Кибербезопасность - это практика защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от злонамеренных атак. Это также известно как безопасность информационных технологий или безопасность электронной информации.

Любой может случайно занести вирус в защищенную систему, не соблюдая надлежащие методы обеспечения безопасности.

Компьютерный вирус - это вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение.

Основная функция - нарушение работы программно-аппаратных комплексов:
удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п.

Методы защиты от вредоносных программ:

1.Использовать современные операционные системы с серьёзным уровнем защиты;
2. Своевременно устанавливать обновления своей операционной системы. Скачивать их только с официального сайта разработчика ОС;
3. Работать на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
4. Использовать антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничить физический доступ к компьютеру для посторонних лиц;
6. Использовать внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;
7. Не открывать компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислали знакомые. Лучше уточнить у отправителя, отправлял ли он эти файлы.

Сети WI-FI

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Но многие эксперты считают, что общедоступные WiFi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi

1.Не передавать свою личную информацию через общедоступные Wi-Fi сети. Не вводить пароли доступа, логины и какие-то номера;
2.Использовать и обновляй антивирусные программы и брандмауэр;
3.При использовании Wi-Fi лучше отключить 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 использовать публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;
5. Использовать только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводить именно «https://»;
6.В мобильном телефоне отключить функцию «Подключение к Wi-Fi автоматически». Не допускать автоматического подключения устройства к сетям Wi-Fi без согласия.

Социальные сети

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, содержащая личную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. 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. Ограничить список друзей. Не должно быть случайных и незнакомых людей;
2. Защищать свою частную жизнь. Не указывать пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о родителях и планах на каникулы;
3. Защищать свою репутацию. Подумать, прежде чем что-то опубликовать, написать и загрузить;
4. В разговоре с незнакомыми людьми не сообщать личную информацию: имя, место жительства, место учебы и прочее;
5.Избегать размещения фотографий в Интернете, по которым можно определить местоположение;
6.При регистрации в социальной сети необходимо использовать сложные пароли, состоящиеиз букв и цифр и с количеством знаков не менее 8;
7.Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда, при взломе, злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги -это очень удобный способ платежей, однако существуют мошенники, которые этим пользуются.
В России 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 не анонимных идентификация пользователя является обязательной.

Основные советы по безопасной работе с электронными деньгами:

1.Привязать к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если Вы забудете свой платежный пароль или зайдете на сайт с незнакомого устройства;
2.Использовать одноразовые пароли. После перехода на усиленную авторизацию Вам уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Нужно выбрать 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.
4. Нельзя вводить свои личные данные на сайтах, которым Вы не доверяете.

Электронная почта

Электронная почта - это технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети .

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 указывать в личной почте личную информацию;
3. Использовать 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, лучше использовать эту возможность;
6. Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым Вы доверяете. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывайте файлы и другие вложения в письмах даже если они пришли от друзей. Лучше уточнить у них, отправляли ли они эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1.Не бросаться в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если отвечать оскорблениями на оскорбления, то только еще больше разовьётся конфликт;
2.Управлять своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4.Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все действия и сохраняет их. Удалить их будет крайне затруднительно;
5.Вести себя вежливо;
6.Игнорировать единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7.Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8.Если Вы стали свидетелем кибербуллинга. Действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

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.

Основные советы для безопасности мобильного телефона:

1.Будьте осторожны,получая предложение бесплатного контента, в нем могут быть скрыты какие-то платные услуги;
2. Думайте, прежде чем отправить SMS, фото или видео. Нужно быть уверенным в том, где они будут в конечном итоге.
3. Необходимо обновлять операционную систему смартфона;
4. Используйте антивирусные программы для мобильных телефонов;
5. Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После выхода с сайта, где вводилась личная информация, лучше зайти в настройки браузера и удали cookies;
7. Периодически нужно проверять какие платные услуги активированы на Вашем номере;
8. Давать свой номер мобильного телефона можно только знакомым людям, которым доверяете;
9.Bluetooth должен быть выключен, когда Вы им не пользуетесь. Не забывайте иногда проверять это.