ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

ВИДЫ УГРОЗ

Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной чертой которой является способность к размножению.

В дополнение к этому, вирусы могут повредить или 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:

- Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- 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, включите его;
- Работайте на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

Методы защиты от вредоносных программ:

- Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничьте физический доступ к компьютеру для посторонних лиц;
- Используйте внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
- Не открывайте компьютерные файлы, полученные из ненадёжных источников.

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 Wireless Fidelity, 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».

Многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности в общедоступных сетях Wi-fi:

- Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то персональные данные;
- Используйте и обновляйте антивирусные программы и брандмауэр. Тем самым Вы обезопасите себя от закачки вируса на твое устройство;
- 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;

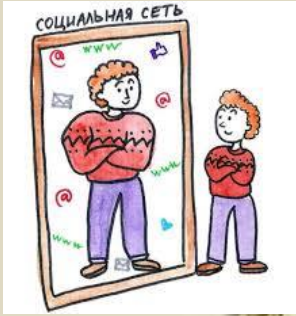
Советы по безопасности в общедоступных сетях Wi-fi:

- Не используйте публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту;
- Используйте только защищенное соединение через HTTPS, а не HTTP, т. е. при наборе веб-адреса вводите именно «https://»;
- В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускайте автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

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 необязательно с благими намерениями.



Основные советы по безопасности в социальных сетях:

- Ограничьте список друзей. У вас в друзьях не должно быть случайных и незнакомых людей;
- Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату рождения и другую личную информацию;
- Если Вы говорите с людьми, которых не знаете, то не используйте свое реальное имя и другую личную информации: имя, место жительства и другие данные;

Основные советы по безопасности в социальных сетях:

- Избегайте размещения фотографий в интернете, где Вы изображены на местности, по которой можно определить ваше 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 Вас взломают, то 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 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:

• 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;

• Используйте одноразовые пароли. После перехода на усиленную авторизацию Вам уже не будет угрожать опасность кражи или перехвата платежного пароля;

Основные советы по безопасной работе с электронными деньгами:

• Выберите сложный пароль. Преступникам будет непросто 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 вводите свои личные данные на сайтах, которым не доверяете.

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.

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 знаете и кто первый в рейтинге;
- Не указывайте в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
- Используйте двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
- Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

Основные советы по безопасной работе с электронной почтой:

- Если есть возможность написать самому свой личный вопрос, используйте эту возможность;
- Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым Вы доверяете. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах;
- Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей или коллег;
- 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:

- Не бросаться в бой. Если отвечать оскорблениями на оскорбления, то только еще больше можно разжечь конфликт;
- Управляйте своей киберрепутацией;
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
- Игнорируйте единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов

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:

- Ничего не является по-настоящему бесплатным. Будьте осторожны, ведь когда предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
- Необходимо обновлять операционную систему смартфона;
- Используйте антивирусные программы для мобильных телефонов;

Основные советы для безопасности мобильного телефона:

- Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
- Периодически проверяйте какие платные услуги активированы на номере;
- Давайте свой номер мобильного телефона только людям, которых Вы знаете и кому доверяете;
- Bluetooth должен быть выключен, когда Вы им не пользуетесь.

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:

- 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;
- Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
- Используйте сложные и разные пароли;

Основные советы по борьбе с фишингом:

- Если Вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у Вас в друзьях, о том, что Вас взломали и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
- Установите надежный пароль (PIN) на мобильный телефон;
- Отключите сохранение пароля в браузере;
- Не открывайте файлы и другие вложения в письмах даже если они пришли от друзей или коллег.

Источник информации:

Сайт «Единый урок» https://единыйурок.рф/
(курс «Основы кибербезопасности»)