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
- Malicious Attachments
- Malicious Links
- Social Engineering
- Spam
- 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

This message was sent from a notification-only email address that does not accept incoming email. Please do not reply to this message. If you have any questions, please our Help Center to find answers to frequently asked questions.

Dear Valued Customer,
You have a new alert from Google Adwords.

Sign in to your AdWords account at http://www.googlzmn.com/Select/login

Yours Sincerely,
The Google AdWords Team
Spam

Hello,

Please revise the attached invoice and resend. Find invoice attached.

Regards,
Jessie
2nd Floor, No 3505 Jalan Technokrat 5
Cyberjaya, Selangor Darul Ehsan
Malaysia.
Tel: +60-3-8318-3111
Fax: +60-3-8318-8190

This message was sent using IMP, the Internet Messaging Program.

Invoice.pdf
Infected By Email

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of coronavirus. This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[Signature]

General Internist
Intensive Care Physician
WHO Plague Prevention & Control

World Health Organization
Infected By Email

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

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

HTTP [80] → Cleartext
POP [110] → Cleartext
SMTP [25] → Cleartext
IMAP [143] → Cleartext
Email Protocols - Encrypted

Server

HTTP [443] ➔ Encrypted using SSL/TLS
POPS [995] ➔
SMTPS [465] ➔
IMAPS [993] ➔

User
Secure Email Communication

SSL/TLS Tunnel

- HTTPS [443]
- POPS [995]
- SMTPS [465]
- IMAPS [993]
Secure Email Communication

![Internet E-mail Settings window with TLS selected for encrypted connection]
Encrypt Attachments

Email Security

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

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.
Encrypt Attachments

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.

This file contains:
- Document server properties, content type information,
- Embedded image data
Email Security Solutions

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

Secure Email Gateway filters out spam and malicious emails
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

---

Dear PayPal Member,

This email confirms that you have paid Debbie’s RC World, Inc. (eric@debbiesrcworld.com) $28.99 USD using PayPal.

This credit card transaction will appear on your bill as “PAYPAL DICK’S Sporting”.

PayPal Shopping Cart Contents

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Quantity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>InStep® &quot;My Caddy&quot;</td>
<td>1</td>
<td>$28.99 USD</td>
</tr>
</tbody>
</table>

Cart Subtotal: $28.99 USD
Shipping Charge: $9.60 USD
Cart Total: $38.59 USD

Shipping Information

- Shipping Info: William Quay
- 11 Ranter Avenue
- Highland Park, NJ 08904
- United States
- Address Status: Unconfirmed

If you have not authorized this charge, click the link below to cancel the payment and get a full refund.

Dispute Transaction

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the “Help” link in the footer of any page.
Example of Phishing Email

Dear Citibank customer,

We are letting you know that you, as a Citibank checking account holder, must become acquainted with our new Terms & Conditions and agree to it.

Please, carefully read all the parts of our new Terms & Conditions and post your consent.
Otherwise, we will have to suspend your Citibank checking account.

This measure is to prevent misunderstanding between us and our valued customers.
We are sorry for any inconvenience it may cause.

Click here to access our Terms & Conditions page and not allow your Citibank checking account suspension.

http://205.214.89.85/ebay.html

Dear eBay User,

During our regular update and verification of the accounts, we couldn't verify your current information. Either your information has changed or it is incomplete.
Please update and verify your information by clicking here and signing into your account. If the account information is not updated to current information within 5 days then, your access to bid, buy or sell on eBay will be restricted.

Thank you
Accounts Management

Copyright 2003 eBay Inc. All Rights Reserved.

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

www.c1t1bank.com:ac%398HAAA9UWDTYAZJWVWAAAA9pYWWgc2l6ZT00PjxTVgc2l6ZT00PjxT3Ac%398HAAA9UWDTYAZJWVWAAAA9pYWWgc2l6ZT00PjxTVgc2l6ZT00PjxT@211.155.234.84

http://205.214.89.85/ebay.html
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.facebook.com/re_activate

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

Regards,

Facebook Copyright Team.
Phishing Website

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

- Russian Federation: 18.72%
- United States: 12.29%
- India: 9.92%
- Germany: 6.22%
- Vietnam: 3.35%
- United Kingdom: 3.26%
- France: 3.25%
- Italy: 2.49%
- China: 2.30%
- Ukraine: 2.25%
- Others: 35.95%
Email Security

- Limit the size of email to prevent wastage of bandwidth.
- Avoid sending sensitive information over email but in case it's 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

Message is encrypted using Ahmed’s private key and Abdullah’s public key.

Message is decrypted using Abdullah’s private key and Ahmed’s public key.

Attacker sniffs and sees encrypted message

213$fjdsifjfjh$&**se!!?#@%G*!!#$@%^&~! #%GCD)G7l#%***%#@q!@
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