**Основные рекомендации и советы по обеспечению персональной информационной безопасности**

С каждым годом становиться все больше активных пользователей Интернета. 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**. У Вас в друзьях не должно быть случайных и незнакомых людей.
2. Защищайте свою частную жизнь. **Не указывайте пароли**, телефоны, адреса, дату и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как Вы планируете провести отпуск или каникулы.
3. Если Вы **говорите с людьми, которых не знаете**, **не используйте свое реальное** имя и другую личную информации: имя, место жительства, место учебы и прочее.
4. **Избегайте размещения фотографий** в Интернете, где Вы изображены на местности, по которой можно определить Ваше местоположение.
5. При регистрации в социальной сети необходимо **использовать сложные пароли**, состоящие из букв и цифр и с количеством знаков не менее 8.
6. Для социальной сети, почты и других сайтов необходимо использовать **разные пароли**. Тогда если Вас взломают, то злоумышленники получат доступ только к одному ресурсу, а ко всем сразу.

***Электронные деньги.*** Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. В законодательстве России их разделяют на несколько видов – анонимные и не анонимные. Анонимные - **это те, в которых разрешается проводить операции без идентификации пользовател**я, а в неанонимных идентификация пользователя является обязательной.

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 забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства.
2. **Используйте 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 и т.п., например, $tR0ng!.
4. **Не вводи свои личные данные** на сайтах, которым не доверяешь.

***Электронная почта.***Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. 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 указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13».
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS.
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность.
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым Вы доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах.
7. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».