**Формирование познавательных компетенций обучающихся 7-9 классов в сети Интернет**

**Осторожно, подделка!**

**Чем опасны сайты-подделки?**

* крадут пароли
* распространяют вредоносное ПО
* навязывают платные услуги

Как не стать жертвой мошенников?

Как определить подделку?

Как обезопаситься?

Используй функционал браузера: «избранное», «закладки»!

Используй функционал браузера: «избранное», «закладки»!

Обрати внимание на настоящий адрес сайта!

При наведении мыши реальный адрес отображается
во всплывающей подсказке.

Как обманывают в Интернете?

* Просят подтвердить логин/пароль.
* Предлагают бесплатный антивирус.
а устанавливают вредоносное ПО, вирусы.
* Просят отправить СМС (платное).

Закрой страницу, блокировка пропала? Все в порядке!

Проверь систему антивирусом

Авторизуйся под своими аккаунтами и убедись, что все в порядке!

Смени пароли к аккаунтам, которые используешь!

***Осторожно, спам!***

Первоначально слово «SPAM» появилось в 1936 г. Оно расшифровывалось как SPiced hAM (острая ветчина) и было товарным знаком для мясных консервов.

Cпам – это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания.

ПОМНИ: идя на поводу у СПАМа есть риск:

1. Отправить платное СМС, оплатить навязанную услугу.
2. Получить платную подписку на ненужную информацию.
3. Потерять учётные и (или) иные данные.
4. Стать жертвой обмана.

Будь внимателен!

Настрой безопасность браузера и почтовой программы (подключи антифишинг, защиту от спама и др. встроенные средства защиты)!

Используй дополнительные расширения браузеров, например AddBlock (позволяет блокировать СПАМ и рекламные блоки), WOT (показывает рейтинг сайта среди интернет-пользователей)!

Используй Антивирус и файерволл!

Проверяй надёжность поставщика услуг, используй информационные сервисы «who is»!

**Персональные данные и личная информация в Интернете**

Персональные данные – твоя частная собственность, прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Персональные данные охраняет Федеральный Закон № 152 – ФЗ «О персональных данных»

**Кому и зачем нужна твоя персональная информация?**

80% преступников берут информацию в соц. сетях.

Личная информация используется для кражи паролей.

Личная информация используется для совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг , хищение!

Меры предосторожности

При регистрации в социальных сетях следует использовать только Имя или Псевдоним (ник)!

Настрой приватность в соц. сетях и других сервисах

Не публикуй информацию о своём местонахождении и (или) материальных ценностях!

Хорошо подумай, какую информацию можно публиковать в Интернете!

Не доверяй свои секреты незнакомцам из Интернета!

**Анонимность в сети**

ЗАПОМНИ! АНОНИМНОСТЬ В ИНТЕРНЕТЕ - ЭТО МИФ!

Следы пребывания в Интернете хранятся долго, даже прокси и анонимайзеры не помогут скрыться!

Веди себя в интернете вежливо, как в реальной жизни

ВНИМАНИЕ: Будь осторожен при общении с незнакомцами в сети!
Ими могут оказаться:

Маньяки, педофилы, извращенцы. Завлекают в свои сети, склоняют к совершению развратных действий! Такое общение может быть опасным для жизни!

Интернет-ХАМЫ (Тролли) провоцируют на необдуманные поступки и необоснованную агрессию!

Киберпреступники зачастую обманом похищают чужое имущество!

Хакеры используют анонимность для распространения вредоносного программного обеспечения, завладения учётными данными, платёжными реквизитами, персональной информацией!

**Открытые сети, чужая техника**

Небрежное отношение к личной информации может привести к её утере!

ПОМНИ :

1. Будь осторожен в открытых и небезопасных сетях. Подключение
к ложной сети может моментально лишить тебя всей персональной информации, хранящейся в твоем электронном устройстве: преступнику станут доступны пароли, и другая информация.
2. Опасно оставлять свои учётные данные на устройстве, которое тебе не принадлежит, этими данными могут воспользоваться
в преступных целях.

Несколько простых правил, которые следует соблюдать при работе в открытых сетях или с использованием «чужой» техники:

1. При работе с публичным устройством используй пункт «чужой компьютер».
2. Используй режим «приватного просмотра»
в браузере.
3. Всегда используй кнопку «выйти» при завершении работы с ресурсом.
4. Отказывайся от сохранения пароля при работе на «чужом компьютере».
5. Используй безопасное соединение с почтой и сервисами (безопасное соединение обозначено замком
с зелёным текстом).
6. Не оставляй без присмотра устройства доступа в сеть (телефон, планшет, ноутбук).
7. Используй шифрованные хранилища данных, которые помогут защитить твои личные файлы.
8. Используй сложные пароли, состоящие из прописных и заглавных латинских букв и цифр, а также символов.
9. Используй только открытые сети в надежности которых ты уверен.

**Интенет-мошенничество**

Знай:
Современный мобильный телефон/планшет - это не просто средство связи или красивая игрушка,
а полноценное коммуникационное устройство не уступающее по производительности и функционалу персональному компьютеру.

Внимание! Персональные данные!

Сегодня мобильные устройства содержат важную информацию:

* Список контактов;
* Личные фотографии/видеозаписи;
* Данные доступа к электронной почте и иным аккаунтам в сети;
* Данные о банковских картах/платежах;
* Имеют привязку к балансу сим-карты оператора связи.
* установи мобильную версию антивируса на своё мобильное устройство;
* установи приложения, шифрующие твои данные - они защитят личные файлы;
* устанавливай приложения только из проверенных источников, внимательно читай отзывы пользователей
* отключи функцию автоподключения к открытым Wi-Fi сетям
* используй только защищённые Wi-Fi сети;
* обязательно правильно завершай работу с публичным Wi-Fi;
* внимательно изучай права, запрашиваемые мобильными приложениями;
* используй только проверенные мобильные сервисы.

ПОМНИ: Чем больше Всемирная Паутина проникает в жизнь людей, тем больше появляется злоумышленников, пытающихся всеми возможными путями лишить тебя денег!

Кардинг - способ мошенничества с использованием банковских карт. Преступники похищают реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя.

Фишинговые сообщения - это уведомления,

отправленные от имени администраторов банковских или других платежных систем. Они призывают пользователей пройти по фальшивой ссылке, чтобы украсть конфиденциальные данные. Действия подобного рода нацелены на банковский счет или учетную запись в виртуальной платежной системе. Как только преступники получают необходимую им информацию, они моментально используют ее для доступа к банковскому счету.

Уведомления о выигрыше:

В письме сообщается о том, что ты выиграл крупную сумму денег. Цель мошенника - выманить у тебя деньги за получение выигрыша. Обычно он списывает это на налог. Потеряв бдительность, ты можешь перевести крупную сумму на счет мошенников.

«Нигерийские» письма:

В тексте такого письма обычно содержится информация о том, что у автора письма есть много денег, полученных не совсем законным путём, и поэтому он не может хранить деньги на счету в банках своей страны. Ему срочно необходим счет за рубежом, куда можно перечислить деньги. Авторы подобных писем попросят тебя обналичить крупную денежную сумму, в качестве вознаграждения обещая от 10% до 30% от заявленной в письме суммы. Идея мошенничества заключается в том, что пользователь предоставит доступ к своему счету, с которого позже будут списаны все денежные средства.

Попрошайничество:

Мошенники давят на жалость и отправляют письма с просьбой о помощи якобы от благотворительных организаций или нуждающихся людей.

В действительности такие сообщения содержат ссылки на реальные организации и фонды, но реквизиты для перечисления денежных средств указываются ложные.

Удаляй письма, которые содержат не относящуюся к тебе информацию, связанную с денежными средствами, особенно от неизвестных людей.

Не будь слишком доверчивым, проверяй всю информацию, содержащую просьбы
о помощи, иначе помощь потом потребуется тебе самому.

Не сообщай посторонним лицам свои персональные данные, номера счетов, пин-коды и т.п.

Не переходи по ссылкам, указанным в подозрительных письмах.

**Правила безопасности:**

* Не уверен в своих знаниях? Используй учетную запись с ограниченными правами!
* Не работай от имени администратора (root) - это убережет
от большинства заражений;
* Используй антивирусную защиту (лучше бесплатный антивирус,
чем никакого; коммерческие программы предоставляют дополнительные функции и удобства);
* Регулярно обновляй систему и антивирус;
* Настрой дополнительные функции (блокировку рекламы в браузере, функции антифишинга, блокировку всплывающих окон, режим безопасного поиска);
* Используй официальное лицензионное и (или) свободное программное обеспечение;
* Учитывай рекомендации программ защиты (не заходи на сайты, которые помечены как опасные, не открывай файлы, которые блокирует антивирус);
* Ограничивай время работы
в Интернете – живи реальной жизнью!