

**ПРОКУРАТУРА ВОЛОСОВСКОГО РАЙОНА   
ЛЕНИНГРАДСКОЙ ОБЛАСТИ**

**РАЗЪЯСНЯЕТ**

**Информационная памятка по вопросам кибербезопасности в сети «Интернет»**

***Компьютерные вирусы***

Компьютерный вирус — это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию). В большинстве случаев распространяются вирусы через интернет.

***Методы защиты от вредоносных программ:***

1. Используйте современные операционные системы, имеющие высокий уровень защиты от вредоносных программ;
2. Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением;
3. Ограничьте физический доступ к компьютеру для посторонних лиц;
4. Используйте внешние носители информации или файл из Интернета, только из проверенных источников;
5. Не открывай компьютерные файлы, полученные из ненадёжных источников.

***Электронная почта***

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети.

***Основные советы по безопасной работе с электронной почтой:***

1. Не указывать в личной почте личную информацию;
2. Используйте двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
3. Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к «взлому» пароль;
4. Используйте несколько почтовых ящиков;

***Мобильный телефон***

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. 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:***

1. Будьте осторожны, когда предлагают бесплатный контент, так как в нем могут быть скрыты какие-то платные услуги;
2. Необходимо обновлять операционную систему смартфона;
3. Используйте антивирусные программы для мобильных телефонов;
4. Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
5. Периодически проверяйте какие платные услуги активированы на номере телефона;
6. Давайте свой номер мобильного телефона только людям, которых знаете и которым доверяете;

***Фишинг или кража личных данных***

Главная цель фишинг - вида Интернет-мошенничества, 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:***

1. Следите за своим аккаунтом. Если подозреваете, что Ваша 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. Используйте сложные и разные пароли. Таким образом, если Вас взломают, то злоумышленники получат доступ только к одному профилю в сети, а не ко всем;
4. Если Вас взломали, то необходимо предупредить всех своих знакомых, о том, что Вас взломали и, возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установите надежный пароль (PIN) на мобильный телефон;
6. Отключите сохранение пароля в браузере;