
- не поддавайся на провокацию перевести деньги за снятие блокировки с компьютера

Фиктивные звонки от платежных сервисов



Рекомендации:

- помни, что банки и платежные сервисы **НИКОГДА** не просят сообщать по телефону пароль, пин-код, код из SMS
- никому не сообщай пароли, пин-коды, коды из SMS, номер банковской карты



Выманивание SMS-пароля незнакомцем

Фальшивые квитанции

Рекомендации:

- проверь реквизиты, указанные в платежке.

Если не совпадают – **НЕ ПЛАТИ**

- проверь номер своего лицевого счета. Он всегда один.
- настрой онлайн-платежи на проверенные реквизиты и плати только по ним через проверенные сайты

Фальшивые выигрыши в лотерею

Признаки:

- ты не принимал участие в лотерее и ничего о ней не знаешь
- ты не оставлял своих личных данных на этом ресурсе
- почтовый адрес отправителя – общедоступный почтовый сервис

Бесплатное скачивание файлов с подпиской

Рекомендации:

- не указывай свой мобильный номер на незнакомых сайтах
- если подписка уже оформлена позвони в службу поддержки оператора и попроси отключить ее

Фальшивые SMS от якобы знакомого

Рекомендации:

- лично свяжись с пользователем, от имени которого прислано SMS, чтобы проверить информацию

Слишком выгодные покупки

Рекомендации:

- не доверяй объявлениям о слишком дешевых товарах
- перед покупкой прочитай отзывы в интернете об интернет-магазине или частном продавце

Безопасность при оплате картами

Рекомендации:

- не сообщайте номер карты другим людям
- храните банковскую карту в надежном месте
- заведите отдельную карту для покупок в интернете.
- подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах

Фишинг атаки

Фишинг — вид интернет–мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям

Рекомендации:

- используй сложные пароли – минимум 10 символов, латинские буквы верхнего и нижнего регистров, цифры и специальные символы
- никому не сообщай свой пароль
- для восстановления пароля используй привязанный к аккаунту мобильный номер

Практикум «Угроза 419»

Задание:

1. Внимательно прочитайте текст письма.
2. Выделите в нем моменты, указывающие на то, что это спам.
3. Перечислите факты, указанные в письме, которые кажутся недостоверными, подозрительными



Памятка безопасности в сети Интернет

1. Прежде чем заходить в интернет, убедись, что у тебя стоит АПО
2. Своевременно обновляй антивирус.
3. Не ходи по подозрительным ссылкам, не отвечай на подозрительные письма.
4. Возьми себе за правило не разглашать лишней информации о себе в социальных сетях
5. Старайся никогда не использовать чужие флеш – накопители
6. Осторожно относись ко всем скачиваемым файлам и программам. Сканируй их на наличие вирусов.
7. Очень осторожно относись к таким требованиям, как срочно провести какой-то платеж, отправить смс, авторизоваться и т.д

Осторожно вирус !

1. Что является основным каналом распространения компьютерных вирусов?

- а) Веб-страницы
- б) Электронная почта
- в) Флеш-накопители (флешки)

2. Для предотвращения заражения компьютера вирусами следует:

- а) Не пользоваться Интернетом
- б) Устанавливать и обновлять антивирусные средства
- в) Не чихать и не кашлять рядом с компьютером

3. Если вирус обнаружен, следует:

- а) Удалить его и предотвратить дальнейшее заражение
- б) Установить какую разновидность имеет вирус
- в) Выяснить как он попал на компьютер

4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:

- а) Применение брандмауэра
- б) Обновления операционной системы
- в) Антивирусная программа

5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?

- а) Уничтожение компьютерных вирусов
- б) Создание и распространение компьютерных вирусов и вредоносных программ
- в) Установка программного обеспечения для защиты компьютера

Осторожно вирус !

1. Что является основным каналом распространения компьютерных вирусов?

- а) Веб-страницы
- б) **Электронная почта**
- в) Флеш-накопители (флешки)

2. Для предотвращения заражения компьютера вирусами следует:

- а) Не пользоваться Интернетом
- б) **Устанавливать и обновлять антивирусные средства**
- в) Не чихать и не кашлять рядом с компьютером

3. Если вирус обнаружен, следует:

- а) **Удалить его и предотвратить дальнейшее заражение**
- б) Установить какую разновидность имеет вирус
- в) Выяснить как он попал на компьютер

4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:

- а) **Применение брандмауэра**
- б) Обновления операционной системы
- в) Антивирусная программа

5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?

- а) Уничтожение компьютерных вирусов
- б) **Создание и распространение компьютерных вирусов и вредоносных программ**
- в) Установка программного обеспечения для защиты компьютера

Осторожно Интернет !

1. Какую информацию нельзя разглашать в Интернете?

- а) Свои увлечения
- б) Свой псевдоним
- в) Домашний адрес

2. Чем опасны социальные сети?

- а) Личная информация может быть использована кем угодно в разных целях
- б) При просмотре неопознанных ссылок компьютер может быть взломан
- в) Все вышеперечисленное верно

3. Виртуальный собеседник предлагает встретиться, как следует поступить?

- а) Посоветоваться с родителями и ничего не предпринимать без их согласия
- б) Пойти на встречу одному
- в) Пригласить с собой друга

4. Что в Интернете запрещено законом?

- а) Размещать информацию о себе
- б) Размещать информацию других без их согласия
- в) Копировать файлы для личного использования

5. Действуют ли правила этикета в Интернете?

- а) Интернет - пространство свободное от правил
- б) В особых случаях
- в) Да, как и в реальной жизни

Осторожно Интернет !

1. Какую информацию нельзя разглашать в Интернете?

- а) Свои увлечения
- б) Свой псевдоним
- в) **Домашний адрес**

2. Чем опасны социальные сети?

- а) Личная информация может быть использована кем угодно в разных целях
- б) При просмотре неопознанных ссылок компьютер может быть взломан
- в) **Все вышеперечисленное верно**

3. Виртуальный собеседник предлагает встретиться, как следует поступить?

- а) **Посоветоваться с родителями и ничего не предпринимать без их согласия**
- б) Пойти на встречу одному
- в) Пригласить с собой друга

4. Что в Интернете запрещено законом?

- а) Размещать информацию о себе
- б) **Размещать информацию других без их согласия**
- в) Копировать файлы для личного использования

5. Действуют ли правила этикета в Интернете?

- а) Интернет - пространство свободное от правил
- б) В особых случаях
- в) **Да, как и в реальной жизни**