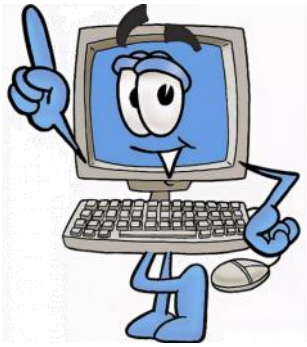
По материалам сайта https://единыйурок.рф/index.php/proekty/urok.
Картинки – https://yandex.ru
https://bipbap.ru/pictures/kartinki-bezopasnyj-internet-23-foto.html

Информационная памятка для родителей



«Компьютерные вирусы»

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, 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 распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливайте патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивайте их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включайте его;
3. Работайте на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
4. Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничьте физический доступ к компьютеру для посторонних лиц;
6. Используйте внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывайте компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал Ваш знакомый. Лучше уточните у него, отправлял ли он Вам их.

Информационная безопасность «*Сети WI-FI*»

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «WirelessFidelity», который переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi:

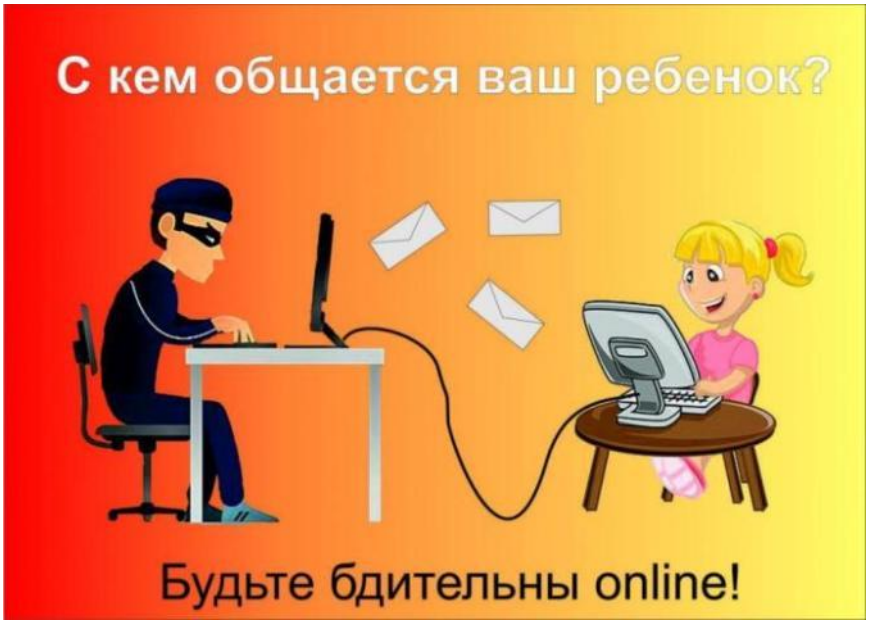
1. Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используйте и обновляйте антивирусные программы и брандмауер. Тем самым вы обезопасите себя от закачки вируса на свое устройство;
3. При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
4. Не используйте публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
5. Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводите именно «https://»;
6. В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускайте автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

Информационная памятка «*Социальные сети*»

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. 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:

1. Ограничьте список друзей. В друзьях не должно быть случайных и незнакомых людей;
2. Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать эту информацию;
3. Защищайте свою репутацию - держите ее в чистоте и задавайте себе вопрос: хотел бы я, чтобы другие пользователи видели, что я загружаю? Подумайте, прежде чем что-то опубликовать, написать и загрузить;
4. Если вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информацию: имя, место жительства;
5. Избегайте размещения фотографий в Интернете, где вы изображены на местности, по которой можно определить ваше местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.



Информационная памятка «*Электронные деньги*»

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

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжите к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудете свой платежный пароль или зайдете на сайт с незнакомого устройства;
2. Используйте одноразовые пароли. После перехода на усиленную авторизацию Вам уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выберите сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;
4. Не вводите свои личные данные на сайтах, которым не доверяете.

Информационная памятка «*Электронная почта*»

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывайте в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
3. Используйте двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используйте эту возможность;
6. Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым доверяете. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывайтефайлы и другие вложения в письмах даже если они пришли от друзей. Лучше уточните у них, отправляли ли они Вам эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

Информационная памятка «*Мобильный телефон*»

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будьте осторожны, ведь когда предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему вашего смартфона;
4. Используйте антивирусные программы для мобильных телефонов;
5. Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После того как выйдете с сайта, где вводили личную информацию, зайдите в настройки браузера и удалитеcookies;
7. Периодически проверяйте, какие платные услуги активированы на вашем номере;
8. Давайте свой номер мобильного телефона только людям, которым вы знаете и кому доверяете;
9. Bluetooth должен быть выключен, когда Вы им не пользуетесь. Не забывайте иногда проверять это.

Информационная памятка«*Online игры»*

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, 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.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи вашего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности вашего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает вам неприятности, заблокируйте его в списке игроков;
2. Пожалуйтесь администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3. Не указывайте личную информацию в профайле игры;
4. Уважайте других участников по игре;
5. Не устанавливайте неофициальные патчи и моды;
6. Используйте сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока играете, ваш компьютер могут заразить.

Информационная памятка
«Фишинг или кража личных данных»

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

1. Следите за своим аккаунтом. Если Вы подозреваете, что ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используйтебезопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используйте сложные и разные пароли. Таким образом, если Вас взломают, то злоумышленники получат доступ только к одному вашему профилю в сети, а не ко всем;
4. Если Вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у вас в друзьях, о том, что васвзломали и, возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установите надежный пароль (PIN) на мобильный телефон;
6. Отключите сохранение пароля в браузере;
7. Не открывайте файлы и другие вложения в письмах, даже если они пришли от Ваших друзей. Лучше уточните у них, отправляли ли они Вам эти файлы.

Информационная памятка «*Цифровая репутация*»

Цифровая репутация - это негативная или позитивная информация в сети о Вас. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на реальной жизни. «Цифровая репутация» - это имидж, который формируется из информации о ва в интернете.

Ваше место жительства, учебы, ваше финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.

Многие легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Вы даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять Вас на работу.

Комментарии, размещение ваших фотографий и другие действия могут не исчезнуть даже после того, как вы их удалите. Вы не знаете, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о Вас окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумайте, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установите ограничения на просмотр вашего профиля и его содержимого, сделайте его только «для друзей»;
3. Не размещайте и не указывайте информацию, которая может кого-либо оскорблять или обижать.

Информационная памятка «*Авторское право*»

Пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к вашим аккаунтам до блокировки вашего устройства, где установленный не легальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.