Профилактика кибератак (фарминг, социальная инженерия, фишинг)

Что такое «фарминг», «фишинг» и «социальная инженерия»:

Фарминг — вид кибератаки, при котором злоумышленники перенаправляют жертву на подложный сайт или в группу, внешне неотличимые от настоящего ресурса. Цель — похищение конфиденциальной информации: паролей, банковских реквизитов, личных данных.

Фишинг — метод получения конфиденциальных данных через обманные сообщения (например, письма или SMS со ссылками на поддельные сайты).

Социальная инженерия — манипуляция людьми с целью заставить их раскрыть конфиденциальную информацию или выполнить определённые действия (например, открыть заражённый файл).

Способ действия злоумышленников:

Злоумышленники используют **комплексную схему**, которая включает: дублирование профиля вашего знакомого; создание фейковой «группы помощи» в мессенджерах (например, в Telegram); размещение заманчивого рекламного контента; наполнение группы множеством поддельных участников, демонстрирующих активность; приглашение настоящих пользователей после формирования доверия (при этом право оставлять комментарии может быть ограничено).

При запуске опасного файла вирус может: заменить значок программы на прозрачный (чтобы скрыться от внимания пользователя); передать хакерам историю входящих сообщений за последние 3 дня; активировать окно для отправки снимков из фотогалереи на удалённый сервер преступников; автоматически отправить заражённый файл всем контактам в списке мессенджера; отправлять SMS-сообщения на случайные номера.

Чтобы избежать таких результатов необходимо соблюдать простые правила:

1. Будьте бдительны при переходе по ссылкам: проверяйте адрес сайта в адресной строке браузера — он должен совпадать с официальным; не переходите по ссылкам из подозрительных писем, SMS или сообщений в мессенджерах.

2. Проверяйте подлинность профилей и групп: если вам пишет «знакомый», но что-то кажется странным (непривычный стиль общения, срочная просьба о помощи), свяжитесь с ним другим способом для подтверждения; проверяйте количество подписчиков, активность и отзывы о группах и каналах перед вступлением.

3. Не открывайте подозрительные файлы и вложения: не запускайте файлы из неизвестных источников, даже если они отправлены «знакомым» контактом.

4. Настройте безопасность аккаунтов: регулярно меняйте пароли, используйте сложные комбинации; ограничьте доступ к личной информации в настройках приватности.

Помните: лучшая защита от кибератак — это бдительность и осведомлённость. Соблюдайте правила кибербезопасности и делитесь этой информацией с коллегами и близкими.

Прокуратура г. Сосновый Бор Ленинградской области, 2026 г.