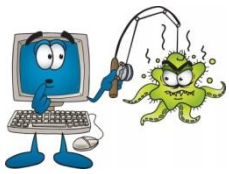


Компьютерные вирусы

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:

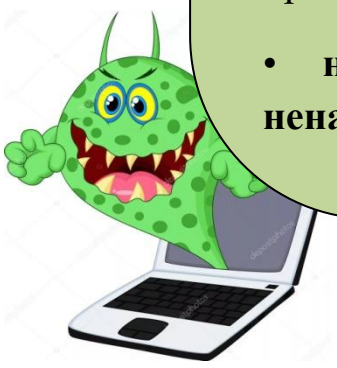
• используй современные **лицензионные операционные системы**, имеющие серьёзный уровень защиты от вредоносных программ;

• постоянно **устанавливай пачти** (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие **обновления** своей операционной системы: скачивай их только с **официального сайта разработчика ОС**;

• работай на своем компьютере **под правами пользователя**, а не администратора - это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

• используй **антивирусные программные продукты** известных производителей, с автоматическим обновлением баз;

• **не открывай** компьютерные файлы, полученные из **ненадёжных** источников



Wi-Fi

Сеть, которая раздает **доступ в интернет** без проводов, **по радиоканалам**. Как и с любым гаджетом, работа через wi-fi имеет свои положительные и отрицательные стороны.

Плюсы: беспроводное подключение, комфортное размещение в любой части дома, кафе и т.д., подключение нескольких устройств одновременно.

Минусы: небольшие задержки во время соединения; редко, но бывают сбои в работе роутера, и ,как следствие, время на перезагрузку.

Советы по безопасности работе в общедоступных сетях Wi-fi:

• **НЕ передавай** свою **личную** информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

• Используй и **обновляй антивирусные программы** и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

• При использовании Wi-Fi **отключи** функцию «Общий доступ к файлам и принтерам»;

• **Не используй публичный** WI-FI для передачи **личных** данных, например для выхода в социальные сети или в электронную почту;

• Ипользуй **только защищенное соединение** через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
• В мобильном телефоне **отключи** функцию «**Подключение к Wi-Fi автоматически**». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Кибербуллинг (виртуальное издевательство)

Преследование сообщениями, содержащими **оскорбления**, агрессию, **запугивание**; хулиганство; социальное **бойкотирование** с помощью различных интернет-сервисов

Основные советы по борьбе с кибербуллингом:

• не бросайся в бой - лучший способ: **нужно посоветоваться** как себя вести и, если нет того, к кому можно обратиться, то вначале **успокоиться**; если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

• управляй своей **киберрепутацией**;

• **анонимность** в сети **мнимая**: существуют способы выяснить, кто стоит за анонимным аккаунтом;

• **не стоит** вести **хулиганский** образ виртуальной жизни: интернет **фиксирует** все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

• **соблюдай** свой виртуальную **честь** смолоду;

• **игнорируй** единичный негатив. Обычно агрессия прекращается на начальной стадии;

• **бан агрессора**: в программах обмена мгновенными сообщениями, в социальных сетях есть **возможность блокировки** отправки сообщений с определенных адресов;

• **сообщи взрослым** о факте агрессивного поведения в сети.

Социальные сети

Это **онлайн-платформы**, которые используются для общения, знакомств, создания **социальных отношений между людьми**, которые имеют схожие интересы или офлайн-связи, а также для **развлечения** (музыка, фильмы) и **работы**. 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:

- **ограничь** список друзей. У тебя в друзьях **не должно** быть **случайных** и **незнакомых** людей;
- **защищай** свою **частную жизнь**. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию;
- **защищай** свою **репутацию** - подумай, прежде чем что-то опубликовать, написать и загрузить;
- если ты говоришь с **людьми**, которых **не знаешь, не используй** свое **реальное** имя и другую личную информации: имя, место жительства, место учебы и прочее;
- **избегай** размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- **при регистрации** в социальной сети необходимо использовать **сложные пароли**, состоящие из букв и цифр и с количеством знаков не менее 8;
- для социальной сети, почты и других сайтов необходимо использовать **разные пароли**, тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Платежное средство, существующее исключительно в электронном виде, то есть в виде записей в специализированных электронных системах. Это очень удобный способ платежей. В России они функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные (те, в которых разрешается проводить операции без идентификации пользователя) и не анонимные (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:

• **привяжи** к счету **мобильный** телефон. Это самый **удобный** и **быстрый** способ восстановить доступ к счету; привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

• используй **одноразовые пароли**: после перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

• выбери **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!);

• **Не вводи** свои **личны**е данные на сайтах, которым не доверяешь.

Электронная почта

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:

• надо выбрать **правильный почтовый сервис**. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

• **не указывай** в личной почте **личную информацию** (ФИО, дату рождения и пр.);

• используй **двухэтапную авторизацию**, когда помимо пароля нужно вводить код, присылаемый по SMS;

• выбери **сложный пароль**: для каждого почтового ящика должен быть **свой надежный**, устойчивый к взлому пароль;

• если есть **возможность** написать самому свой личный вопрос, **используй** эту возможность;

• используй **несколько** почтовых ящиков: первый для частной переписки с адресатами, которым ты доверяешь, это электронный адрес не надо использовать при регистрации на форумах и сайтах;

• **не открывай** файлы и другие вложения в письмах даже если они пришли от твоих друзей, лучше **уточни** у них, отправляли ли они тебе эти файлы;

• после **окончания работы** на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на **«Выйти»**.

Online игры

Красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции. Эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи, закрываются уязвимости серверов**. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.**

Основные советы по безопасности твоего игрового аккаунта:

• Если другой игрок ведет себя плохо или создает тебе неприятности, **заблокируй** его в списке игроков;

• **Пожалуйся администраторам** игры на плохое поведение этого игрока, желательно приложить какие-то **доказательства** в виде скринов;

• **Не указывай личную** информацию в профайле игры;

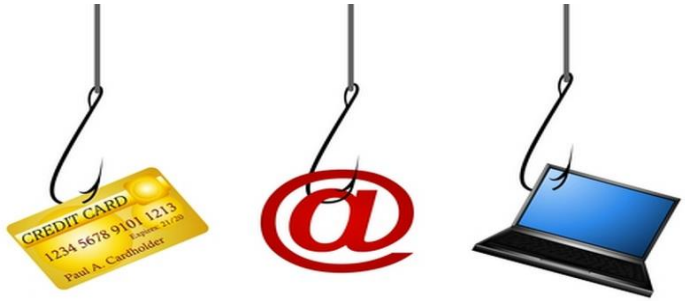
• **Уважай** других участников по игре;

• **Не устанавливай неофициальные** патчи и моды;

• Используй **сложные** и разные **пароли**;

• Даже во время игры **не** стоит **отключать антивирус**. Пока ты играешь, твой компьютер могут заразить.

Фишинг (кража личных данных)



Получение 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:

4

• **следи за своим аккаунтом**: если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

• используй **безопасные веб-сайты**, в том числе, интернет-магазинов и поисковых систем;

• используй **сложные** и **разные пароли**, таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

• если тебя **взломали**, то необходимо **предупредить** всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

• установи **надежный пароль** (PIN) на мобильный телефон;

• **отключи сохранение пароля** в браузере;

• **не открывай** файлы и другие вложения в письмах даже если они пришли от твоих друзей, лучше **уточни** у них, отправляли ли они тебе эти файлы.

.

Цифровая репутация

Негативная или позитивная информация в сети о человеке. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на реальной жизни. «Цифровая репутация» - это имидж, который формируется из информации о человеке в интернете. Место жительства, учеба, финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.

Комментарии, размещение фотографий и другие действия могут не исчезнуть даже после того, как они будут удалены. Неизвестно, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред.

Основные советы по защите цифровой репутации:

• **Подумай**, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

• В настройках профиля **установи ограничения** на просмотр твоего профиля и его содержимого, сделай его только «**для друзей**»;

• Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.