Одной из наиболее распространенных форм киберпреступлений является мошенничество через интернет. Злоумышленники создают фальшивые сайты, имитирующие официальные ресурсы банков, интернет-магазинов и других организаций, чтобы получить личные данные пользователей. Они также могут использовать фишинговые письма для кражи данных учетных записей и паролей.

Другой формой киберпреступлений является взлом компьютерных систем. Злоумышленники используют уязвимости в программном обеспечении и операционных системах для получения доступа к конфиденциальной информации и ее последующего использования в своих целях.

Социальная инженерия используется злоумышленниками для манипулирования поведением людей и их действиями в интернете. Например, они могут создавать фальшивые профили в социальных сетях, чтобы привлечь внимание потенциальных жертв и получить от них информацию. Также злоумышленники могут использовать психологические приемы для того, чтобы убедить жертву предоставить им доступ к своим устройствам или системам.

В целях профилактики и предупреждения преступлений, совершаемых с использованием информационных технологий и методов социальной инженерии, Дальневосточным юридическим институтом (филиалом) Университета прокуратуры Российской Федерации при участии студенческого объединения «Киберволонтеры» подготовлены социальные видеоролики на темы:

– «Мошенническая схема «Направление электронных писем, сообщений и звонки от имени различных фондов» (disk.yandex.ru/i/I06gdo2q...);

– «Мошенническая схема «Игра на бирже» (disk.yandex.ru/i/VgQM6cWL...);

– «Мошенническая схема «Звонок от сотрудников правоохранительных органов» (disk.yandex.ru/i/WaxOnz8z...);

– «Мошенническая схема «Звонок из службы безопасности банка» (disk.yandex.ru/i/VieGq2HB...).

Предлагаем вам ознакомиться с видеороликами, чтобы знать, как защитить себя, а главное своих детей от киберпреступников.