



СПУФИНГ — ЧТО ЭТО? МЕТОДЫ И МЕРЫ ЗАЩИТЫ

СПУФИНГ (от англ. spoofing - «подделывать») — это кибератака, при которой мошенники выдают себя за кого-то другого, чаще всего — за официальных представителей банков, магазинов, государственных и других организаций.

Цель спуфинга — завоевать доверие жертвы, чтобы получить доступ к устройствам, украсть деньги, личные данные или распространить вирусные программы.



ОСНОВНЫЕ ТИПЫ СПУФИНГА

- ▶ **Спуфинг с подменой адреса электронной почты:** мошенники подделывают адрес отправителя, чтобы вы поверили в подлинность письма.
- ▶ **Спуфинг с подменой сайта:** создание фальшивого сайта, похожего на настоящий, для кражи учётных данных.
- ▶ **Спуфинг с подменой номера вызывающего абонента:** на экране отображается ложный номер телефона.
- ▶ **SMS спуфинг:** отправка сообщений с поддельного номера, часто имитирующего известные компании.
- ▶ **IP спуфинг:** подмена IP адреса для маскировки источника атаки.
- ▶ **ARP спуфинг (ARP poisoning):** перехват данных в локальной сети путём подмены ARP сообщений.
- ▶ **DNS спуфинг:** перенаправление на поддельные сайты через подмену DNS записей.

ПРИЗНАКИ СПУФИНГ АТАКИ

В электронной почте:

- ✓ подозрительный или слегка изменённый адрес отправителя (например, замена буквы «о» на цифру «0»);
- ✓ грамматические ошибки и опечатки;
- ✓ слишком заманчивые предложения («вы выиграли приз»);
- ✓ просьбы срочно предоставить личные данные или перевести деньги;
- ✓ подозрительные вложения или ссылки.



На сайтах:

- ✓ отсутствие HTTPS в адресной строке (нет буквы «s» в https://);
- ✓ нет значка замка или зелёной полосы слева от URL;
- ✓ искажённые логотипы, цвета или неполная информация;
- ✓ пустые разделы (например, «Политика конфиденциальности»).



В звонках и SMS:

- ✓ незнакомый номер, маскирующийся под официальный;
- ✓ настойчивые просьбы сообщить личные данные (пароли, CVV коды);
- ✓ сообщения о «срочных действиях» или «проблемах с аккаунтом».

КАК ЗАЩИТИТЬСЯ ОТ СПУФИНГА: ПОШАГОВЫЕ РЕКОМЕНДАЦИИ



ЧТО ДЕЛАТЬ:

Проверяйте отправителя:

- ✓ внимательно изучите адрес электронной почты или номер телефона;
- ✓ наведите курсор на ссылку в письме, чтобы увидеть реальный URL.

Используйте HTTPS и значок замка:

- ✓ убедитесь, что сайт защищён (адрес начинается с <https://>, есть значок замка).

Включите спам фильтры:

- ✓ настройте фильтры в почте и на телефоне, чтобы отсеивать подозрительные сообщения.

Подтвердите информацию:

- ✓ если письмо или звонок кажутся подозрительными, свяжитесь с организацией по официальному номеру или через официальный сайт.

Используйте менеджер паролей:

- ✓ он не заполнит данные на поддельных сайтах.

Настройте двухфакторную аутентификацию (2FA):

- ✓ это добавит дополнительный уровень защиты вашим аккаунтам.

Установите антивирусное ПО:

- ✓ регулярно обновляйте его для защиты от новых угроз.

Создавайте надёжные пароли:

- ✓ используйте разные пароли для разных аккаунтов;
- ✓ комбинируйте заглавные и строчные буквы, цифры и специальные символы;
- ✓ меняйте пароли периодически.

Обновляйте ПО:

- ✓ устанавливайте обновления ОС, браузеров и приложений.

Будьте бдительны:

- ✓ не доверяйте сообщениям с просьбами «срочно» что то сделать;
- ✓ проверяйте информацию через официальные источники.

ЧТО НЕ ДЕЛАТЬ:



- ✗ не переходите по подозрительным ссылкам;
- ✗ не открывайте вложения от неизвестных отправителей;
- ✗ не отвечайте на письма или звонки от незнакомых номеров;
- ✗ не разглашайте личную информацию (номера карт, пароли, CVV коды и т.д.);
- ✗ не используйте один и тот же пароль для нескольких аккаунтов.

При необходимости личного приема или для составления проекта
досудебной претензии потребитель могут обратиться
в Минторг РБ по адресу:

450008, г. Уфа, ул. Цюрупы, 13, кабинет 703

с 9.00 до 18.00 по будням, перерыв с 13.00 до 14.00

Телефон «горячей линии»
8 (347) 218-09-78

Уфа-2026

Посетите раздел «Защита прав
потребителей» сайта Минторга
РБ, где размещена актуальная
информация для потребителей.

