

СПЛУФИНГ

кибератака, при которой злоумышленник
маскируется под другого человека / компанию,
чтобы завоевать **ВАШЕ** доверие



**СЕТЕВАЯ
БЕЗОПАСНОСТЬ**



ЦЕЛЬ СПУФИНГА

- получить доступ к Вашим устройствам
- распространить вирусные программы
- украсть денежные средства
и личную информацию



**СЕТЕВАЯ
БЕЗОПАСНОСТЬ**



ПРИМЕР АТАКИ



ПОДМЕНА НОМЕРА

используется ложная информация о входящем вызове на вашем смартфоне. Например, звонят якобы с номера 900 или от имени вашего друга



ПОДМЕНА САЙТА

создаётся вредоносный поддельный сайт с похожим адресом и оформлением на официальный сайт известного ресурса.

ПОДМЕНА ФАЙЛА

рассылается вредоносный файл, похожий на рабочий документ или архив, но при открытии такого файла выполняется скрытая установка вирусной программы на Ваше используемое устройство



**СЕТЕВАЯ
БЕЗОПАСНОСТЬ**



КАК СЕБЯ ЗАЩИТИТЬ?

- ✓ ОБРАЩАЙТЕ ВНИМАНИЕ НА АДРЕС ОТПРАВИТЕЛЯ СООБЩЕНИЙ
- ✓ БУДЬТЕ БДИТЕЛЬНЫ И ОСТОРОЖНЫ С ПОЧТОВЫМИ ВЛОЖЕНИЯМИ
- ✓ ПРОВЕРЯЙТЕ АДРЕСНУЮ СТРОКУ В БРАУЗЕРЕ
- ✓ ОСМОТРИТЕЛЬНО ОТНОСИТЕСЬ К ТЕЛЕФОННЫМ ЗВОНКАМ
- ✓ НЕ РАЗГЛАШАЙТЕ В СЕТИ ВАШИ ЛИЧНЫЕ ДАННЫЕ



**СЕТЕВАЯ
БЕЗОПАСНОСТЬ**

