FORTRA

How to Protect Your Data from Spoofing Attacks

While scammers use many different spoofing tactics, they're all deployed with the same goal in mind: to obtain sensitive data and use it to fuel malicious acts. Responding to a spoofed email or opening a fake website can lead to data corruption, leaked confidential information, and infected devices or networks. Here's how to avoid becoming a victim of spoofing:

1

MAKE SURE A WEBSITE IS SECURE

Most browsers will display whether or not a site is secure in the address bar. If the padlock or shield icon to the left of the URL is missing, or if the URL starts with http instead of https, the website is not secure and likely spoofed. Verify the spelling of the website URL or use a bookmark.

USE A PASSWORD MANAGER FOR YOUR CREDENTIALS

Many websites will autofill your name and passwords, especially if you've saved your credentials in your browser. To protect against automatic logins, use a password manager to store your credentials. If the password manager doesn't recognize a site, it won't autofill your details.

2

3

EXAMINE THE SENDER'S EMAIL DOMAIN

Beware of email address descriptions that look official. The displayed name of an email address can be faked. Inspect the actual address of the sender containing the "@" sign. The words on the left and the right of the last period in the email address represent the sender's domain.

DON'T CLICK ON SUSPICIOUS LINKS

Even if a message appears to come from a legitimate source, never click on suspicious links. Examine each hyperlinked URL carefully by hovering your mouse over the anchor text and using the text preview in your browser or email window to inspect the website address elements.

4

5

AVOID OPENING UNTRUSTWORTHY EMAIL ATTACHMENTS

Avoid opening email attachments from untrustworthy senders or simply to satisfy your curiosity, especially if a message urges you to do so immediately. Suspicious attachments can be carriers for malware and ransomware payloads that can corrupt your data and harm your device.

BE WARY OF CALLER ID RED FLAGS

Be on the lookout for signs that a caller ID may be spoofed. Common red flags include if a phone number displays without brackets or dashes, if the number is very similar to your own (i.e. – with only one or two digits changed), or if the number or caller's name are hidden.

6

7

AVOID UNSECURED PUBLIC WI-FI

Never connect to open unsecured public Wi-Fi, even if this is the only Wi-Fi available. Providing your email address and accepting the terms and conditions of the Wi-Fi owner does not mean you are connecting to a secure Wi-Fi.