



Email Security

Cybersecurity Awareness

Securing Email



Email

- Most common technology used for social engineering attacks.
- Everyone uses email.
- Criminals use hacked computers to send out millions of emails every day (spam).



Why Secure Email?

- Protect data
- Maintain authenticity of sender and the recipient
- Avoid junk emails



Email Threats

Phishing

**Social
Engineering**

**Malicious
Attachments**

Spam

Malicious Links

Email Flooding



Spam- What is it?

- Spam is an electronic Junk Mail.
- Do not reply to spam messages.
- Spam is used to distribute viruses and other malicious code.
- Spam is also used for advertising products through mailing lists or newsgroups.

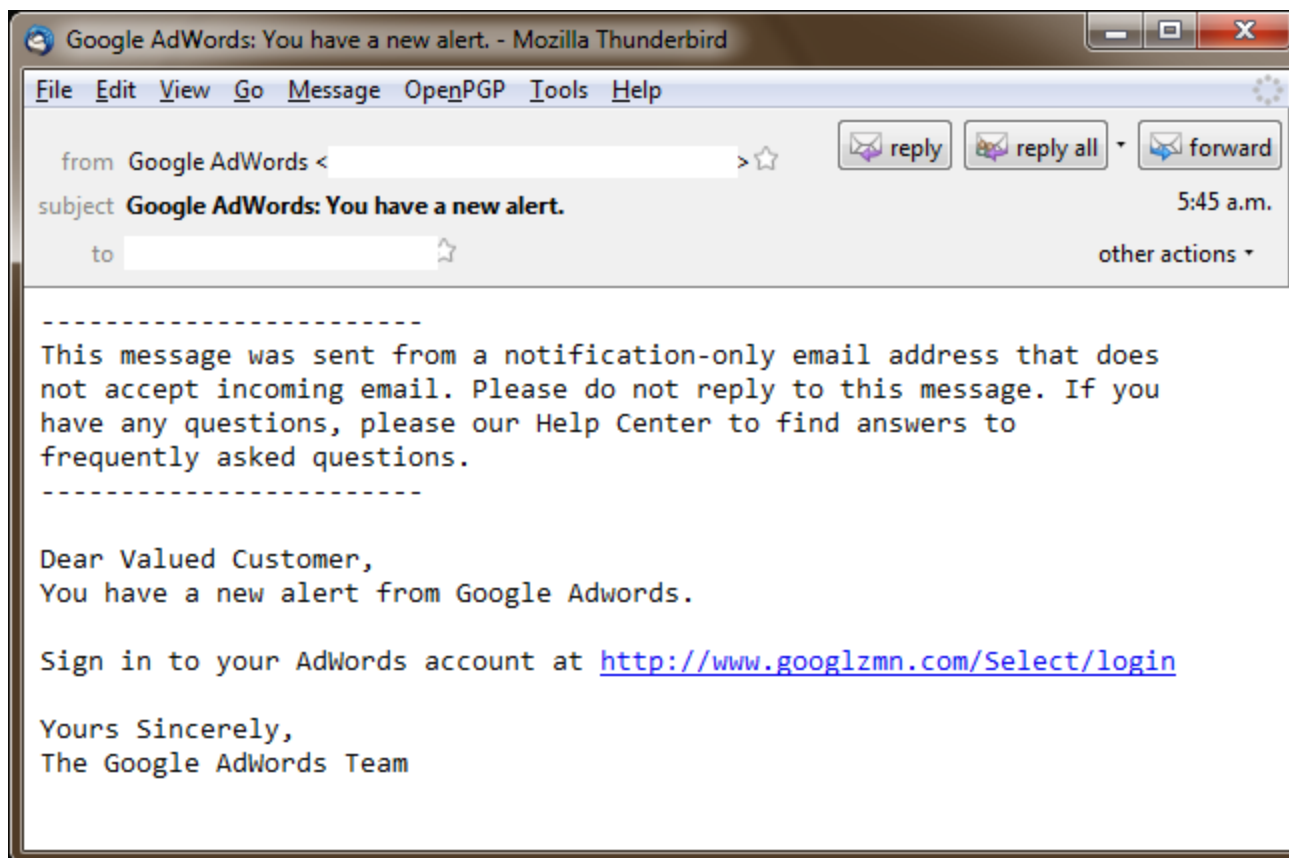


Spam

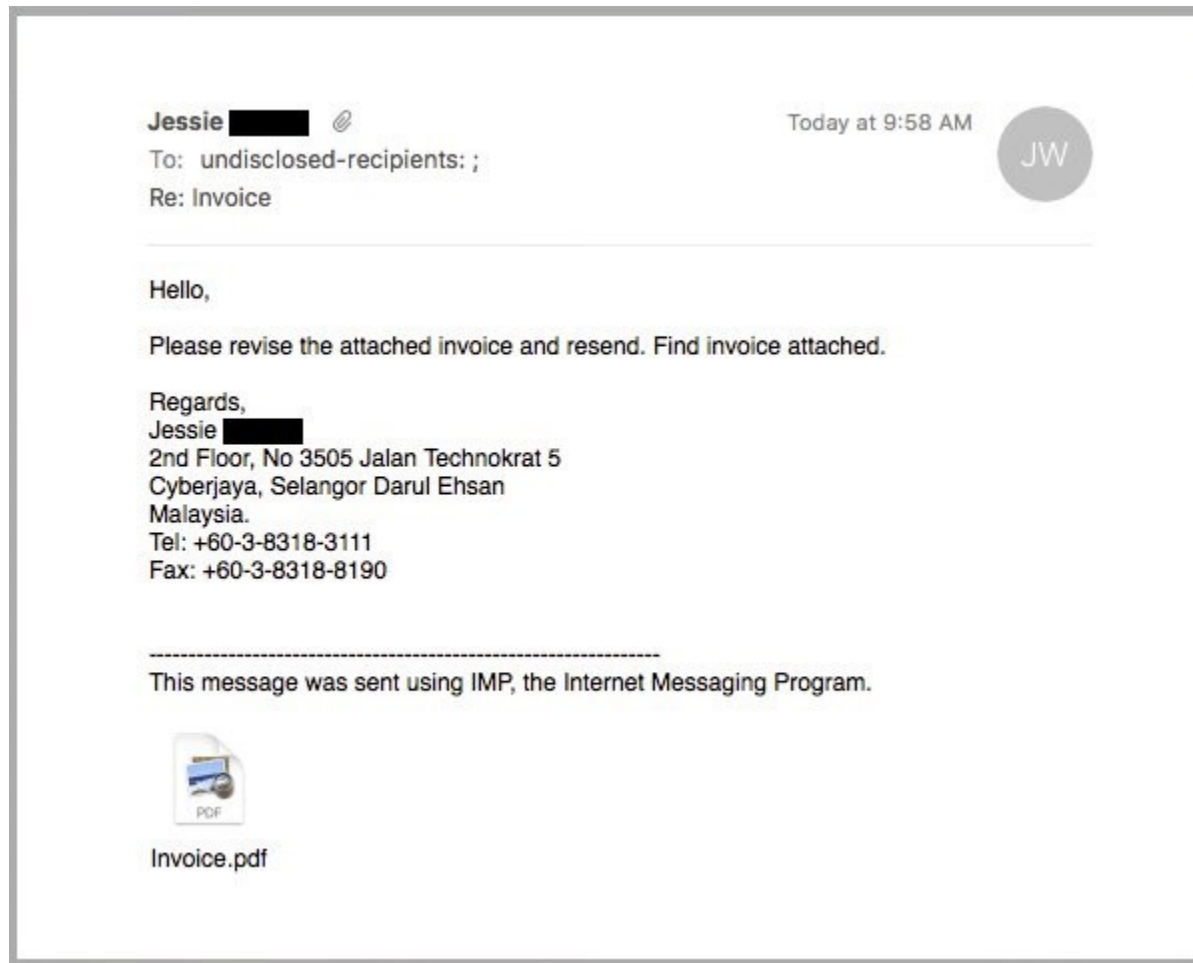
- Spam consumes a lot of network bandwidth.
- Spam emails can not be prevented unless the online service provider institutes a policy that prevents spammers from spamming their subscribers.



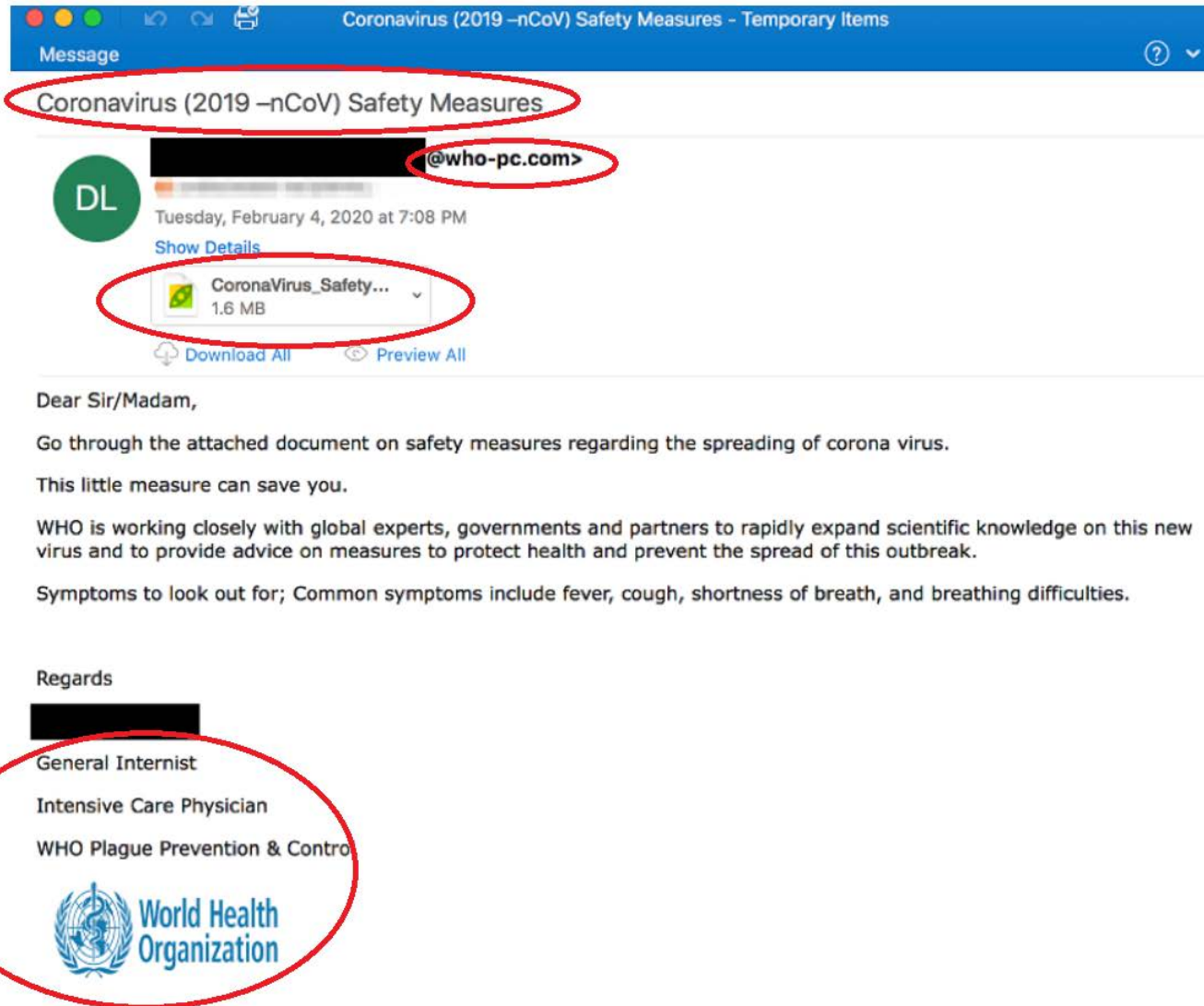
Spam



Spam




Infected By Email



Infected By Email

From: sec@sycamorepd.com
Subject: Mail server report.
Date: July 22, 2013 4:23:55 CDT
To: victim@example.com

►  1 Attachment, 18.6 KB Save ▾ Quick Look

Do not reply to this message

Dear Customer,

Our robot has fixed an abnormal activity from your IP address on sending e-mails. Probably it is connected with the last epidemic of a worm which does not have patches at the moment. We recommend you to install a firewall module and it will stop e-mail sending. Otherwise your account will be blocked until you do not eliminate malfunction.

Customer support center robot



[Update-KB2....zip \(18.6 KB\)](#)

Email Security

Everyone uses email

- Register your personal Email on selected and trusted websites only to avoid spam.
- Never reply to spam.
- Scan Email attachments before opening them.
- Prevent forwarding unnecessary chain emails.

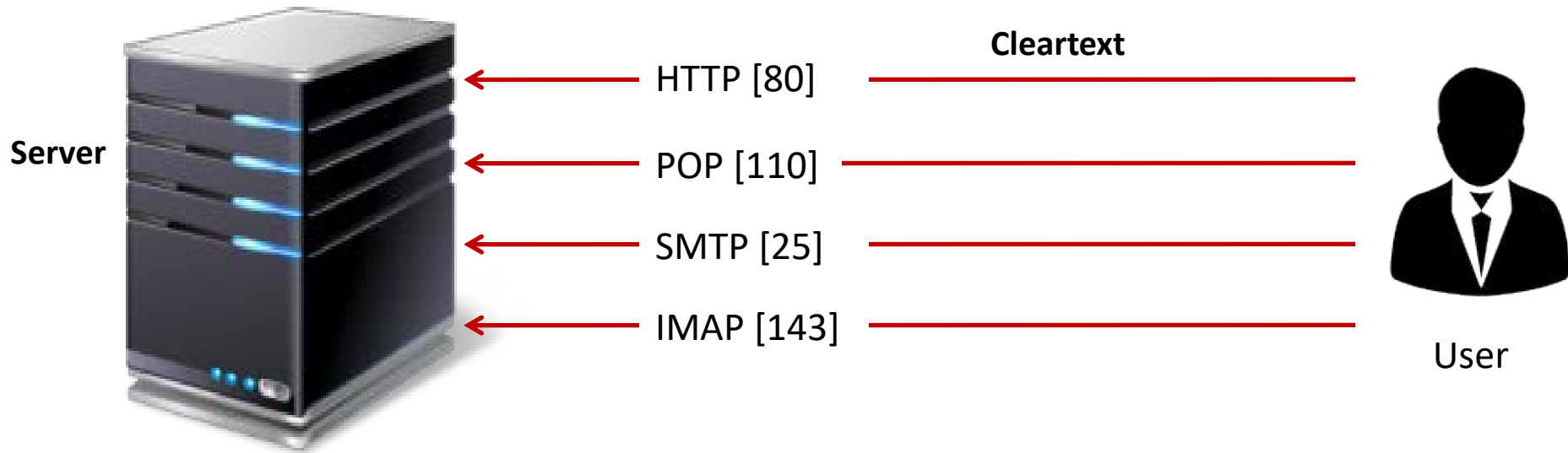


Malicious Attachments

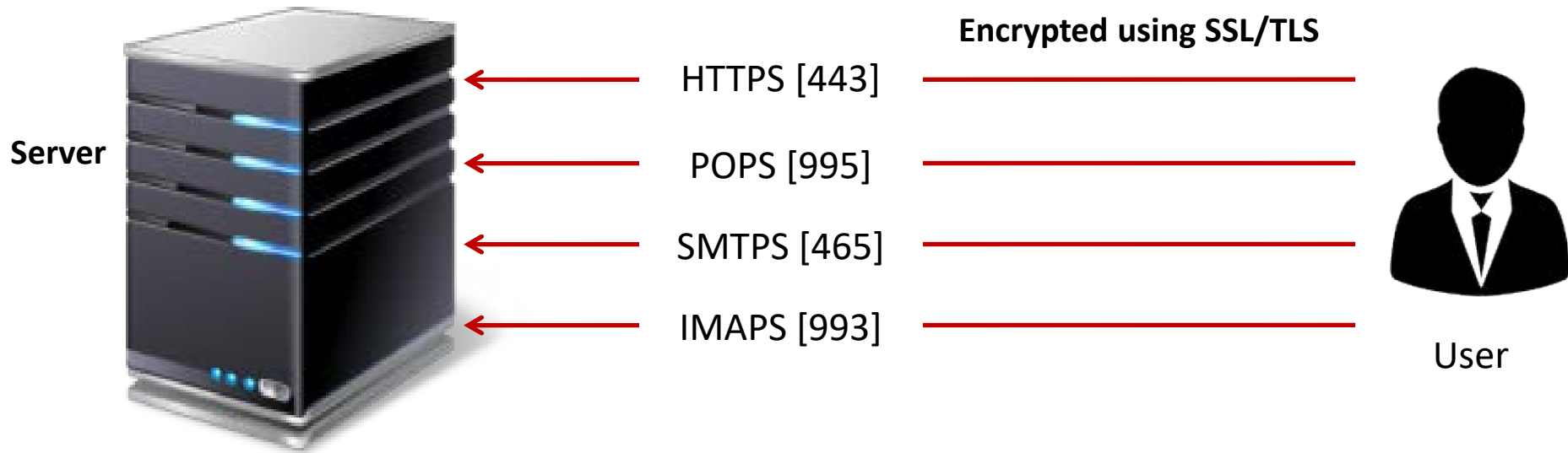
- Check the sender
- Check file names
- Be aware of ZIPs and RARs
- Be aware of office documents
- Never open EXEs



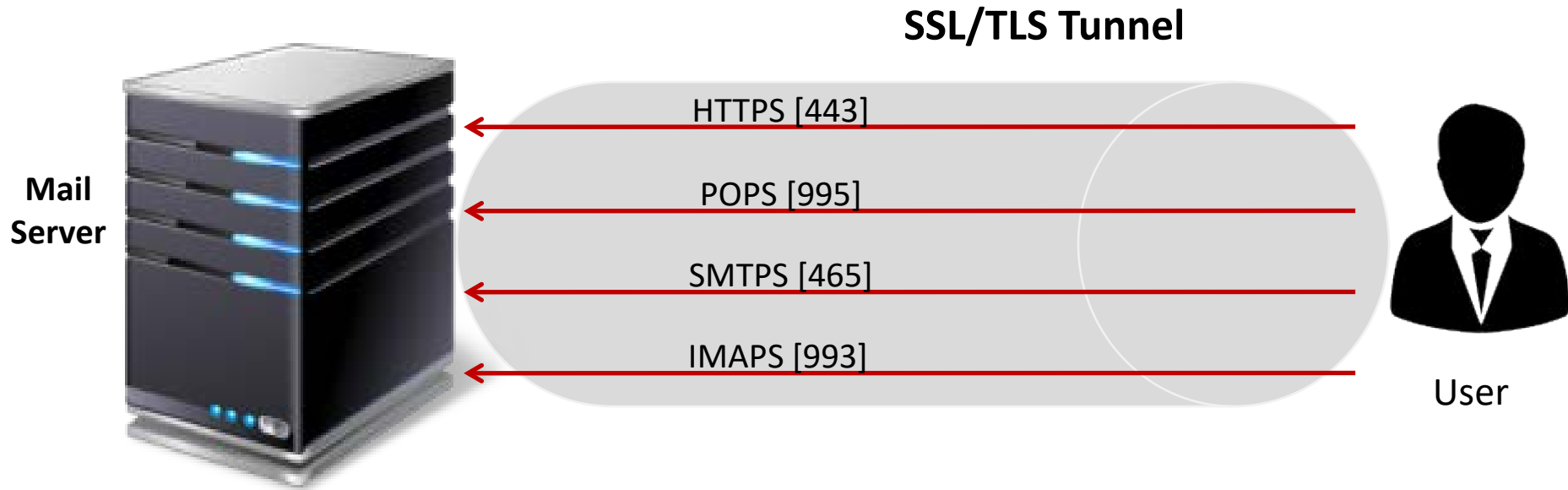
Email Protocols - Cleartext



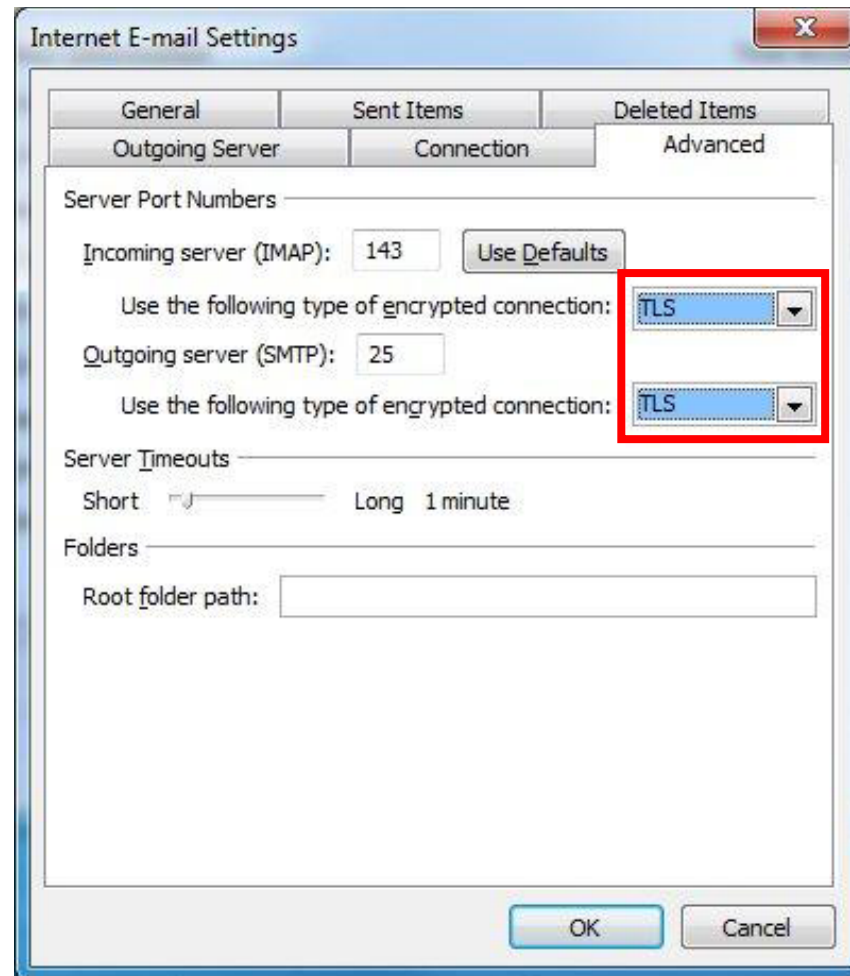
Email Protocols - Encrypted



Secure Email Communication



Secure Email Communication






Encrypt Attachments


Email Security.pptx - Saving...

Info

Email Security


Ebdaa » Shared Documents » Projects » Awareness » aeCERT » 2020 » OIC Presentations » Awareness material » 6

 Share  Copy path  Open file location



Protect Presentation ▾

Control what types of changes people can make to this presentation.




Check for Issues ▾

Inspect Presentation

Before publishing this file, be aware that it contains:

- Document properties, document server properties, content type information, author's name and cropped out image data
- Presentation notes
- Custom XML data
- Embedded documents
- Revision tracking data
- Content that people with disabilities are unable to read



Version History

View and restore previous versions.

← Home New Open

Info Save a Copy Print Share Export Close

Account Feedback Options

Encrypt Attachments

The screenshot shows the Microsoft PowerPoint interface. On the left is a dark red sidebar with navigation options: Home, New, Open, Info (selected), Save a Copy, Print, Share, Export, Close, Account, Feedback, and Options. The main area is titled 'Email Security.pptx' and shows the 'Info' tab. Below the title bar, there are buttons for 'Share', 'Copy path', and 'Open file location'. The 'Protect Presentation' menu is open, displaying five options: 'Always Open Read-Only', 'Encrypt with Password' (highlighted with a blue selection bar), 'Restrict Access', 'Add a Digital Signature', and 'Mark as Final'. Each option includes an icon and a brief description of its function.

Email Security.pptx - Saving...

Info

Email Security

Ebdaa » Shared Documents » Projects » Awareness » aeCERT » 2020 » OIC Presentations » Awareness material » 6 Em

Share Copy path Open file location

Protect Presentation

Control what types of changes people can make to this presentation.

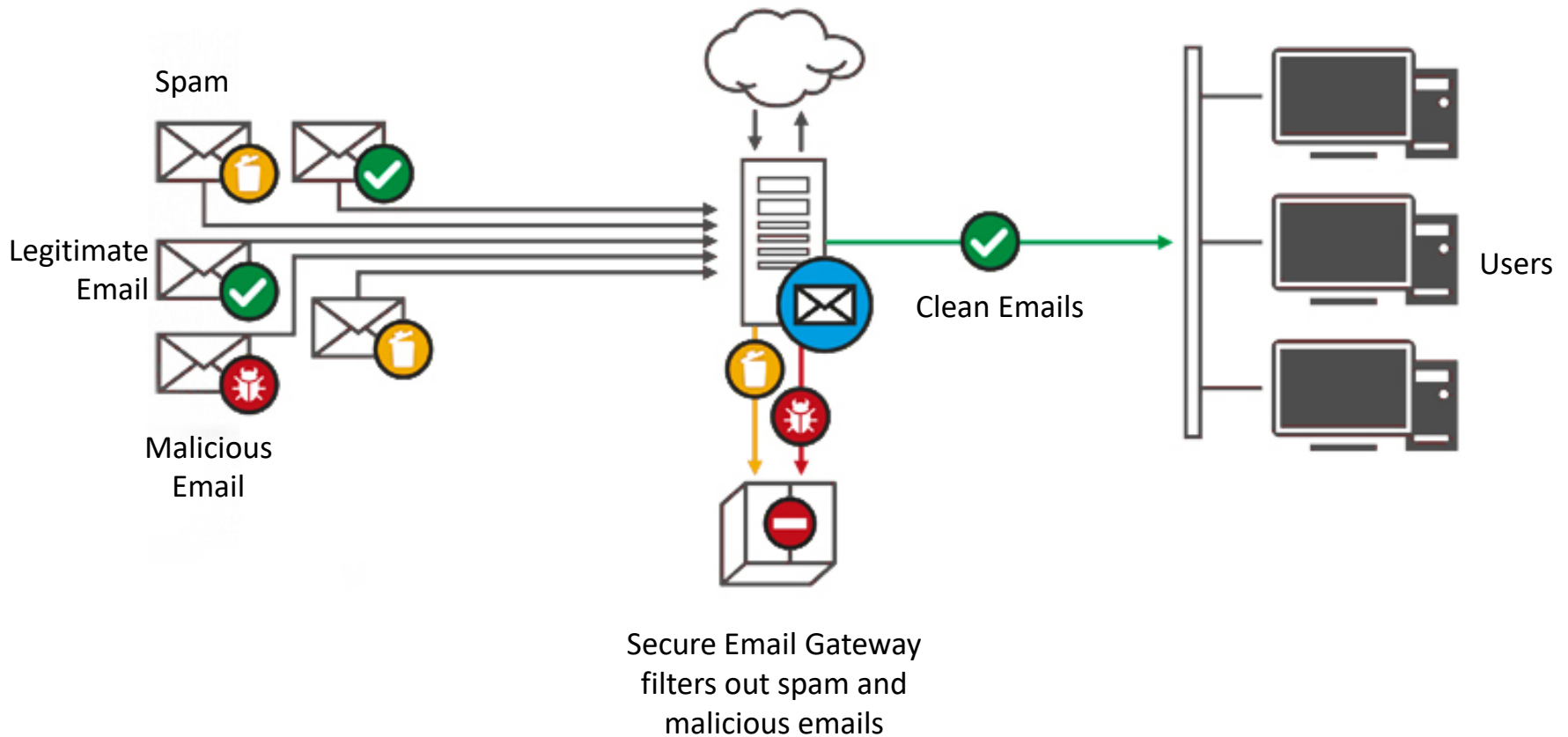
- Always Open Read-Only**
Prevent accidental changes by asking readers to opt-in to editing.
- Encrypt with Password**
Require a password to open this presentation.
- Restrict Access**
Grant people access while removing their ability to edit, copy, or print.
- Add a Digital Signature**
Ensure the integrity of the presentation by adding an invisible digital signature.
- Mark as Final**
Let readers know the presentation is final.

Email Security Solutions

- Antivirus
- Anti-spam
- Secure Email Gateway
- Email Firewall
- Email Archiving
- Phishing Protection
- Cloud-based Email Security



Secure Email Gateway



Phishing

- Initially the purpose was to launch email attack to obtain online banking username and password.
- Phishing has evolved into an attack where an attacker pretends to be someone you trust.



Phishing

- They then exploit that trust to get what they want such as your identity and bank account.
- User is usually directed to a website that looks similar to a popular site but is actually an illegitimate website.
- The user is asked to fill in personal information such as username/password of online banking, credit card information, social networking credentials, etc.



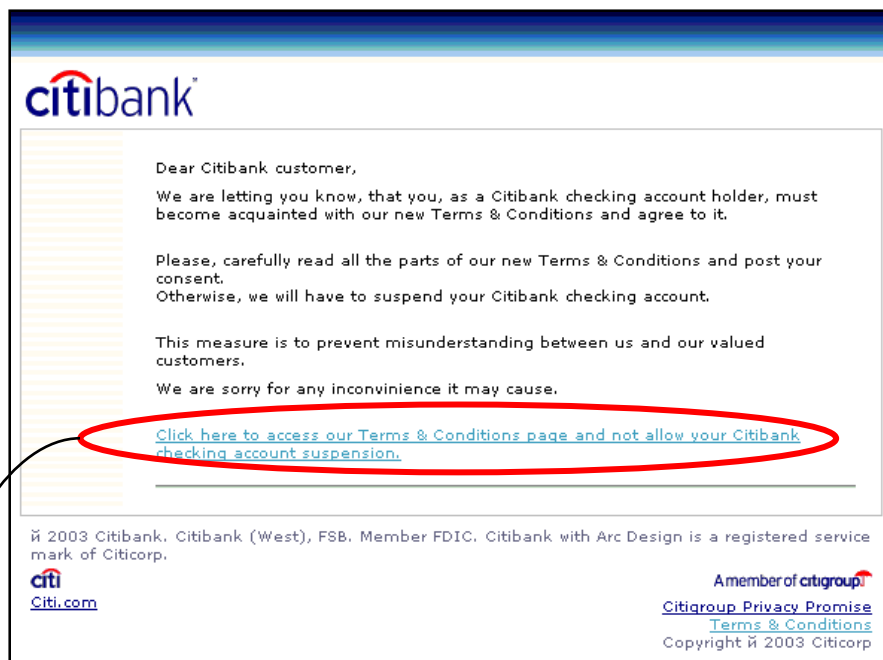
Phishing Email

- Phishing is not anything new and many of you may have seen examples in emails from your personal / at-home email accounts.

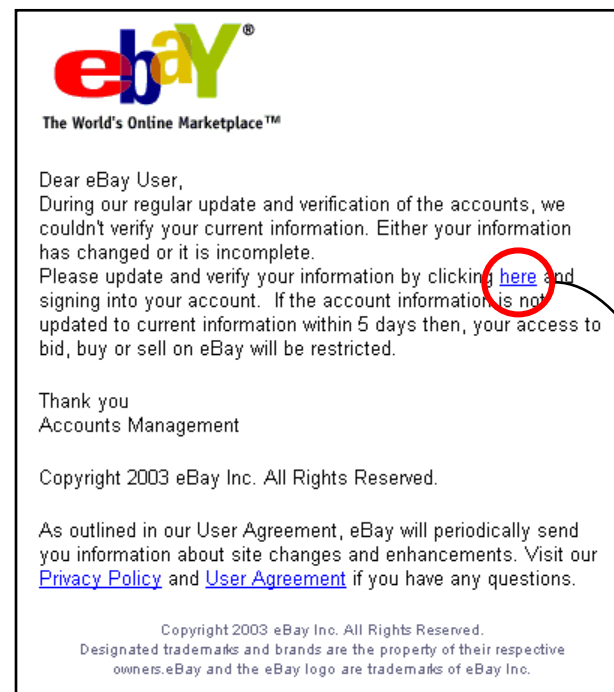


- You may have seen emails that appear to come from your bank or other online financial institutions.
- Commonly Seen Commercial Examples:
 - ❖ eBay, PayPal, all banking and financial institutions

Example of Phishing Email



[www.c1t1bank.com:ac%398HAAA9UWDTYAZJWVWAAA
A9pYWwgc2l6ZT00PjxTVgc2l6ZT00PjxT3Aac%398HAAA9
UWDTYAZJWVWAAA9pYWwgc2l6ZT00PjxTVgc2l6ZT00
PjxT@211.155.234.84](http://www.c1t1bank.com:ac%398HAAA9UWDTYAZJWVWAAA
A9pYWwgc2l6ZT00PjxTVgc2l6ZT00PjxT3Aac%398HAAA9
UWDTYAZJWVWAAA9pYWwgc2l6ZT00PjxTVgc2l6ZT00
PjxT@211.155.234.84)



<http://205.214.89.85/ebay.html>

Identifying Phishing Email

Hello

As part of our security procedures, we closely monitor activities being performed in the Facebook system.

We recently discovered unusual Copyright activity linking to your account. We regret to inform you that your account has been suspended due to this activity. In order to re-activate your account, kindly verify using following link:

www.faceb00k.com/re_activate

Note: If you do not re-activate your account, your account will be permanently blocked.

Regards,

Facebook Copyrights Team.

Spelling

External links

Threat

**Popular
Company Name**

Phishing Website

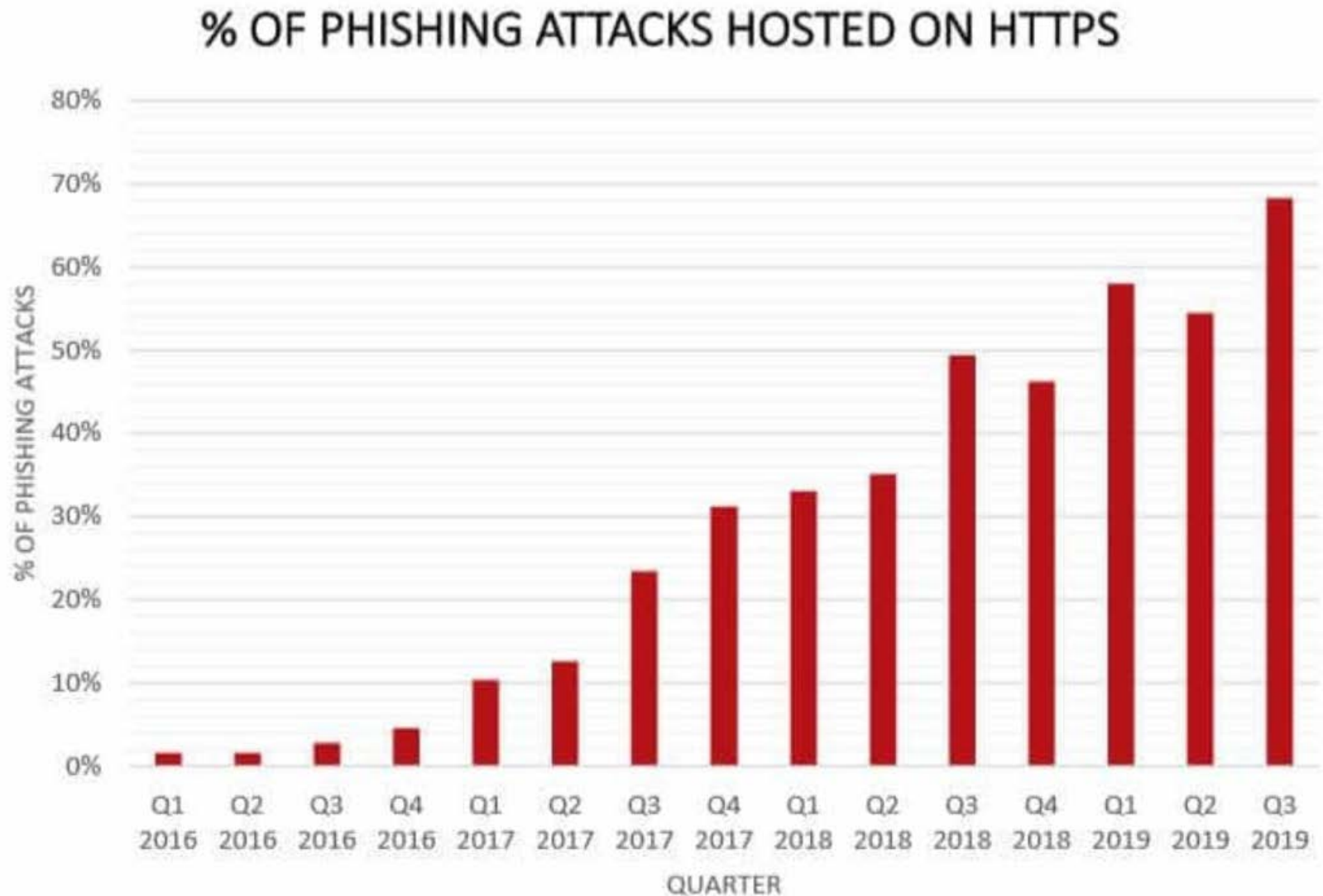


Fake Facebook URL:

A screenshot of a fake Facebook login form. At the top, it says 'Facebook Login'. Below that is a yellow warning box with the text 'You must log in to see this page.' The form includes fields for 'Email address:' and 'Password:'. There is a checkbox for 'Keep me logged in' and a blue 'Log in' button. To the right of the button is a link that says 'or Sign up for Facebook'. Below the button is a link that says 'Forgotten your password?'. At the bottom, there is a row of language links: 'English (US)', 'Español', 'Português (Brasil)', 'Français (France)', 'Deutsch', 'Italiano', 'العربية', '日本語', and '中文(香港)'. Below these links is a small link that says '日本語 *'.

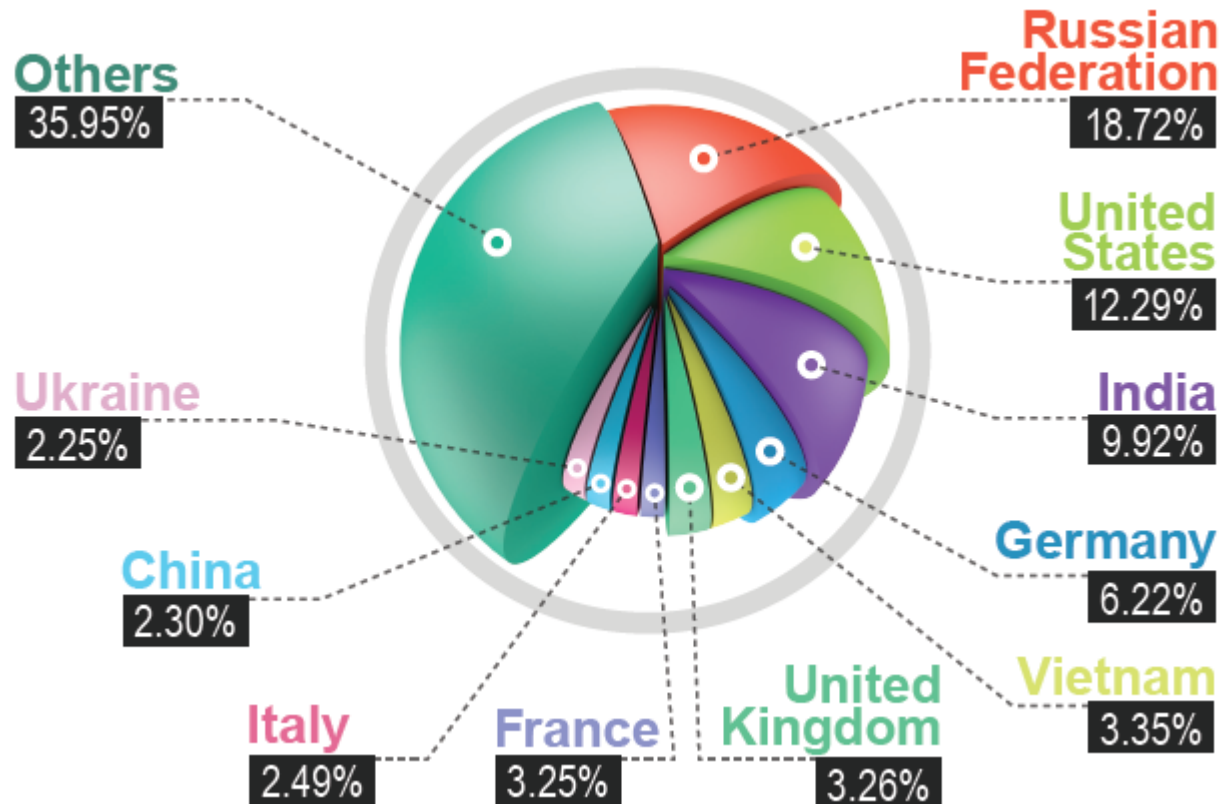
Fake website designed to harvest your login and password.

Worldwide Phishing Attacks



<https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/>

Top 10 Phishing Target Countries



Email Security

- Limit the size of email to prevent wastage of bandwidth.
- Avoid sending sensitive information over email but in case its necessary, use encryption.
- Use digital signature which is a digital code that verifies the authenticity of the email sender.



Secure Email Practices

- Use encryption and digital signatures
- Configure secure email software
- Use complex passwords for your email
- Never share your email password
- Use secure email standards such as S/MIME and OpenPGP
- Always log out of email websites when you are done emailing

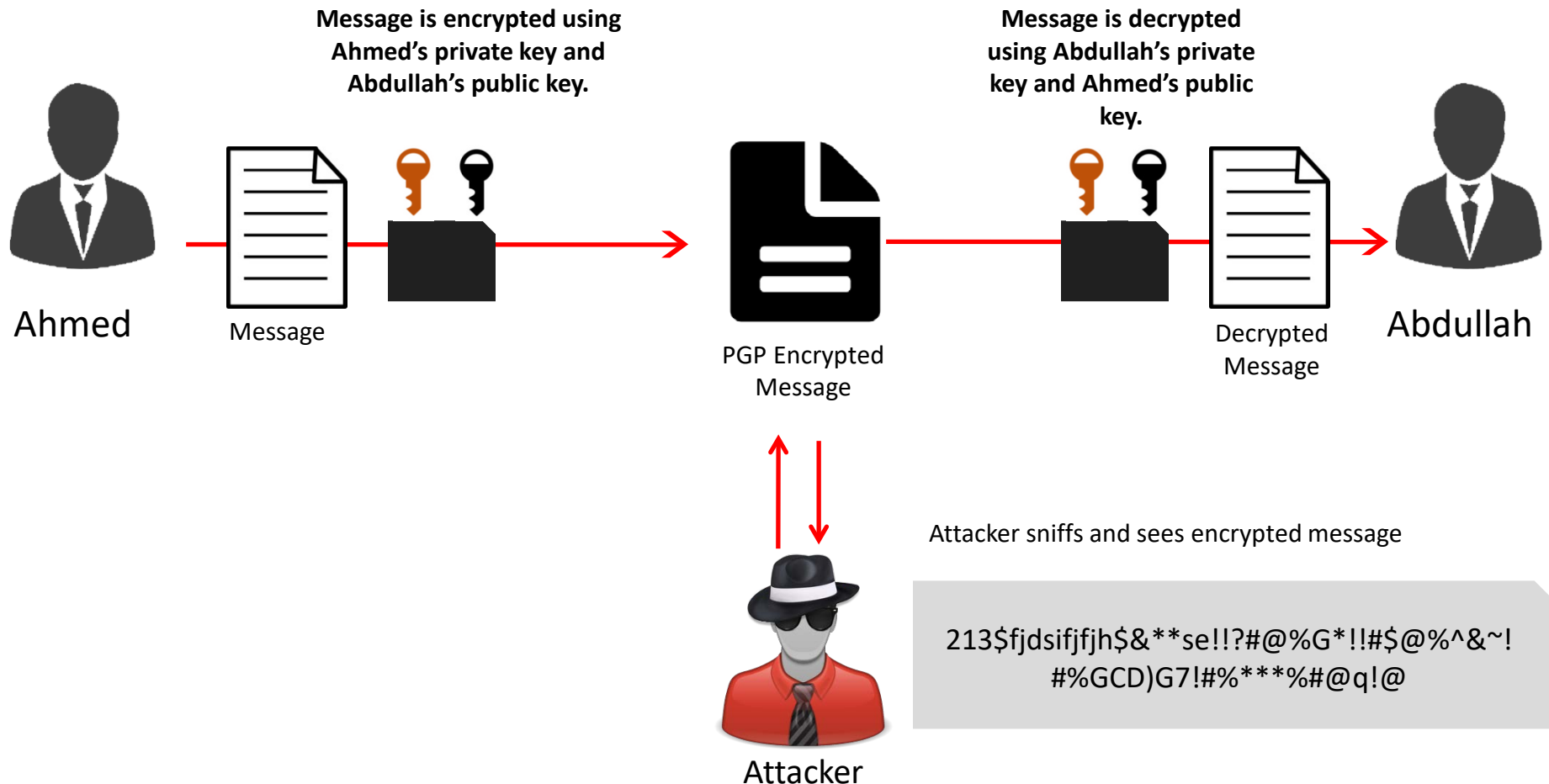


PGP (Pretty Good Privacy)

- PGP is a method to encrypt(code) and decrypt (decode) email over the internet.
- Purpose is to protect privacy of the email.
- PGP uses public key method (two keys are used i.e. public and private).
- Message is encrypted using a public key which is publicly available while the private key is limited to a particular user who uses it to decrypt the message.




Scenario: PGP Implementation



Email Security Policy



Following are types of email security policies that an organization should implement:

- 
- **E-mail Retention Policy**
 - ❖ This policy is devised to help employees determine which information sent or received by email should be retained and for what period of time.

Questions

