13.3.2 Email Security Facts

This lesson covers the following topics:

- Email threats
- Email security

Email Threats

To secure email, you must be aware of the following email attacks.

Attack	Description
Virus	A virus is malware that often uses email as its distribution mechanism. Users receive the virus as an attachment and then activate the virus by clicking on that attachment. To mitigate viruses, you should install antivirus software on every system, and install antivirus software on the email server to scan attachments. A best practice is to detect viruses and messages on the email server before it gets to the client and send warnings to the recipient about the malicious email.
Spam	Spam is unwanted and unsolicited email sent to many recipients. Spam consists of the following attributes: - Can be as benign as emails trying to sell products - Can be malicious and contain phishing content, drive-by downloads, or malware - Can contain malware as attachments - Wastes bandwidth and could fill the inbox, resulting in a denial-of-service condition To control spam: - Enable spam filters on the client and email servers. Filter junk email by identifying safe senders (whitelists), blocked senders (blacklists), countries to block email from, and languages to block. - Enable antivirus scanning for attachments on the client and email servers. - In the email client, disable preview screens. An email can have links for active items that can report back to the spammer. - Don't click on an unsubscribe link at the bottom of an unsolicited email. Doing this verifies to the spammer that the email address is a current and active email address. Only unsubscribe from trusted organizations. - Install server-level anti-spam software on the email server. - Don't post your full email address anywhere on the web. Spammers use software to scan websites to find email addresses and then add them to their email lists for spamming.
Open SMTP relay	An SMTP relay is an email server that accepts mail and forwards it to other mail servers. An open SMTP relay allows anyone to forward mail. - If your mail server is an open SMTP relay, it can be used by spammers to send mail. Spammers use your relay to obscure the actual source of the email. - A repudiation attack is an attack on open relays in which the attacker accesses your email server and sends spoofed emails to others, making them appear as if they came from you. - If spammers use your relay for sending mail, your server will soon be placed on a blacklist. Other mail servers then stop receiving any mail (even legitimate mail) sent from your servers. - As a best practice:

	▪ Configure your mail server to accept mail only from authenticated users or specific email servers that you authorize. ▪ Require TLS encryption to connect to the server. ▪ Implement restrictions for accessing the server and relaying email for your environment if feasible.
Phishing	A phishing email is an email pretending to be from a trusted organization that asks to verify personal information or send money. In a phishing attack: ▪ A fraudulent message (that appears to be legitimate) is sent to a target. ▪ The message requests that the target visit a fraudulent website (which also appears to be legitimate). Graphics, links, and web pages look almost identical to the legitimate requests and websites the attacker tries to represent. ▪ The fraudulent website requests that the victim provide sensitive information, such as the account number and password. To protect against phishing: ▪ Check the email header information to see more info about the sender and the links that are in the email. ▪ Only open emails if you recognize the sender. ▪ Check the actual link destination within emails to verify that they go to the correct URL and not a spoofed one. ▪ Do not click on links in emails. Instead, type the real URL into the browser. You could also look up the website in a search engine. ▪ Verify that HTTPS is used when going to e-commerce sites. HTTPS requires a certificate that matches the server name in the URL that is verified by a trusted CA. You can also look for the lock icon to verify that HTTPS is used. ▪ Implement phishing protections within your browser.

Email Security

Email is cleartext by default. To secure email, use either Secure/Multipurpose Internet Mail Extensions (S/MIME) or Pretty Good Privacy (PGP).

- Both solutions use certificates to provide authentication, message integrity, non-repudiation (through digital signatures), and privacy (encryption).
- Certificates are bound (associated) with an email address.
- To prove who has sent an email, a digital signature is added to it using the sender's private key. Only the sender who has the private key could have sent the message.
- To encrypt email, the message is encrypted using the recipient's public key. Only the recipient who has the private key can decrypt the message. Before you send an encrypted email to someone, you must first obtain their public key, which is normally done by having them send you a signed email.
- S/MIME uses certificates issued by either public or in-house CAs using the X.509 system.
- PGP uses two methods for validating certificates:
  - With a web of trust, individual users decide which certificates they trust. Users can then trust other designated users to introduce or recommend additional trusted users.
  - With trust signatures, digital signatures from certain certificates are trusted as being able to sign other keys. Trust signatures create a hierarchy similar to that of Certificate Authorities.
- Both S/MIME and PGP are used primarily for email encryption, although PGP can also be used for encryption of phone calls and whole disk encryption.