United States Secret Service Cybercrime Investigations

Cyber Security Basics
Spoofed Emails

A spoofed email is an email disguised to appear as an email from a trusted source, such as a bank or a company, in order to deceive the recipient into providing personal information or clicking on a malicious link. Spoofed emails can be difficult to detect as they often appear legitimate, they may even include the actual logo and other design features of the organization being impersonated. Cyber criminals commonly use spoofed emails in phishing attacks to steal sensitive information or install malware.

How to Identify Spoofed Emails

Check the sender's email address.

- ✓ There are various methods to spoof emails, including imitating the "From" address, using a look-alike domain name, or using a compromised (stolen) email account.
- ✓ Be wary of emails from unfamiliar email addresses or email addresses that look slightly different from legitimate ones.

Look for poor grammar or spelling errors.

- ✓ Legitimate companies typically have professional communications, so poor grammar or spelling errors could be a red flag.

Check the content of the email.

- ✓ Legitimate emails usually have a specific purpose, so be cautious of emails that ask you to provide personal information, click on a suspicious link, or download a file.

Verify the sender's identity.

- ✓ If you receive an email from an organization, verify the sender's identity by calling them or visiting their official website.

How to Determine if a Domain is Legitimate

Check the domain name carefully.

- ✓ Legitimate email domains typically match the domain (website) name of the organization.
- ✓ Hover your mouse over any links in the email to see the actual URL before clicking on it.
- ✓ Verify email domains through an Internet search.

Look for the secure HTTPS connection.

- ✓ Most legitimate organizations have secure HTTPS connections to their website, which is indicated by a lock icon 🔒 in the address bar.

Use email authentication protocols.

- ✓ Organizations can use email authentication protocols, such as DKIM, SPF, and DMARC, to verify the authenticity of their emails. These protocols help verify that the emails came from the legitimate domain.

Spoofing and Phishing

Don't fall for it.

- ✓ Cyber criminals impersonate banks, social media platforms, e-commerce websites, or even government agencies in their spoofed emails.
- ✓ Once the recipient clicks on a link or responds to the spoofed email, they can unintentionally download malware, or share sensitive information, such as login credentials or credit card numbers, with the cyber criminal.