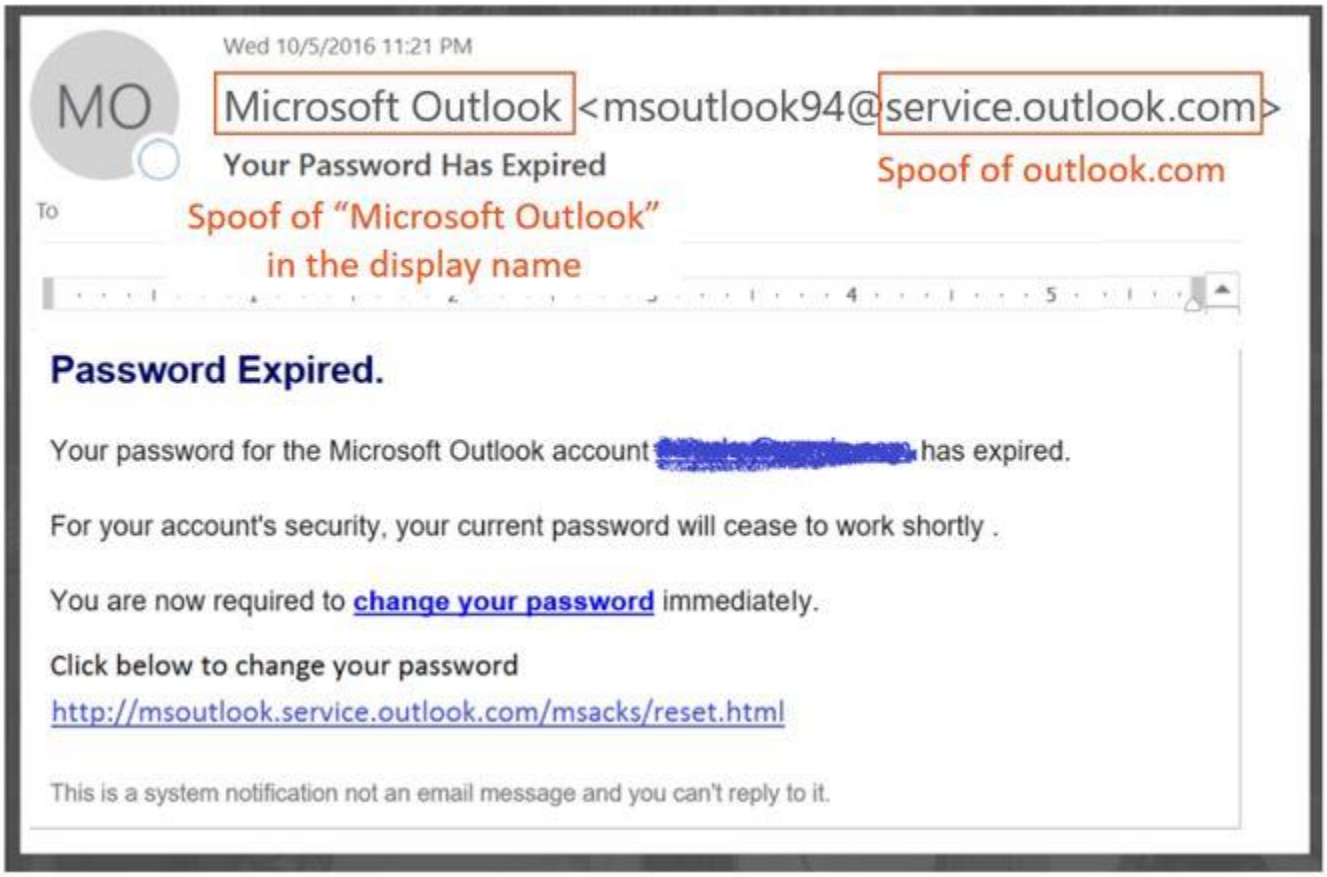
How spoofing is used in phishing attacks

When it comes to protecting its users, Microsoft takes the threat of phishing seriously. One of the techniques that spammers and phishers commonly use is spoofing, which is when the sender is forged, and a message appears to originate from someone or somewhere other than the actual source. This technique is often used in phishing campaigns designed to obtain user credentials. Microsoft's Anti-spoof technology specifically examines forgery of the 'From: header' which is the one that shows up in an email client like Outlook. When Microsoft has high confidence that the From: header is spoofed, it identifies the message as a spoof.

Spoofing messages have two negative implications for real life users:

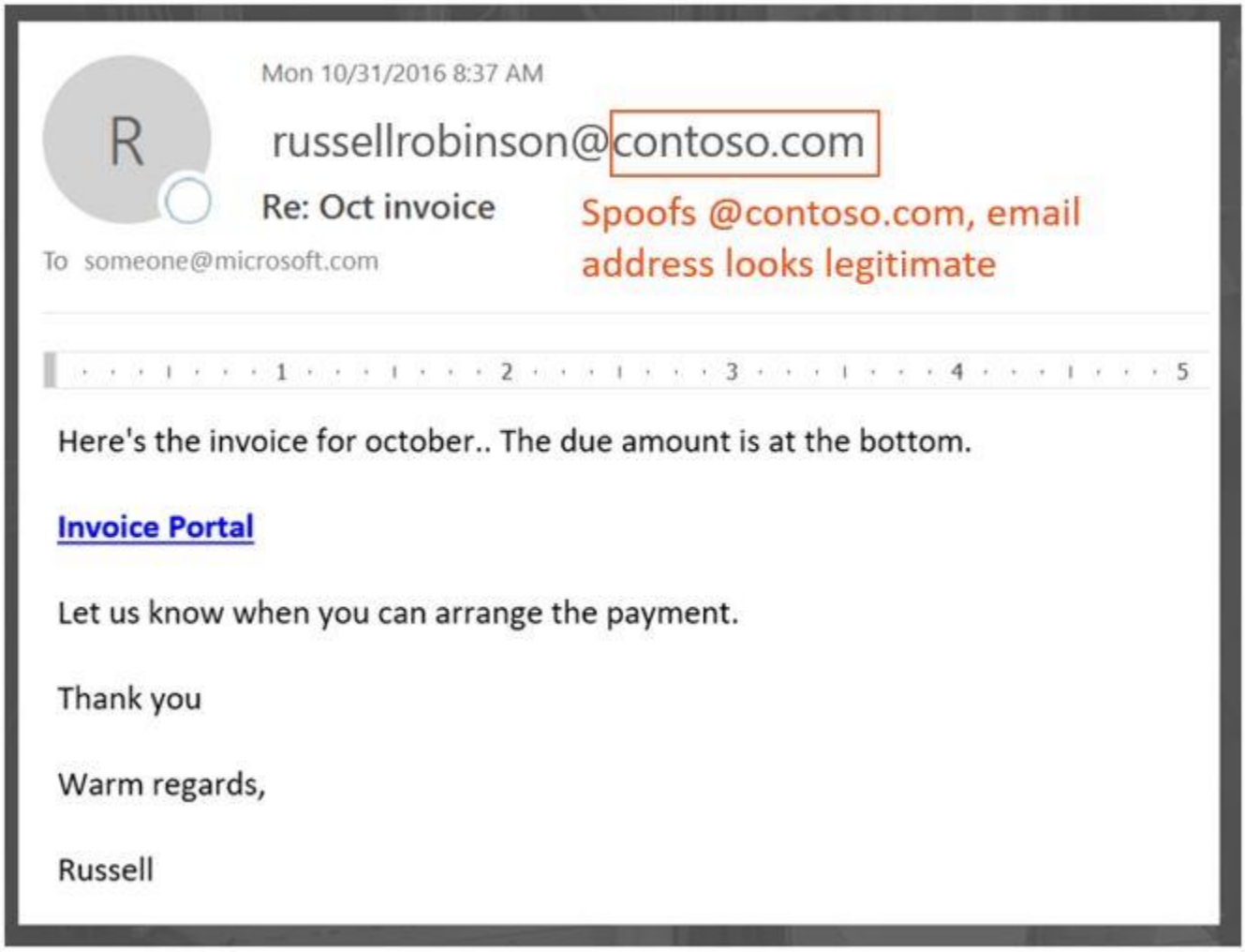
1. Spoofed messages deceive users

First, a spoofed message may trick a user into clicking a link and giving up their credentials, downloading malware, or replying to a message with sensitive content (the latter of which is known as Business Email Compromise). For example, the following is a phishing message with a spoofed sender of msoutlook94@service.outlook.com:



The above did not actually come from service.outlook.com, but instead was spoofed by the phisher to make it look like it did. It is attempting to trick a user into clicking the link within the message.

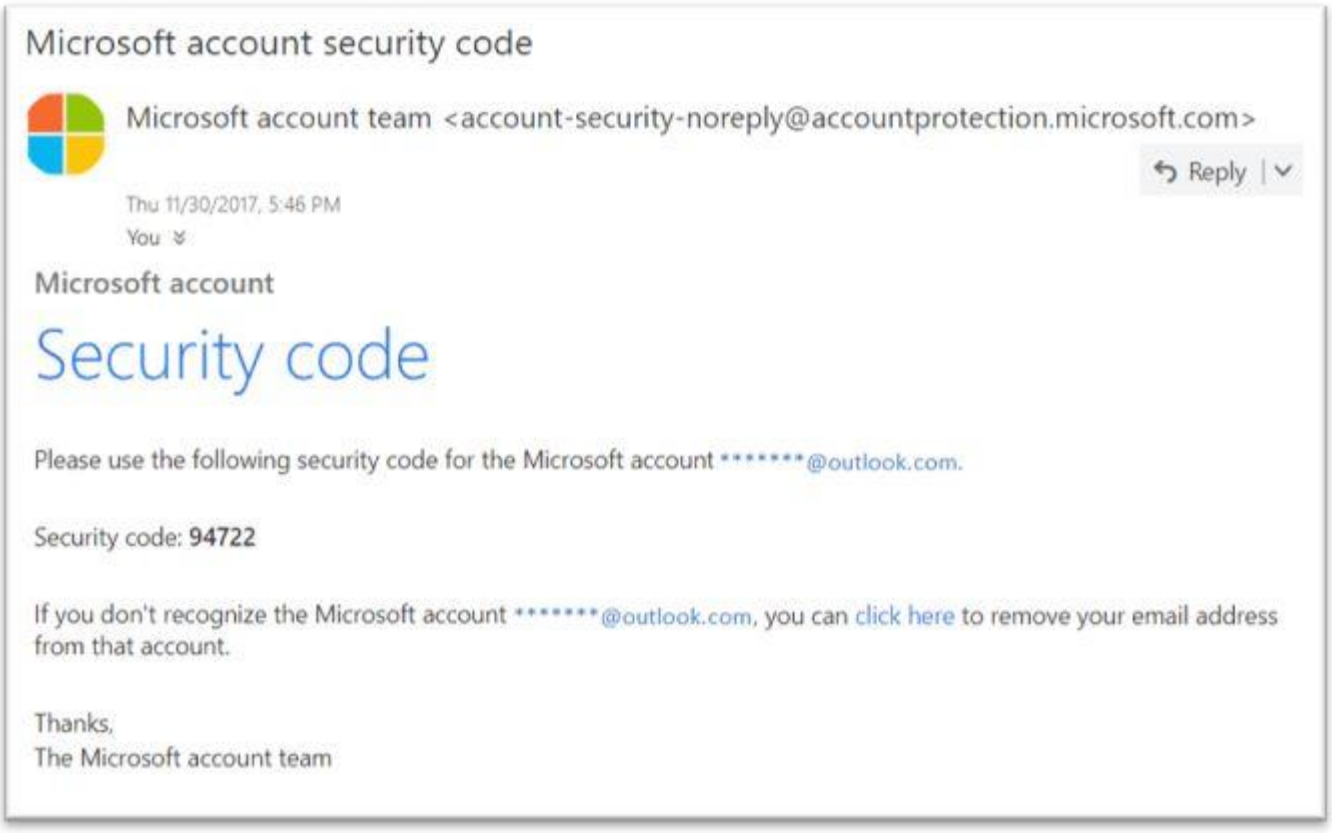
The next example is spoofing contoso.com:



The message looks legitimate, but in fact is a spoof. This phishing message is a type of Business Email Compromise which is a subcategory of phishing.

2. Users confuse real messages for fake ones

Second, spoofed messages create uncertainty for users who know about phishing messages but cannot tell the difference between a real message and spoofed one. For example, the following is an example of an actual password reset from the Microsoft Security account email address:



The above message did come from Microsoft, but at the same time, users are used to getting phishing messages that may trick a user into clicking a link and giving up their credentials, downloading malware, or replying to a message with sensitive content. Because it is difficult to tell the difference between a real password reset and a fake one, many users ignore these messages, report them as spam, or unnecessarily report the messages back to Microsoft as missed phishing scams.