Основные правила безопасности в сети Интернет

1. Советы по безопасности работе 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 номера;
- Используйте и обновляйте антивирусные программы и брандмауер. Тем самым Вы обезопасите себя от закачки вируса на 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 или учебе;
- 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 вводи именно «https://»;
- В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускайте автоматического подключения устройства к сетям Wi-Fi без Вашего согласия.

2. 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 твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как Вы и Ваши родители планируете провести досуг;
- Если Вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- 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.

3. 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;
- Используй одноразовые пароли. После перехода на усиленную авторизацию Вам уже не будет угрожать опасность кражи или перехвата платежного пароля;
- Выберите 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, StROng!;;
- Не вводите свои личные данные на сайтах, которым не доверяете.

4. 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 «темаI3»;
- 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;
- Если есть возможность написать самому свой личный вопрос, используйте эту возможность;
- 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;
- Не открывайте файлы и другие вложения в письмах даже если они пришли от Ваших друзей. Лучше уточните у них, отправляли ли они Вам эти файлы;
- После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

5. Основные советы по борьбе с фишингом (интернет-мошенничества):

- Следите за своим аккаунтом. Если ты подозреваешь, 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. Таким образом, если Вас взломают, то злоумышленники получат доступ только к одному Вашему профилю в сети, а не ко всем;
- 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;

6. Основные советы по защите цифровой репутации (негативная или позитивная информация в сети о Вас):

- Подумайте, прежде чем что-то публиковать и передавать у Вас в блоге или в социальной сети;
- В настройках профиля установите ограничения на просмотр Вашего профиля и его содержимого, сделайте его только «для друзей»;
- Не размещайте и не указывайте информацию, которая может кого-либо оскорблять или обижать.

Соблюдайте правила:

- Помните, что в виртуальном пространстве ответственность наступает по реальным законам;
- Уважительно и добросовестно относитесь к другим пользователям сети Интернет.

Здесь вам помогут

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор):
Справочно-информационный центр:**8 (495) 983-33-93 (пн-чт 9:00-18:00, пт 9.00-16:45)**