ACROPOLIS INSTITUTE OF TECHNOLOGY AND RESEARCH INDORE

EVALUATION OF INTERNSHIP

EMAIL SPOOFING

Submitted To-Prof. Nidhi Nigam
Submitted by- Kushagra Paliwal

WHAT IS EMAIL SPOOFING?

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. If it's a name they recognize, they're more likely to trust it. So they'll click malicious links, open malware attachments, send sensitive data and even wire corporate funds.

A Brief History of Email Spoofing

Because of the way email protocols work, email spoofing has been an issue since the 1970s. It started with spammers who used it to get around email filters. The issue became more common in the 1990s, then grew into a global cybersecurity issue in the 2000s.

Security protocols were introduced in 2014 to help fight email spoofing and phishing. Because of these protocols, many spoofed email messages are now sent to user spamboxes or are rejected and never sent to the recipient's inboxes.

How to Protect from Email Spoofing

Even with email security in place, some malicious email messages reach user inboxes. Whether you're an employee responsible for financial decisions or as someone who uses personal email at work, there are several steps you can take to avoid becoming a victim of email spoofing:

Never click links to access a website where you're asked to authenticate. Always type the official domain in your browser and authenticate directly on the site.

The steps to view email headers are different for each email client, so first look up how to view email headers for your inbox software. Then, open email headers and look for the Received-SPF section of the headers and look for a PASS or FAIL response.

How to Protect from Email Spoofing

Copy and paste the content of an email message into a search engine. Chances are that text used in a common phishing attack has already been reported and published on the Internet.

Be suspicious of email supposedly from an official source with bad spelling or grammar.

Avoid opening attachments from suspicious or unknown senders.

Emails promising riches—or anything else that's too good to be true—is likely a scam.

Beware of emails that create a sense of urgency or danger. Phishing and BEC attacks often try to short-circuit recipients' natural skepticism by suggesting that something bad will happen if they don't act quickly. Treat email links with extra caution if the message warns of pending account closures, scheduled payment failures or suspicious activity on one of your financial accounts. Visit the website directly through your browser, not the link in the email.


THANK
YOU