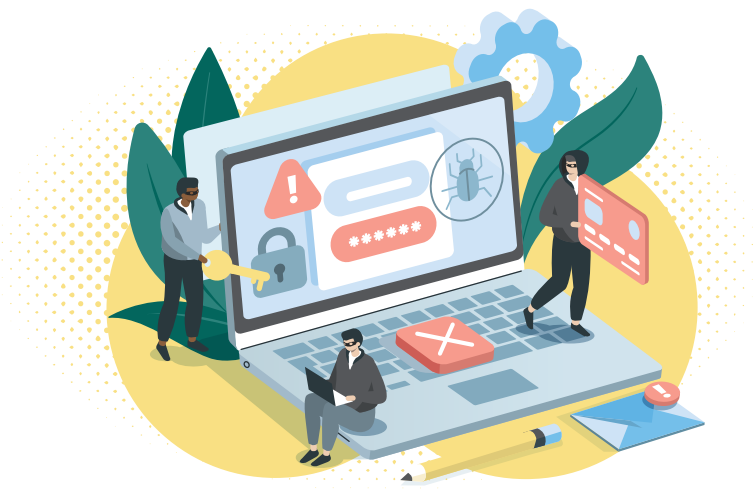
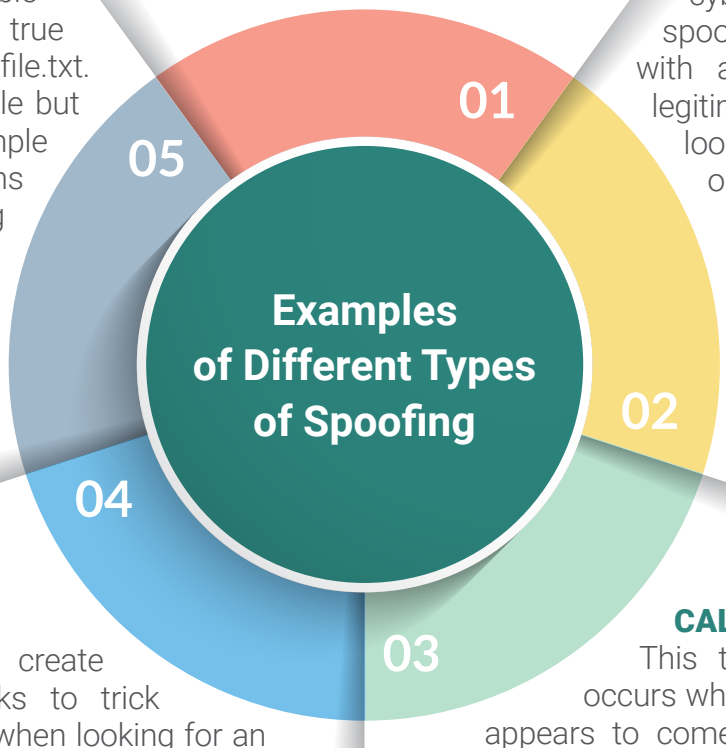
FORTRA

Terranova Security®

What is Spoofing?

Spoofing occurs when a cyber criminal impersonates an individual or an organization to commit malicious acts. The goal of spoofing is to increase the success of social engineering attacks. Email addresses, websites, phone numbers, and more can be spoofed to trick victims into divulging confidential information.





EMAIL SPOOFING

Email spoofing happens when a hacker uses a fake email address to conduct a social engineering attack. Depending on the tactic used, the sender may spoof the email address, sender's name, or both. Cyber criminals can also use email spoofing to assume multiple identities.

FILE EXTENSION SPOOFING

File extension spoofing is when a file has a double extension to hide its true nature. For example, file.txt.exe is an executable file but may appear as a simple text file if file extensions are hidden. Opening such files will run malicious programs on the system.

WEBSITE SPOOFING

A common tactic used in cyber attacks, website spoofing presents victims with a fake site that looks legitimate. Spoofed websites look exactly like the real ones they imitate, using the same logo, branding, colors, layout, domain name, and contact details to fool visitors.

WI-FI SPOOFING

Cyber criminals can create fake wireless networks to trick users into connecting when looking for an open Wi-Fi hotspot. The threats and risks come when users are traveling, working remotely, attending conferences, or commuting.

CALLER ID SPOOFING

This type of spoofing tactic occurs when a fake phone number appears to come from your area code. Since victims are more likely to answer local numbers, cyber criminals use this tactic in social engineering attacks to trick them into answering a call or responding to a text message.

Who is a Spoofing Target?

Any type of business, government, organization, or individual can be the target of a phishing attack. Spoofing is a scammer's way of seeming legitimate by way of an assumed identity. Using fake email addresses, websites, Wi-Fi hotspots, or phone numbers, cyber criminals can trick victims into thinking their requests are legitimate.