Что такое спуфинг и как предотвратить спуфинг-атаку

Спуфинг (от английского слова spoofing) - это кибер-атака, в рамках которой мошенник выдает себя за какой-либо надежный источник, чтобы получить доступ к важным данным или информации. Такая подмена (спуфинг-атака) может происходить через веб-сайты, электронную почту, телефонные звонки, текстовые сообщения, IP-адреса и серверы.

Как правило, основная цель спуфинга – получить доступ к личной информации, украсть деньги, обойти контроль доступа к сети или распространить вредоносное ПО через ссылки на зараженные веб-страницы или зараженные файлы, вложенные в электронное письмо / сообщение. При любой форме общения в Интернете мошенники будут пытаться использовать спуфинг, чтобы попытаться украсть вашу онлайн-личность и ИТ-активы.

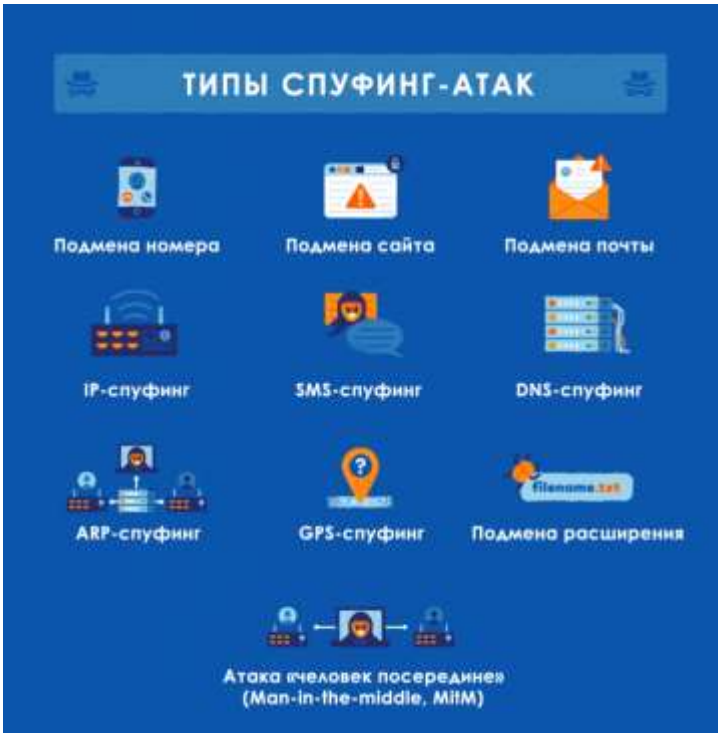
Как происходит спуфинг:

Каждый раз, когда мошенник маскирует себя под другого человека (организацию, сайт, отправитель и пр.), то такой случай – это спуфинг.

Спуфинг может применяться к различным коммуникационным каналам и задействовать различные уровни технических ноу-хау. Мошенники используют методы социальной инженерии, чтобы играть на уязвимых человеческих качествах, таких как жадность, страх и наивность.

Примером такого типа социальной инженерии является случай, когда мошенник полагается на чувство страха жертвы в попытке заполучить от него информацию или деньги. ***Мошенничество с внуками*** - это когда мошенник притворяется членом семьи (внуком) и якобы заявляет жертве (бабушке или дедушке этого внука), что у него неприятности и ему срочно нужны деньги. Мошенники часто нацеливаются в таких ситуациях именно на пожилых людей из-за предвзятого представления о том, что пожилые люди менее технически грамотны.

Типы спуфинг-атак:



Спуфинг может быть реализован в разных формах и типах атак, которых вы должны остерегаться. Вот несколько примеров различных видов спуфинга:

Спуфинг с подменой номера вызывающего абонента (Caller ID Spoofing)

Такой вид спуфинга происходит в тех случаях, когда мошенник использует ложную информацию для изменения идентификатора вызывающего абонента (т.е. мошенник звонит якобы с другого телефона – например, телефон вашего друга). Поскольку спуфинг с подменой идентификатора вызывающего абонента делает невозможной блокировку номера, многие телефонные мошенники используют такой вид спуфинга, чтобы скрыть свой реальный номер телефона, с которого осуществляется данный звонок, чтобы в конечном итоге скрыть свою личность. Иногда мошенники используют ваш код города, чтобы создать впечатление, что звонок местный.

Спуфинг с подменой сайта (Website Spoofing)

Спуфинг с подменой сайта – это тип спуфинг-атаки, в рамках которой мошенник пытается создать опасный (вредоносный) сайт похожим на надежный безопасный сайт. Такие «скопированные» сайты обычно создаются для незаконного получения личной информации посетителя сайта(логина, пароля, данные банковских карт и др.).

Спуфинг с подменой адреса электронной почты (Email Spoofing)

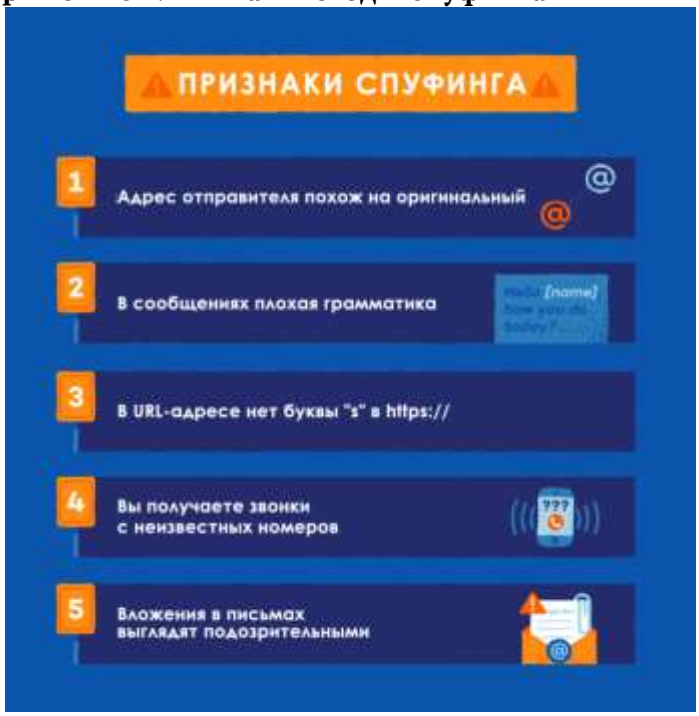
Это тип спуфинг-атаки, в рамках которой мошенник рассылает электронные письма с поддельными адресами отправителей с намерением заразить ваш компьютер вредоносными программами, заполучить деньги или украсть информацию. В качестве адресов электронной почты отправителей зачастую подставляются те адреса, которым вы можете доверять (коллега по работе, друг, родственник, ваш банк и т.д.).

Также в качестве адресов электронной почты отправителей могут подставляться те адреса, которые очень похожи на адреса известных вам отправителей (незаметная разница в букве/цифре).

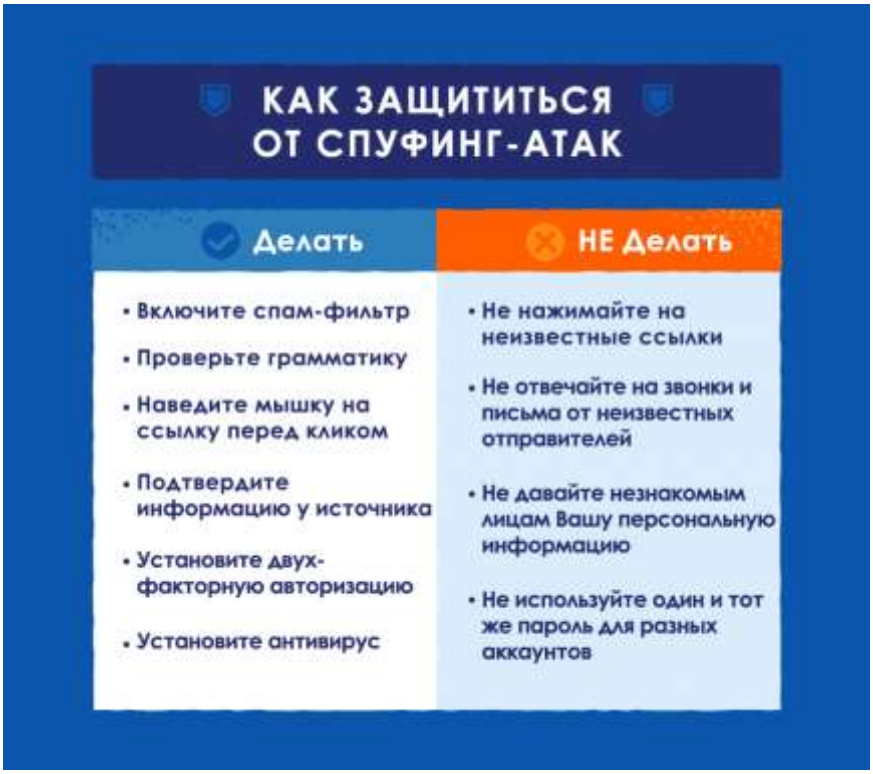
SMS-спуфинг (Text Message Spoofing)

Это тип спуфинг-атаки, в рамках которой мошенник отправляет текстовое или SMS-сообщение, используя номер телефона другого человека. Мошенники делают это, скрывая свою личность за буквенно-цифровым идентификатором отправителя, и обычно в свои сообщения включают ссылки для загрузки вредоносных программ или для перехода на фишинговые сайты.

Как узнать, не применяют ли к вам методы спуфинга.



Как защититься от спуфинг-атак:



Существует ряд рекомендаций, которым вам следует придерживаться, чтобы защитить себя от спуфинг-атак. Оставайтесь на шаг впереди мошенников с нашими полезными советами, что следует делать, а что делать не следует:

Следует делать:

Включите спам-фильтр: это предотвратит попадание большинства поддельных писем в ваш почтовый ящик.

Изучите сообщение: если потенциальная спуфинг-атака содержит признаки плохой грамматики или необычной структуры предложения, это может свидетельствовать о незаконном характере сообщения. Кроме того, не забудьте дважды проверить URL-адрес веб-сайта или адрес отправителя электронной почты.

Подтвердите информацию: если электронное письмо или звонок кажутся подозрительными, отправьте сообщение или отдельно позвоните отправителю, чтобы проверить, является ли полученная вами информация законной или нет. Если письмо или звонок были сделаны якобы от какой-то организации, попробуйте в Интернете найти ее сайт или номер телефона, чтобы проверить эту информацию на сайте или в их колл-центре.

Наведите указатель мыши перед кликом на ссылку: если URL-адрес выглядит подозрительно, наведите курсор мыши на ссылку, чтобы точно увидеть, куда приведет вас ссылка, прежде чем нажать на нее.

Настройте двухфакторную авторизацию: это отличный способ добавить еще один уровень защиты к вашим данным доступа. Однако это не является 100% защитой, а потому убедитесь, что вы также используете и другие меры предосторожности.

Используйте антивирусное ПО: установка программного обеспечения для информационной безопасности – это самая лучшая защита, когда дело доходит до защиты от мошенников в Интернете. Если у вас возникли проблемы, скачайте программу для удаления вредоносных программ или антивирусное программное обеспечение, чтобы защитить ваш компьютер от любых вредоносных угроз или вирусов.

НЕ следует делать:

Не нажимайте на незнакомые ссылки: Если ссылка выглядит подозрительной, воздержитесь от нажатия на нее. Если она пришла от потенциального злоумышленника, то это может привести к загрузке вредоносной программы или других вирусов, которые могут заразить ваш компьютер.

Не отвечайте на электронные письма или звонки от неизвестных отправителей: если отправитель неузнаваем, не отвечайте на звонок или электронное письмо. Это может помочь предотвратить любое общение с потенциальным мошенником.

Не разглашайте личную информацию: избегайте разглашения вашей личной и конфиденциальной информации (например, номер банковской карты, соцстрахования, логины и пароли и т.д.), если вы не уверены, что общаетесь с надежным источником.

Не используйте один и тот же пароль: создайте для всех своих аккаунтов разные и надежные пароли, которые мошенникам будет труднее угадать. Часто меняйте их на случай, если мошенник завладеет одним из них. Кроме того, избегайте использования одного и того же пароля для большинства ваших аккаунтов.

Если вы считаете, что вас обманули, вы можете подать жалобу в центр защиты прав потребителей. Вы также можете обратиться в местное отделение полиции, если потеряли деньги из-за обмана. Также советуем вам использовать антивирусное программное обеспечение, чтобы обезопасить свою цифровую жизнь и защитить себя от обмана и спуфинга.