ИНФОРМАЦИОННЫЙ МАТЕРИАЛ

Что такое спуфинг и как от него защититься?

Спуфинг - кибер-атака, в рамках которой мошенник выдает себя за какой-либо надежный источник, чтобы получить доступ к важным данным или информации. Подмена может происходить через Интернет-сайты, электронную почту, телефонные звонки, текстовые сообщения, IP-адреса и серверы.

Цель спуфинга - получить доступ к личной информации, украсть деньги, распространить вредоносное программное обеспечение.

Типы спуфинг-атак:

-Подмена номера - мошенник использует ложную информацию для изменения идентификатора вызывающего абонента т.е. мошенник звонит якобы с другого телефона – например, телефон вашего друга.

-Подмена сайта - мошенник пытается создать опасный (вредоносный) сайт похожим на надежный безопасный сайт (например, известного банка), используя его шрифты, цвета и логотипы.

-Подмена почты - мошенник рассылает электронные письма с поддельными адресами отправителей с намерением заразить ваш компьютер вредоносными программами, заполучить деньги или украсть информацию. В качестве адресов электронной почты отправителей зачастую подставляются те адреса, которым вы можете доверять.

-Подмена IP-адреса - мошенник стремится скрыть реальное местоположение в Интернете того места, откуда запрашиваются или куда отправляются данные пользователя, чтобы заставить компьютер жертвы думать, что информация, отправляемая мошенником пользователю, исходит из надежного источника, что позволяет вредоносному контенту доходить до пользователя.

-SMS-спуфинг - мошенник отправляет текстовое или SMS-сообщение, используя номер телефона другого человека.

Существует ряд рекомендаций, которым следует придерживаться, чтобы защитить себя от спуфинг-атак:

- Включайте спам-фильтр: это предотвратит попадание большинства поддельных писем в ваш почтовый ящик;

- Изучайте сообщения: грамматические ошибки или необычная структура предложения;

- Подтвердите информацию: если электронное письмо или звонок кажутся подозрительными, отправьте сообщение или позвоните отправителю, чтобы проверить, является ли полученная информация действительной;

- Используйте антивирусное программное обеспечение.

В случае совершения в отношении вас мошеннических действий незамедлительно обращайтесь в правоохранительные органы.

Помощник Усть-Джегутинского

межрайонного прокурора М.А. Гужева