ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

СВЕТЛОВСКАЯ ЦЕНТРАЛИЗОВАННАЯ
БИБЛИОТЕЧНАЯ СИСТЕМА
им. Фёдорова Н.Ф

КАК БЕЗОПАСНО ОБЩАТЬСЯ В СОЦИАЛЬНЫХ СЕТЯХ

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, в соцсетях уже зарегистрировано 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.

Советы по безопасному общению 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. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.

! Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? 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 информацию: имя, место жительства, место учебы и прочее.

! Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение.

Рекомендовано:
Министерство образования и науки РФ

Изготовлено:
Муниципальное бюджетное учреждение культуры «Светловская централизованная библиотечная система им.Фёдорова Н.Ф.»

! 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 ко всем сразу.

КАК БЕЗОПАСНО РАСПЛАЧИВАТЬСЯ ЭЛЕКТРОННЫМИ ДЕНЬГАМИ

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 идентификация пользователя является обязательной.

Меры защиты электронных денег

1. 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 незнакомог устройства.

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.
3. 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. Например, StROng!
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

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.

Меры защиты электронной почты

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.

Например, лучше выбрать
«музыкальный_фанат@»
или
«рок201 8@» вместо «андрей2005@».

Используй двухэтапную авторизацию. Это 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».**

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СМАРТФОНОМ, ПЛАНШЕТОМ

Смартфоны и планшеты содержат в себе взрослый функционал и могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока 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.

Советы по безопасному использованию мобильных устройств

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона.

Используй антивирусные программы для мобильных телефонов.

Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРБУЛЛИНГА

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

КАК ЗАЩИТИТЬСЯ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Компьютерный вирус - это программа, отличительной особенностью которой является способность к размножению. Вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.

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

Используй только защищенное соединение через HTTPS, а не HTTP, то есть при наборе веб-адреса вводи именно «https://». В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически».

4. 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.

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. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

Бань агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.

Периодически проверяй, какие платные услуги активированы на твоем номере.

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

КАК БЕЗОПАСНО ИГРАТЬ ONLINE

Online-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 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 твоего пароля, на котором основана система авторизации большинства игр.

Меры защиты твоего игрового аккаунта

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.
3. Не указывай личную информацию в профайле игры.
4. Уважай других участников по игре.
5. Не устанавливай неофициальные патчи и моды.
6. Используй сложные и разные пароли.
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Обычной кражей денег и документов 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 (от английского слова fishing - рыбная ловля), главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей.

«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 твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

1. 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.
2. Используй безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.

3. 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.