

WHAT IS "SPOOFING"?

"Spoofing" (also called "phishing") occurs when thieves send an email that appears to have been sent from the domain of a legitimate retailer, bank, credit card or insurance agency. In recent months, fraudsters have spoofed customers of Citibank, Best Buy, Earth link, eBay, PayPal and even the Federal Deposit Insurance Corporation (FDIC).

HOW DO THEY GET MY PERSONAL INFORMATION OR STEAL MY IDENTITY?

Thieves send millions of emails to internet users that ask them to update their account information for banks, credit cards, online payment services or popular shopping sites. Frequently, the email claims that the recipient's account information has expired or has been lost and the account holder needs to immediately resend it to the company.

SO HOW CAN YOU TELL IF AN EMAIL IS A SPOOF? THOUGH IT IS DIFFICULT TO DETECT FRAUDULENT EMAILS, THERE ARE CERTAIN CHARACTERISTICS THAT INTERNET USERS SHOULD LOOK FOR THAT ARE COMMON TO MANY SPOOF EMAILS:

• Request for Personal Information

Be careful of any email that asks for personal information such as user ID, password or bank account numbers or Social Security Numbers.

• Sender's Address

Don't rely on the sender's email address to validate the true origin of the email; it may look legitimate, but fraudsters can easily alter the "from" field of an e-mail message.

• Greeting

Many spoof emails begin with a general greeting such as "Welcome User," rather than a specific, personalized greeting.

• Threats to account

Many spoofs declare that a recipient's account is in jeopardy and only by authenticating information can an account be kept from being closed, suspended or restricted.

• Lost information

Consumers should be wary of claims that a company is updating its files or accounts. Legitimate companies with established business practices and strong security measures are not likely to lose account information.

• Links

Links that look like they connect to a particular site may have been forged. Always open up a new browser window and manually type in the website address.

HOW CAN YOU AVOID BECOMING A VICTIM OF SPOOFING? KEEP THESE TIPS IN MIND:

- Be extremely skeptical of emails received from someone you don't know
- Keep separate passwords for each online account
- Never click on a link embedded within any potentially suspicious email
- Call your financial institutions to verify account status before divulging any information
- Never respond to any request for personal information that comes to you via email.
- Update anti-virus software weekly
- Work from the most current versions of web browsers
- Check your online accounts regularly
- Install and run firewalls.