Общие правила безопасности работы в сети «Интернет»

Соблюдение этих правил поможет защитить рабочие устройства и конфиденциальную информацию от киберугроз.

1. Работа с веб-сайтами

❗ **Внимательно проверяйте доменные имена**. Особенно важно при проведении финансовых операций: фишинговые сайты могут отличаться от оригинальных даже на один символ.

❗ **Используйте заранее сформированные закладки** для доступа к часто посещаемым ресурсам – это снижает риск перехода на поддельный сайт.

❗ **Немедленно закрывайте страницы** с большим количеством навязчивой рекламы (баннеры, всплывающие окна и т.д.) сразу после их открытия.

❗ **Проверяйте URL-адрес сайта при скачивании файлов**. Официальные сайты производителей ПО используют защищенное соединение (протокол https, значок закрытого замка в адресной строке браузера). Скачивайте файлы только с проверенных источников.

2. Правила работы с электронной почтой

❗ **Проверяйте адрес отправителя,** даже если имя вам знакомо.

❗ **Будьте бдительны с письмами**, содержащими призывы к действиям («открой», «прочитай», «ознакомься» и т.д.), а также с письмами на темы финансов, банковских операций, геополитики или с содержащими угрозы.

❗ **Не переходите по ссылкам в письмах**, особенно если: ссылка длинная; используется сервис сокращения ссылок (bit.ly, tinyurl.com и т.д.); ссылка заменена словом.

Не открывайте вложения, особенно если они содержат: исполняемые файлы (.exe); файлы с расширениями .rtf, .lnk, .chm, .vhd, .pdf.exe и др.

3. Дополнительные меры безопасности

❗ **Избегайте подключения к общедоступным Wi-Fi – сетям** (без пароля). Такие точки доступа могут использоваться злоумышленниками для фишинговых атак.

❗ **Не передавайте конфиденциальную информацию по открытым каналам связи.**

❗ **Ограничьте публикацию личной информации в социальных сетях.**

Прокуратура г. Сосновый Бор Ленинградской области, 2026 г.