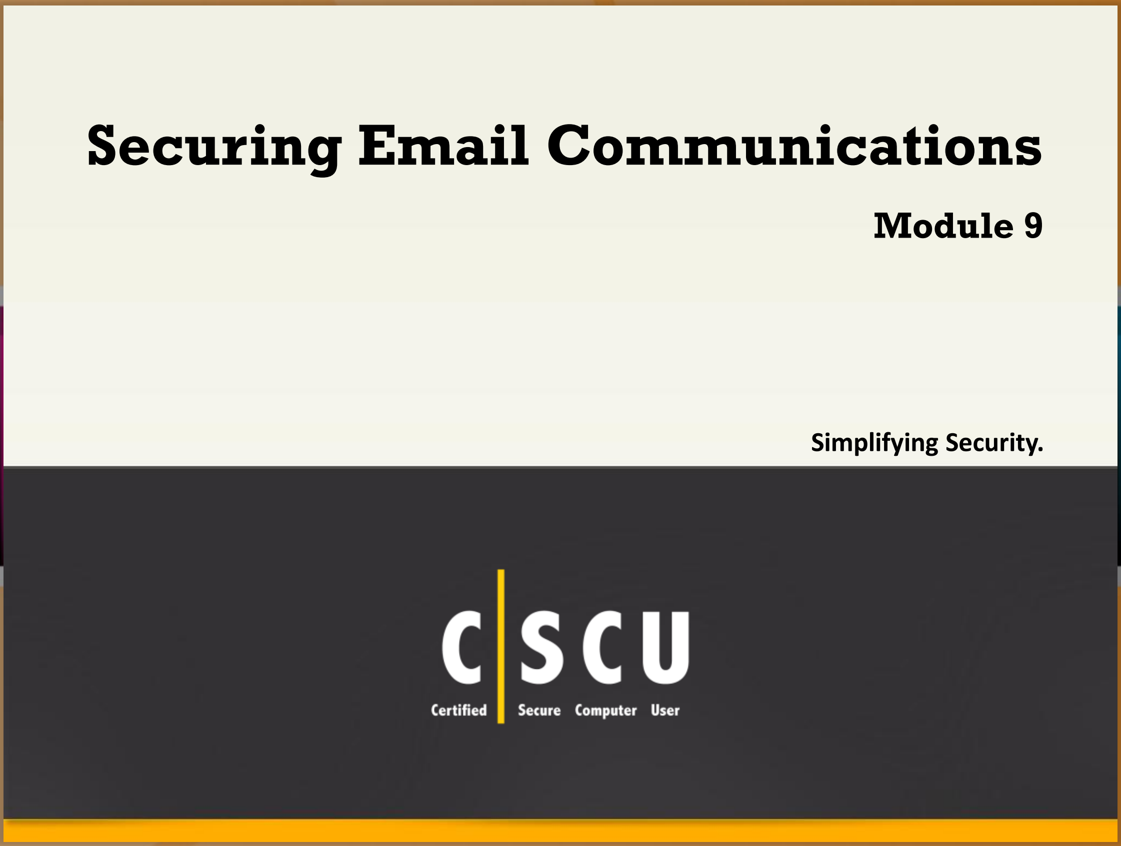


Securing Email Communications

Module 9

Simplifying Security.

CSCU

Certified Secure Computer User

Certified Secure Computer User

Module 9: Securing Email Communications

Exam 112-12

Module Objective

Email communications have entirely changed how humans perceive communication. Emails have allowed individuals to **communicate instantly**. However, relaying confidential information may result in the information being stolen and used against the user. This module talks about securing email communications.

This module will familiarize you with:

- The Email System
- Configuring Microsoft Outlook
- Email Security
- Email Security Threats
- Spamming
- Hoax/Chain and Scam Emails
- Email Security Control Layers
- Email Security Best Practices
- How to Obtain Digital Certificates?
- Online Email Encryption Service
- Email Communication: Don’ts
- Security Checklist
- Guidelines for Checking Emails on Mobile
- Email Security Tools

Module Flow

Introduction to Email Security

Email Security Threats

Email Security Procedures

How to Obtained Digital Certificates?

Email Security Tools

Email Security

In today's electronic world, email is considered as a prime **means of communication** and has become **critical** to any business being competitive. An email system in most of the organizations plays an important role and is used to communicate day-to-day activities within the group or outside the group. As communication is more dependent on the email system today, the importance of its security has become more significant. Email **security is a growing concern** for Internet users. The need for email security is evident for the following reasons:

- When a user sends an email to another user, it is not sent directly to the recipient. It is first stored in the server of the email client before being is delivered to the recipient. Moreover, the **Internet Service Provider** (ISP) may store the emails that can later be used against the sender.
- When the user sends an email to multiple recipients, all respondents can view the email addresses of the other recipients. A **spammer** can use these email lists to send **spam emails** to all of the recipients.
- Emails can be **forged easily**. They can be sent as if they were sent from someone else. This is a major concern because someone may pretend to be the user and send threats, or hate messages, which would get the user in trouble.
- **Insecure emails** allow attackers to check the user's personal and sensitive information.

Emails could be **sources of malware** in the form of attachments. The malware, when downloaded onto the machine, may install unwanted programs such as spyware that allows the attacker to find passwords and usernames to all of the user's accounts. The user's machine may also be used as a "**zombie**" computer to launch attacks on other computers.

Email Security Threats

Email today is a critical business communication tool. All the mail servers exchanging emails unfortunately has become the **number one source of security risk**. Email security issues have become more complicated with the rise of threats such as viruses that can corrupt and destroy critical documents and applications, hackers trying to **compromise the network** and **obtain confidential information**, spam mails that can degrade the performance network components and consume the bandwidth unnecessarily within the communications infrastructure. Some of the email security threats include:

Malicious email attachments

- Attachments may contain a virus, Trojan, worm, keyloggers, and more; opening such attachments infects the computer.

Phishing

- Phishing mails lure victims to provide personal data.

Spamming

- The user may receive spam mails that contain malware, allowing attackers to take control of the user computer.

Hoax/chain mail

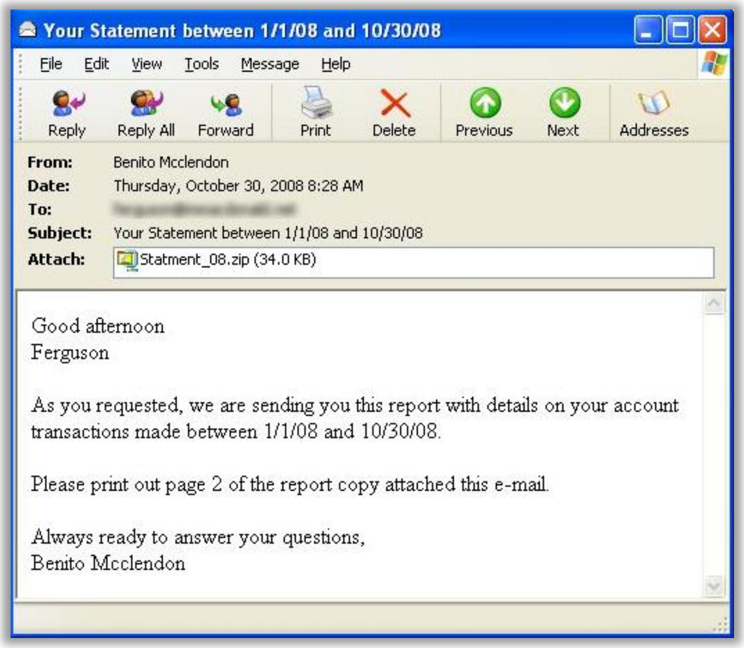
- The user may receive hoax emails that contain false information, insisting that he or she forward the mail.

Malicious user redirection

- Emails may contain links that direct users to malicious websites that host malwares and pornographic material.

Malicious Email Attachments

Email attachments are one of the major email security threats as they offer attackers the easiest and most powerful ways to attack a PC. Most **malicious attachments** install a virus, Trojan, spyware, or any other kind of malware code as soon as you open them.



From: Benito Mcclendon
Date: Thursday, October 30, 2008 8:28 AM
To: [redacted]
Subject: Your Statement between 1/1/08 and 10/30/08
Attach: Statment_08.zip (34.0 KB)

Good afternoon
Ferguson

As you requested, we are sending you this report with details on your account transactions made between 1/1/08 and 10/30/08.

Please print out page 2 of the report copy attached this e-mail.

Always ready to answer your questions,
Benito Mcclendon

Figure09-01: Malicious Email Attachments

Email Attachments: Caution

Attackers use email attachments to **propagate malware**. It is important that users do **not open any link** or **attachment** present in any **unsolicited emails**. A few measures to avoid opening email attachments include:

- Check if the email is from one of your contacts

- Check if the email was ever received from the source
- Never open an email attachment from an unreliable source
- Check if the subject line and name of the attachment are correlated with each other
- Do not open attachments with suspicious or unknown file extensions
  - Example: *.exe, *.vbs,*.bat,*.ini, *.bin, *.com, *.pif, or *.zzx
- Save and scan all email attachments before opening them

Spamming

Spam is junk mail or unsolicited or unwanted mail. Most spam mail is email advertising for various products sent to an email list. The total volume of spam is **more than 100 billion spam emails a day**. Spam averages 45 percent of all email sent.

Spammers amass email addresses from chat rooms, websites, and customer lists. They also use viruses to gather email addresses. They then **sell these email addresses** to other spammers.

Spamming is done mostly to advertise products. When the user clicks on the spam emails, they are directed to the product's website. If the customer decides to sign up for the product, the spammer is paid a predetermined amount of money. Although spam is used for advertising, spamming can waste the user's time. Moreover, merchants may place **tracking cookies** on the system once the user is directed to the merchant's website.

Spam emails may also contain malware such as viruses and Trojans. These can be used to steal personal information or to take control of the user's machine.

Spam email is also used for **clogging networks**. The attacker may send massive amounts of spam emails to the server of the email client or of an organization. Because of the massive amount of email that comes in, the email users will not be able to access their accounts. This attack is called a **denial of service (DOS)** attack.

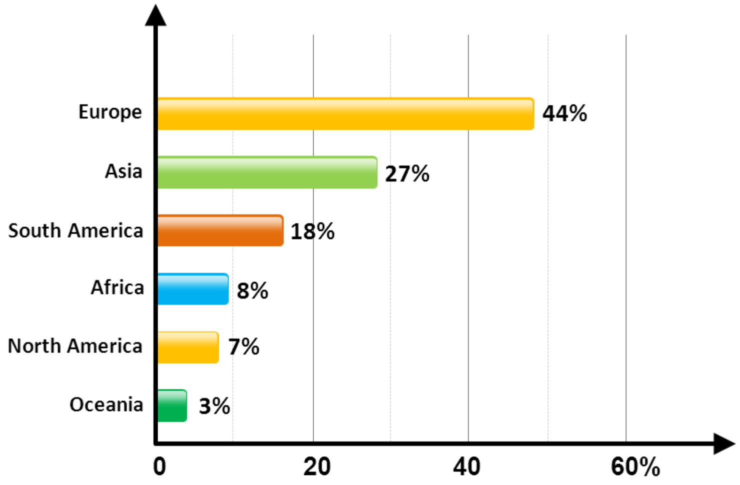


Figure 09-02: Top Spam-Generating Continents

Spamming Countermeasures

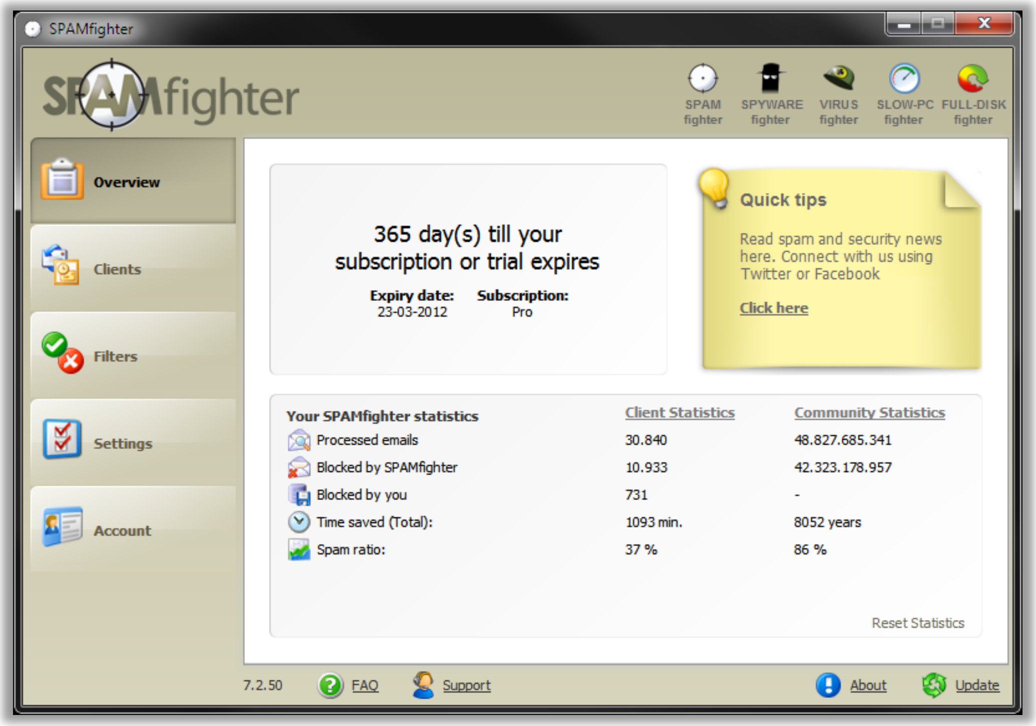
The countermeasures to protect from spam messages include:

- Report suspicious email as SPAM.
- Do not use an official email address while registering with any website.
- Use a different email address when posting messages to a public forum.
- Never follow the links in spam messages.
- Use the email client's spam filter and anti-spamming tools.
- Avoid opening spam messages (classified by spam filters).

Anti-Spamming Tool: SPAMfighter

Source: http://spamfighter.com

SPAMfighter works with Outlook, Outlook Express, Windows Mail or Thunderbird and helps in stopping spam mails getting into your PC. SPAMfighter tests all the new incoming mails automatically and if it's a spam, it will be moved directly to spam folder. Whenever new mail arrives, it will automatically be tested by SPAMfighter, and if it's spam, it will be moved to your spam folder.



365 day(s) till your subscription or trial expires

Expiry date: 23-03-2012

Subscription: Pro

Quick tips

Read spam and security news here. Connect with us using Twitter or Facebook

Click here

Your SPAMfighter statistics	Client Statistics	Community Statistics
Processed emails	30.840	48.827.685.341
Blocked by SPAMfighter	10.933	42.323.178.957
Blocked by you	731	-
Time saved (Total):	1093 min.	8052 years
Spam ratio:	37 %	86 %

Reset Statistics

Figure 09-03: SPAMfighter overview of live statistics of the spam mails

Hoax/Chain Emails

Hoaxes are email messages **warning** the recipients of **nonexistent threats**. Many users believe these messages to be true as they also warn of adverse effects if not forwarded to everyone they know. In some cases, these emails contain virus attachments. They are mostly used for **stealing personal information** that aids in stealing the identity of the user.

Scam Emails

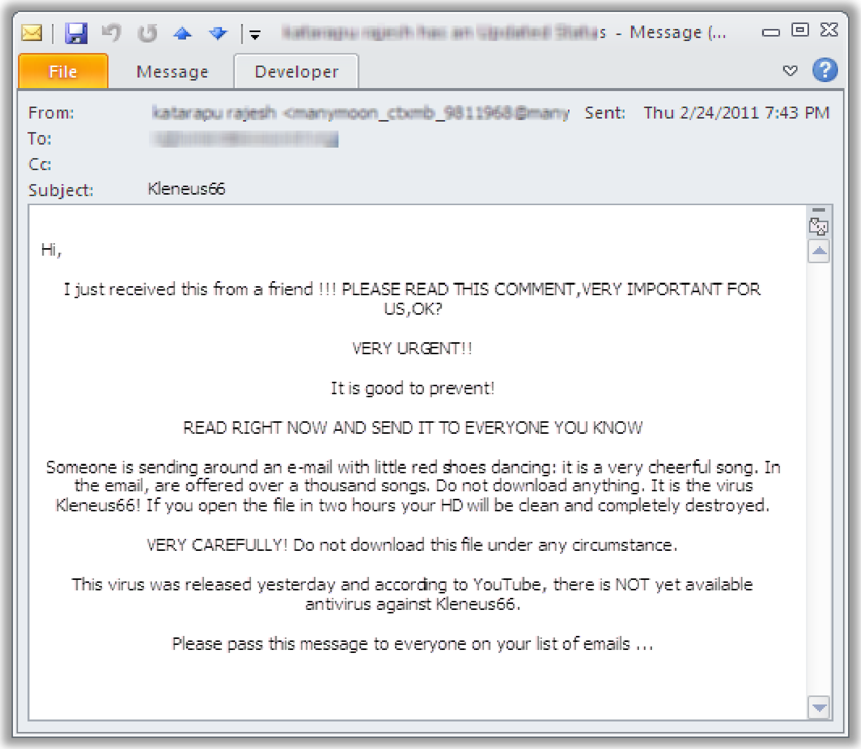
Scam emails are not addressed to the user by name. A scam email asks for a user's personal information such as:

- Bank account details
- Credit card numbers
- Passwords

Sometimes, users are asked to **forward** the mail to others. Scammers send scam emails to users, urging them to invest in their schemes and **promising high-paying rewards** in return. The users may blindly sign up for such schemes without thinking that they may be scammers. The users have to realize that they are being drawn into a **fraudulent scheme** if the rewards are too good to be true. The scammers then disappear without any payback. The users lose valuable time, money, and effort, and are left disappointed.

The different types of scams include:

- Literary scams
- Poetry scams
- Jury duty scams
- Chain letters and email scams
- Lottery scams
- Nigerian scams
- Credit card scams
- IRS email scams
- Vector marketing scams
- PayPal scam
- Missing persons scam
- Envelope stuffing
- Work from home scams
- Free vacation scam



From: [redacted] Sent: Thu 2/24/2011 7:43 PM
To: [redacted]
Cc:
Subject: Kleneus66

Hi,

I just received this from a friend !!! PLEASE READ THIS COMMENT,VERY IMPORTANT FOR US,OK?

VERY URGENT!!

It is good to prevent!

READ RIGHT NOW AND SEND IT TO EVERYONE YOU KNOW

Someone is sending around an e-mail with little red shoes dancing: it is a very cheerful song. In the email, are offered over a thousand songs. Do not download anything. It is the virus Kleneus66! If you open the file in two hours your HD will be clean and completely destroyed.

VERY CAREFULLY! Do not download this file under any circumstance.

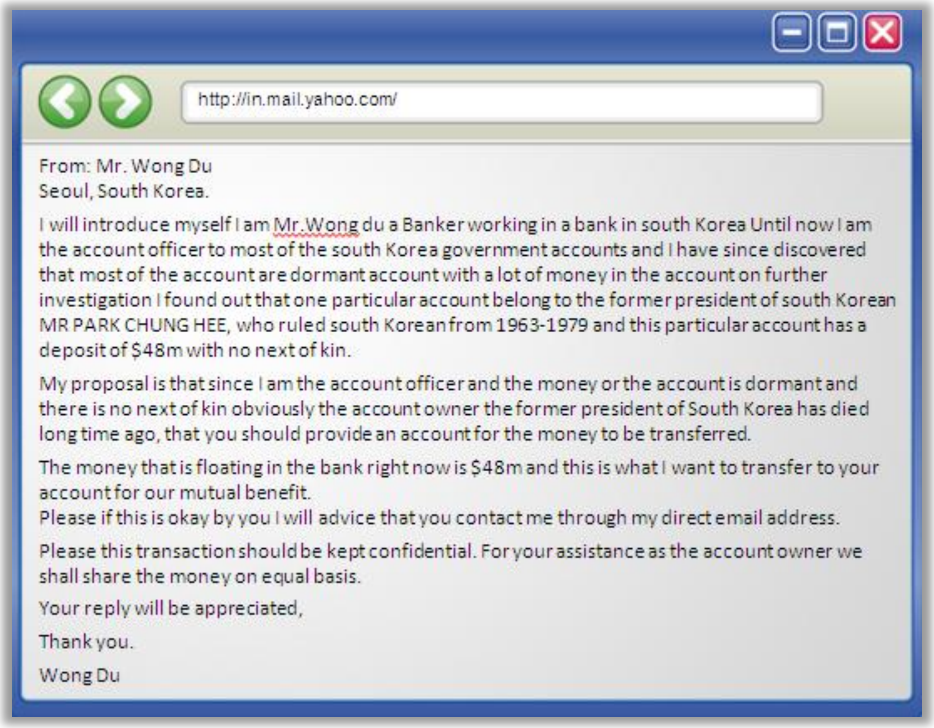
This virus was released yesterday and according to YouTube, there is NOT yet available antivirus against Kleneus66.

Please pass this message to everyone on your list of emails ...

Figure 09-04: Example for Hoax/Chain and Scam Emails

Nigerian Scam

A Nigerian scam is a form of advance payment of money or money transfer. This scam is called a Nigerian scam because it initially **started in Nigeria**, but they can come from anywhere in the world. Using this scam, scammers contact you by sending an email and offer you a share in a large sum of money. They claim that they want to transfer money to your account that is trapped in central banks during civil wars. They may also cite various reasons such as, massive inheritance problems, government restrictions, or taxes in the scammer's country. Scammers ask you to pay money or to give them your bank account details to help them transfer the money.



From: Mr. Wong Du
Seoul, South Korea.

I will introduce myself I am Mr.Wong du a Banker working in a bank in south Korea Until now I am the account officer to most of the south Korea government accounts and I have since discovered that most of the account are dormant account with a lot of money in the account on further investigation I found out that one particular account belong to the former president of south Korean MR PARK CHUNG HEE, who ruled south Korean from 1963-1979 and this particular account has a deposit of $48m with no next of kin.

My proposal is that since I am the account officer and the money or the account is dormant and there is no next of kin obviously the account owner the former president of South Korea has died long time ago, that you should provide an account for the money to be transferred.

The money that is floating in the bank right now is $48m and this is what I want to transfer to your account for our mutual benefit.
Please if this is okay by you I will advice that you contact me through my direct email address.

Please this transaction should be kept confidential. For your assistance as the account owner we shall share the money on equal basis.

Your reply will be appreciated,

Thank you.

Wong Du

Figure 09-05: Example of Nigerian Scam

Email Security Procedures

The email security procedures for any individual/organization include:

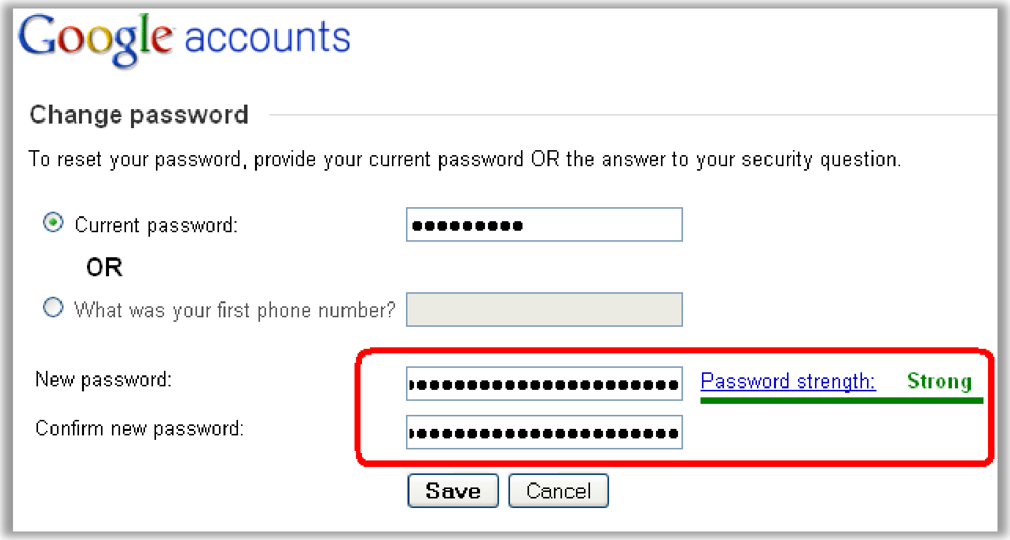
- Create and use strong passwords.
- Provide an **alternate email address** for mail recovery.
- Check for the last **Logging Activity.**
- Use **HTTPS** for browser connection.
- Disable/unselect the **Keep Me Signed In/Remember Me** functions.
- Scan email attachments for **malware.**
- **Turn off** the preview feature and change download settings in email clients.
- Create **Junk email filter** in email clients.
- **Digitally sign** your mail messages.
- Avoid **unwanted emails** using filters.

Creating Strong Passwords

Creating strong passwords for email accounts is the first step in securing email communications. Strong passwords make it **difficult for password crackers** or attackers to learn your password. Strong passwords are those that cannot be cracked by any automated cracking method or by brute force attacks.

The email clients generally have password standards that reveal the strength of the password used. Strong passwords are not necessarily long. Even shorter passwords can be made strong using all four characters—**capital letters**, **lowercase letters**, **numbers**, and **special characters**. But care should be taken that passwords are not shorter than eight characters.

Some social networking sites even deny the usage of passwords that are easily guessed such as "12345," "Password," names of popular cars such as "Ferrari," and "Porsche," or names of celebrities, movies, and so on.



Google accounts

Change password

To reset your password, provide your current password OR the answer to your security question.

◉ Current password: ••••••••••

OR

○ What was your first phone number?

New password: •••••••••••••••••••••••

Confirm new password: •••••••••••••••••••••••

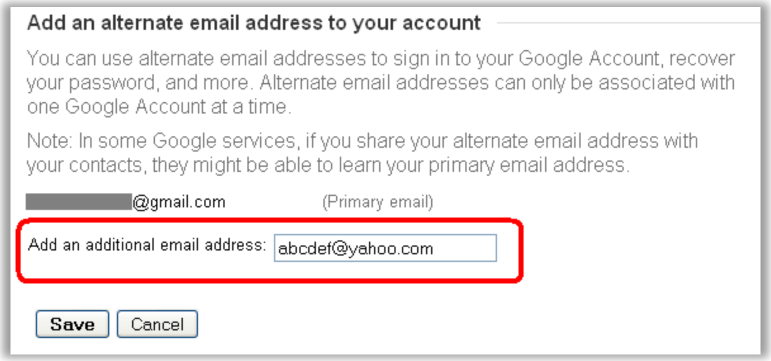
Password strength: Strong

Figure 09-06: Password Standards Used in Gmail States if a Password Is Strong

Alternate Email Address

Email clients offer the option of providing an alternate email address for security purposes. This email address is often termed as the secondary email address. When the user wishes to **reset the password** because he/she suspects it has been compromised, or has forgotten the password, the email client sends instructions to reset the password to the secondary email address provided by the user at the time of sign-up.

The user then has to log into the secondary email account to follow the instructions to reset the password of the primary email account. This inhibits cyber-criminals from resetting the passwords of authorized users' email accounts.



Add an alternate email address to your account

You can use alternate email addresses to sign in to your Google Account, recover your password, and more. Alternate email addresses can only be associated with one Google Account at a time.

Note: In some Google services, if you share your alternate email address with your contacts, they might be able to learn your primary email address.

[redacted]@gmail.com (Primary email)

Add an additional email address: abcdef@yahoo.com

Figure 09-07: Option in Gmail that Allows Users to Provide a Secondary Email Address

Keep Me Signed in/Remember Me

Email clients provide an option for the user to “**stay signed on**” when the user logs into his or her email account. This allows the user to log into his or her email account automatically without having to provide the username and password. Although this provides the user with quicker access to email services, it can be a **major security concern**.

If the computer is accessed by an **unauthorized user**, then he or she will be able to access the user’s email content without providing login information. Email users therefore **should not check this option**—more so when using public computers.

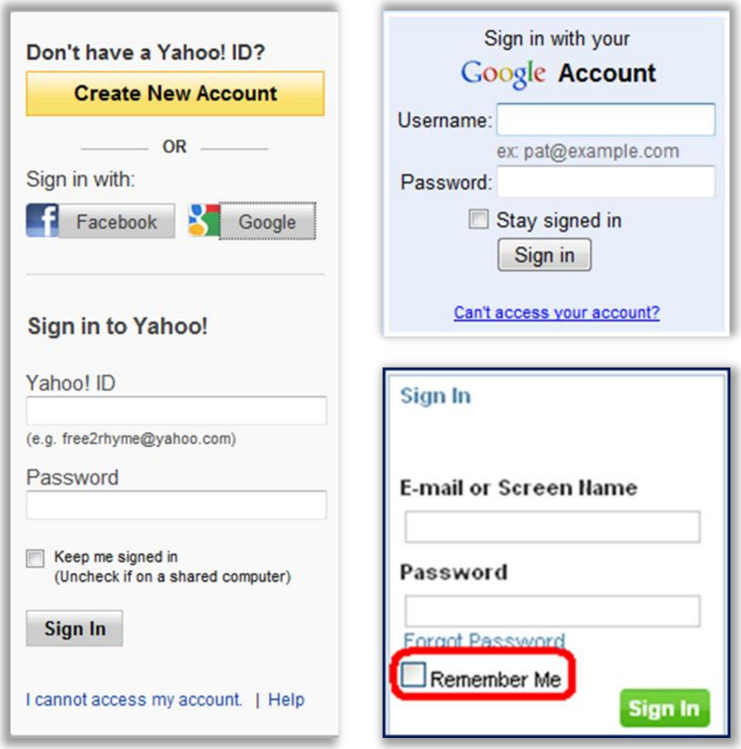
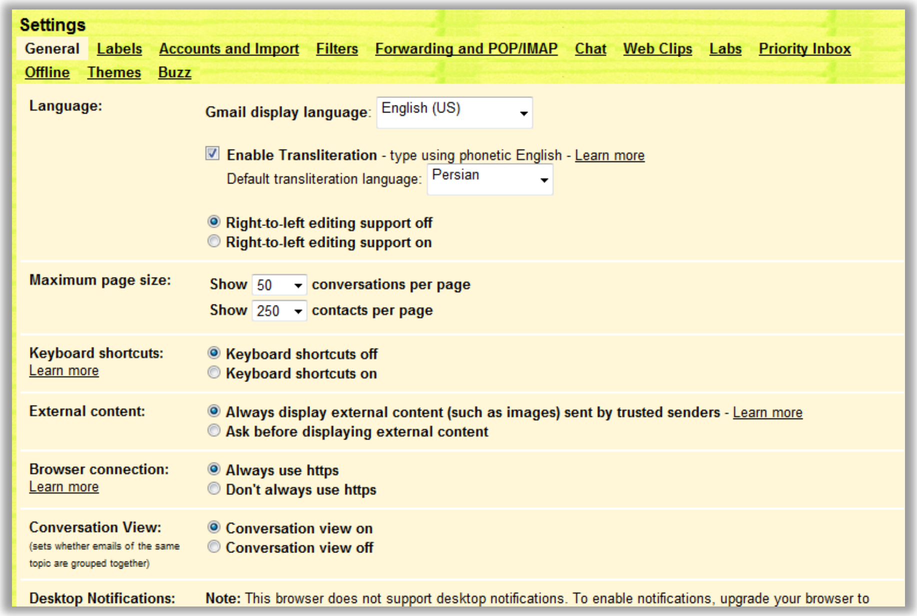


Figure 09-08: Options to Stay Signed On in Various Email Clients

Using HTTPS

Email clients use **Post Office Protocol** (POP) to retrieve email from the remote email server over a **TCP/IP Internet connection**. When the email is popped using the standard **POP3 protocol** (POP has undergone changes from POP1 to POP2; POP3 is the latest version), the user name and password are transmitted over the Internet to the email server. Anyone with sufficient knowledge will be able to sniff the login information.

To avoid login information falling into the wrong hands, email clients allow the user to POP the email over a **Secure Socket Layer** (SSL) connection. **HTTPS** is hypertext transfer protocol with SSL encryption. This encrypts all of the data exchanged between the email client and the server with a digital certificate, making it highly difficult for anyone to steal the user's login information.



Settings

General | Labels | Accounts and Import | Filters | Forwarding and POP/IMAP | Chat | Web Clips | Labs | Priority Inbox | Offline | Themes | Buzz

Language: Gmail display language: English (US)

☑ Enable Transliteration - type using phonetic English - Learn more

Default transliteration language: Persian

● Right-to-left editing support off
○ Right-to-left editing support on

Maximum page size: Show 50 conversations per page
Show 250 contacts per page

Keyboard shortcuts: Learn more
● Keyboard shortcuts off
○ Keyboard shortcuts on

External content:
● Always display external content (such as images) sent by trusted senders - Learn more
○ Ask before displaying external content

Browser connection: Learn more
● Always use https
○ Don't always use https

Conversation View: (sets whether emails of the same topic are grouped together)
● Conversation view on
○ Conversation view off

Desktop Notifications: **Note:** This browser does not support desktop notifications. To enable notifications, upgrade your browser to

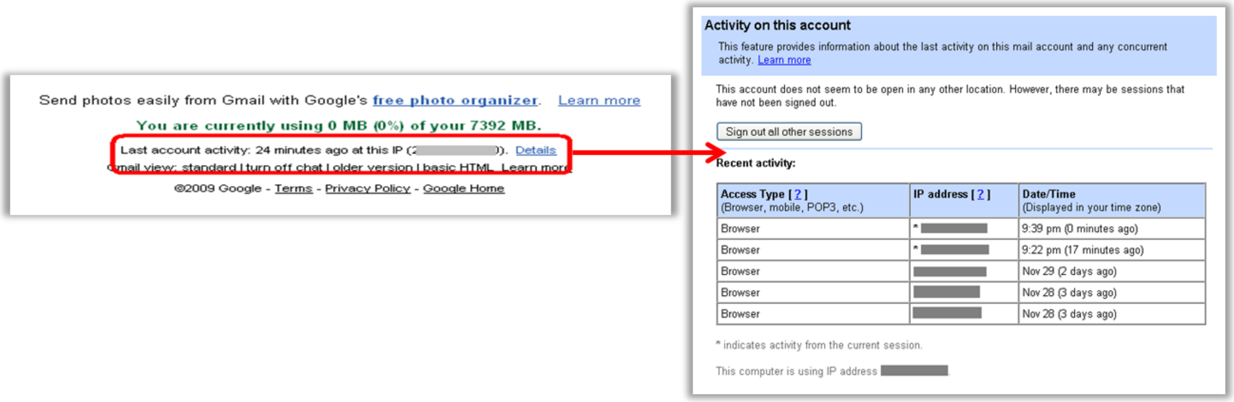
Figure 09-09: Browser Connection Settings in Gmail

Check for Last Account Activity

The users' email accounts can be accessed by a cyber-criminal from anywhere in the world without their knowledge. If the users are suspicious of someone else accessing their email, they can check the recent account activity. The "last account activity" gives details of the most recent account login such as:

- The date/time of login
- The IP address from where the email account was accessed
- Access type—whether the email account was accessed from a browser, mobile, POP3, and so on

Users can also check if the email account is open somewhere else. This may result from unauthorized access or because the user had forgotten to sign out of a session. Users can close all other open sessions by clicking **Sign out of all other sessions.**



Send photos easily from Gmail with Google's free photo organizer. Learn more

You are currently using 0 MB (0%) of your 7392 MB.

Last account activity: 24 minutes ago at this IP (2[redacted]). Details

Gmail view: standard | turn off chat | older version | basic HTML Learn more

©2009 Google - Terms - Privacy Policy - Google Home

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	IP address [?]	Date/Time (Displayed in your time zone)
Browser	* [redacted]	9:39 pm (0 minutes ago)
Browser	* [redacted]	9:22 pm (17 minutes ago)
Browser	[redacted]	Nov 29 (2 days ago)
Browser	[redacted]	Nov 28 (3 days ago)
Browser	[redacted]	Nov 28 (3 days ago)

* indicates activity from the current session.

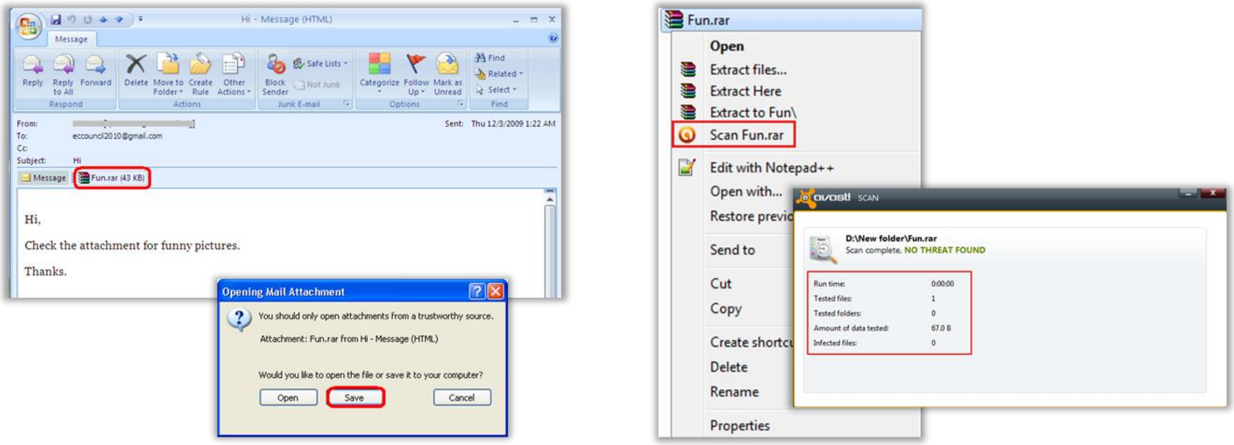
This computer is using IP address [redacted].

Figure 09-10: Checking for Last Account Activity in Gmail

Scanning Email Attachments

Email attachments are used by cyber-criminals to **spread malware**. Email attachments may contain **viruses**, **spyware**, or **keyloggers** that help cyber-criminals **gain control** of the user's machine or **steal personal information**. Hence, the user should not download any email attachments from unsolicited emails.

Even attachments from trusted sources should be **scanned with an anti-virus** after downloading them. Alternately, the anti-virus can be configured so that all downloads are automatically scanned.



From: [redacted]

Sent: Thu 12/3/2009 1:22 AM

To: eccouncil2010@gmail.com

Cc:

Subject: Hi

Hi,

Check the attachment for funny pictures.

Thanks.

Opening Mail Attachment

You should only open attachments from a trustworthy source.

Attachment: Fun.rar from Hi - Message (HTML)

Would you like to open the file or save it to your computer?

D:\New folder\Fun.rar

Scan complete, NO THREAT FOUND

Run time:	0:00:00
Tested files:	1
Tested folders:	0
Amount of data tested:	67.0 B
Infected files:	0

Figure 09-11: Scanning the Email Attachments Using Anti-Virus

Turn Off Preview Feature

Email clients have an option to show a preview of an email. But this option comes with the risk of being infected with a virus or worm after clicking the preview button. Therefore, it is recommended to **disable the preview pane** in email clients to avoid the execution of script code without the user explicitly opening the message.

To turn off the preview pane in Microsoft Outlook:

- Go to the **View** menu and select **Reading Pane.**
- Select the **Off** option**.**

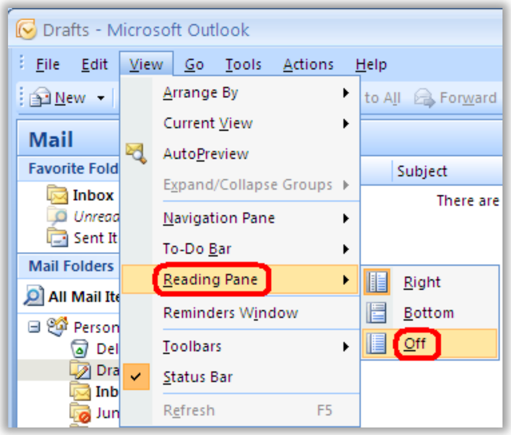


Figure 09-12: Turn Off the preview pane in Microsoft Outlook

To turn off the preview feature in Mozilla Thunderbird:

- Go to the **View** menu and select **Layout.**
- Uncheck the **Message Pane** option.

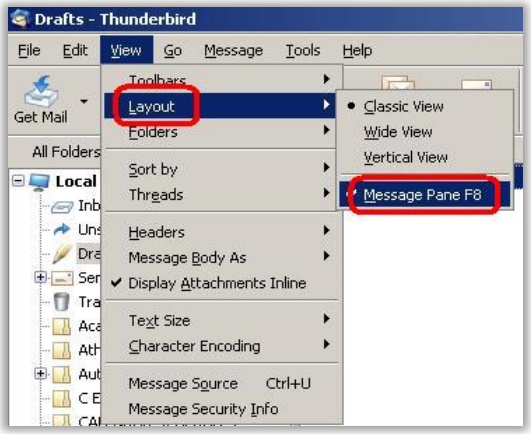
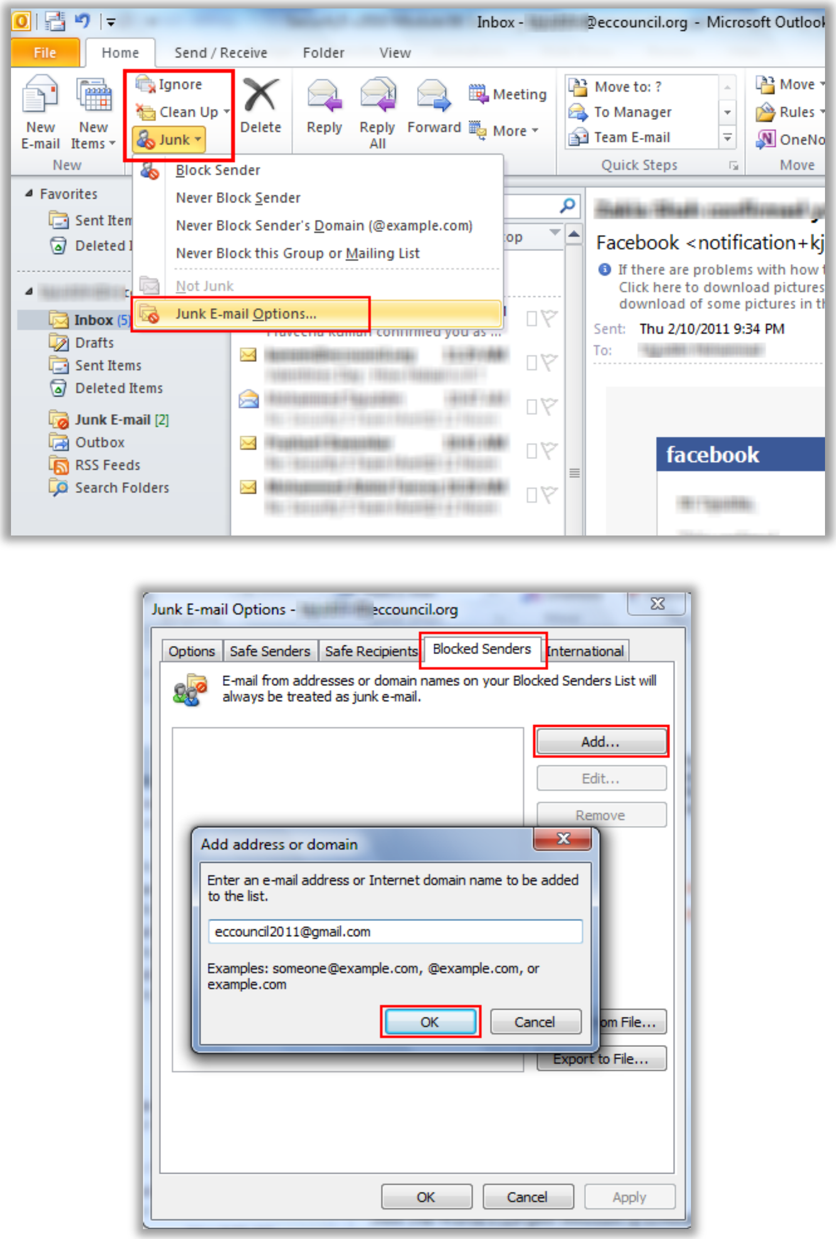


Figure 09-13: Turn Off the Preview Feature in Mozilla Thunderbird

Email Filtering: Avoiding Unwanted Emails

Guidelines for avoiding unwanted emails include:

- Email filtering is the process of organizing emails according to specified criteria.
- Email filters are generally used to identify and categorize spam mails.
- To avoid unwanted emails in Outlook 2010, go to the **Home** tab, click **Junk** and **Junk E-mail Options**, on the **Blocked Sender** tab, and click **Add.**
- Enter an email address or domain name and click **OK.**



Facebook <notification+kj

If there are problems with how t... Click here to download pictures ... download of some pictures in th...

Sent: Thu 2/10/2011 9:34 PM

To:

E-mail from addresses or domain names on your Blocked Senders List will always be treated as junk e-mail.

Enter an e-mail address or Internet domain name to be added to the list.

eccouncil2011@gmail.com

Examples: someone@example.com, @example.com, or example.com

Figure 09-14: Avoiding Unwanted Emails

Digitally Sign Your Emails

A digital signature is an **electronic signature** used to authenticate the sender of an email message. Digital signatures help to ensure that the content of the email is not tampered with. Digital signatures are easily transportable and cannot be mimicked by anyone.

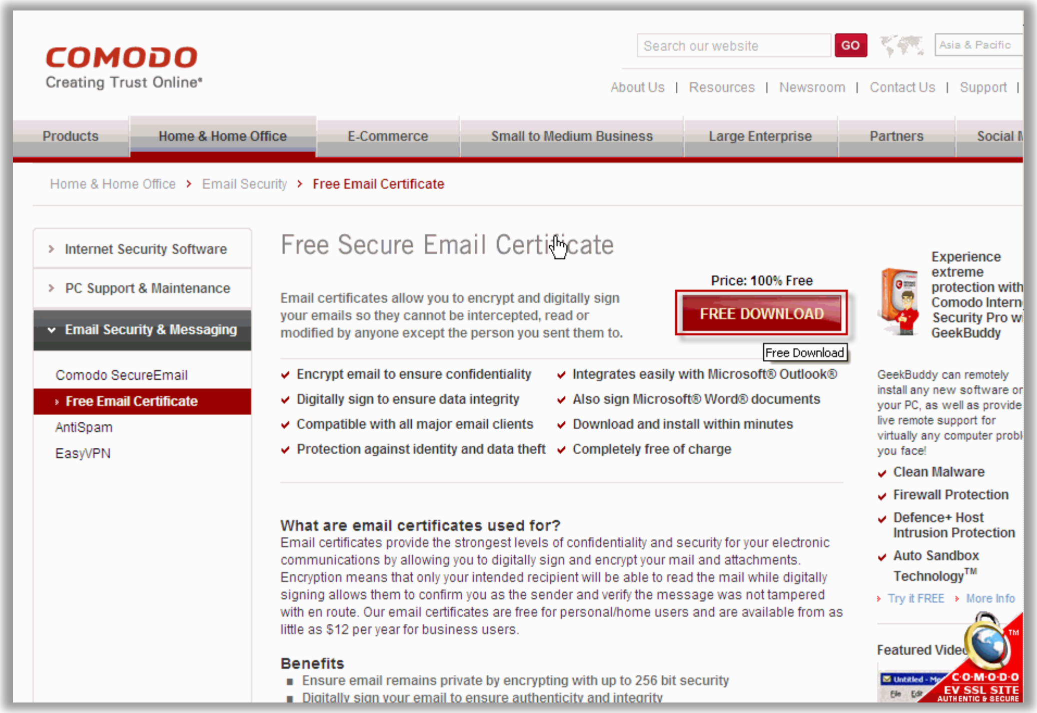
Digital signatures can be requested from vendor websites. Some vendors offering digital signatures include:

- Verisign – http://www.verisign.com
- Thawte – http://www.thawte.com
- Entrust – http://www.entrust.com
- Comodo – http://www.comodo.com
- ARX CoSign – https://www.arx.com
- Avoco secure2trust – http://www.avocosecure.com
- ChosenSecurity Trust Centre – http://www.chosensecurity.com

How to Obtain Digital Certificates

The steps to obtain digital certificate include:

- Go to the **Certificate Authorities** website.
- Purchase and download a digital certificate.
- Some certificate authorities offer a free personal email security certificate such as **Comodo.**
- Provide personal details to download the certificate.
- **Login** to the account you have provided.
- Check your inbox; you will get an **installation link.**



Free Secure Email Certificate

Email certificates allow you to encrypt and digitally sign your emails so they cannot be intercepted, read or modified by anyone except the person you sent them to.

- ✓ Encrypt email to ensure confidentiality
- ✓ Digitally sign to ensure data integrity
- ✓ Compatible with all major email clients
- ✓ Protection against identity and data theft
- ✓ Integrates easily with Microsoft® Outlook®
- ✓ Also sign Microsoft® Word® documents
- ✓ Download and install within minutes
- ✓ Completely free of charge

What are email certificates used for?

Email certificates provide the strongest levels of confidentiality and security for your electronic communications by allowing you to digitally sign and encrypt your mail and attachments. Encryption means that only your intended recipient will be able to read the mail while digitally signing allows them to confirm you as the sender and verify the message was not tampered with en route. Our email certificates are free for personal/home users and are available from as little as $12 per year for business users.

Benefits

- Ensure email remains private by encrypting with up to 256 bit security
- Digitally sign your email to ensure authenticity and integrity

Experience extreme protection with Comodo Intern Security Pro wi GeekBuddy

GeekBuddy can remotely install any new software or your PC, as well as provide live remote support for virtually any computer probl you face!

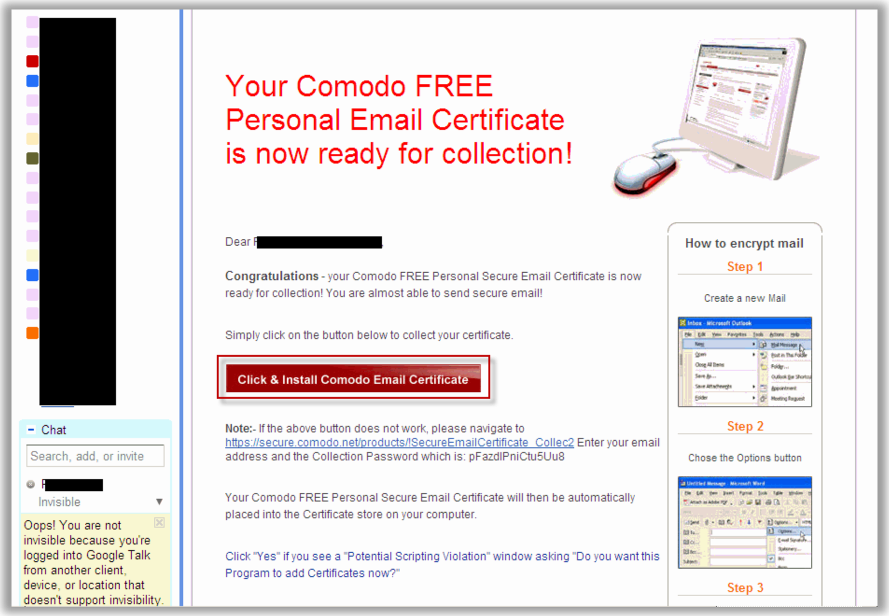
- ✓ Clean Malware
- ✓ Firewall Protection
- ✓ Defence+ Host Intrusion Protection
- ✓ Auto Sandbox Technology™

Figure09-15: COMODO Free Digital Certificate Download

Installing Digital Certificate

The steps to install a digital certificate include:

- Click the installation link to install the digital certificate.
- In **Internet Explorer,** go to **Tools** → **Internet Options** → **Content** tab.
- In the content tab. click the **Certificates** button.
- Select the certificate and click the **Export** button.
- Click **Next.**
- Check the **Yes, export the private key** option.
- Click **Next.**
- Protect the private key by providing a password and confirming it.
- Specify the file you want to export and save it in a particular location.



[redacted]

Oops! You are not invisible because you're logged into Google Talk from another client, device, or location that doesn't support invisibility.

Your Comodo FREE Personal Email Certificate is now ready for collection!

Dear [redacted]

Congratulations - your Comodo FREE Personal Secure Email Certificate is now ready for collection! You are almost able to send secure email!

Simply click on the button below to collect your certificate.

Note:- If the above button does not work, please navigate to https://secure.comodo.net/products/!SecureEmailCertificate_Collec2 Enter your email address and the Collection Password which is: pFazdlPniCtu5Uu8

Your Comodo FREE Personal Secure Email Certificate will then be automatically placed into the Certificate store on your computer.

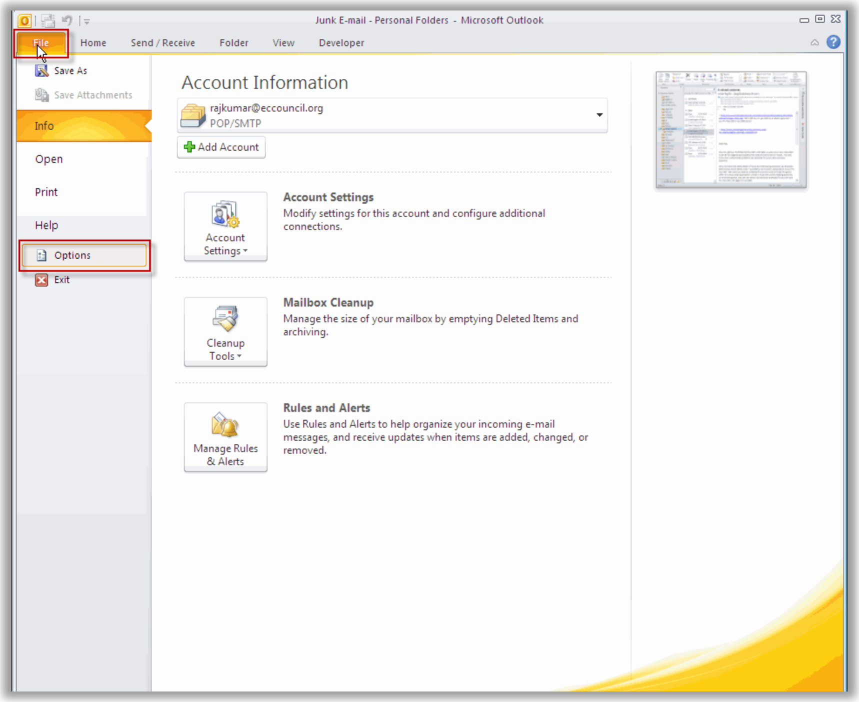
Click "Yes" if you see a "Potential Scripting Violation" window asking "Do you want this Program to add Certificates now?"

Figure 09-16: Installing a COMODO Digital Certificate

Signing your Emails

The steps to sign your emails include:

- Go to the **Microsoft Outlook → File → Options.**
- Click **Trust Center → Trust Center Settings → Email Security.**
- Encrypt the mail by checking the appropriate boxes under the **Encrypted e-mail** section.
- Click the **Import/Export** button.
- Browse the file to open and provide the password and digital ID name.
- Click **OK.**
- Click **New Mail** to write a message.
- After clicking, the **Send** button, it will prompt you to encrypt the message.
- Click **Send Unencrypted** (if the recipient does not have private key).
- Click **Continue** if the recipient has a private key.



Account Information

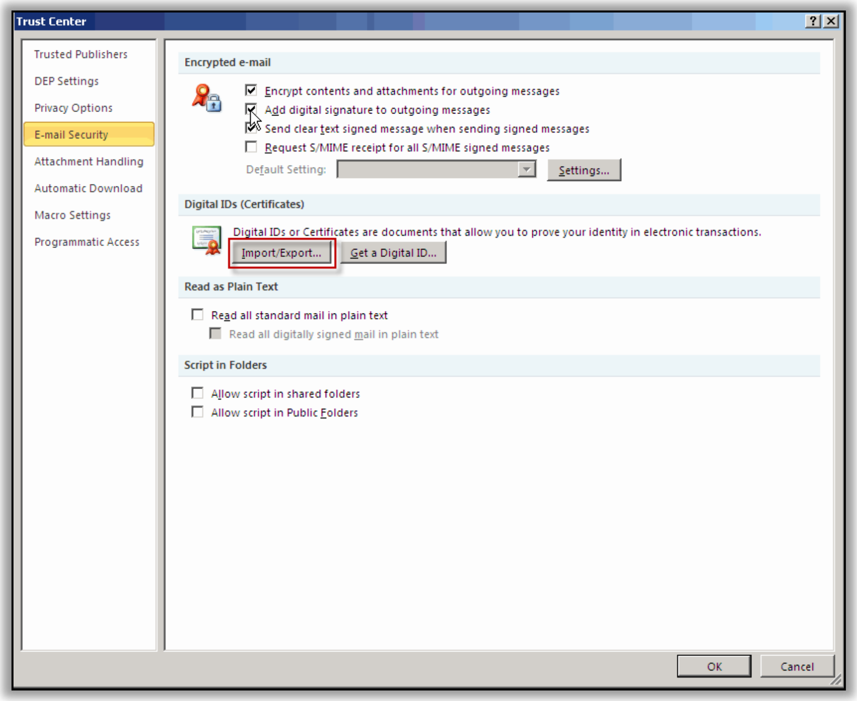
rajkumar@eccouncil.org
POP/SMTP

Add Account

Account Settings
Modify settings for this account and configure additional connections.

Mailbox Cleanup
Manage the size of your mailbox by emptying Deleted Items and archiving.

Rules and Alerts
Use Rules and Alerts to help organize your incoming e-mail messages, and receive updates when items are added, changed, or removed.



Encrypted e-mail

☑ Encrypt contents and attachments for outgoing messages
☑ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
☐ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

☐ Read all standard mail in plain text
☐ Read all digitally signed mail in plain text

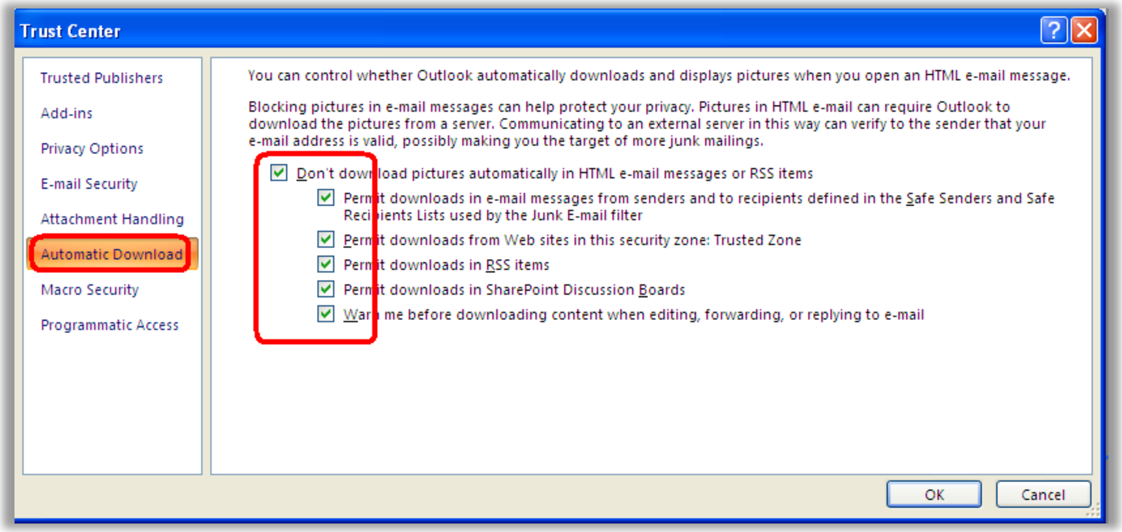
Script in Folders

☐ Allow script in shared folders
☐ Allow script in Public Folders

Figure 09-17: Signing Your Emails Digitally

Microsoft Outlook Download Settings

Choose the **Automatic Download** option and select the options shown in the following figure.



You can control whether Outlook automatically downloads and displays pictures when you open an HTML e-mail message.

Blocking pictures in e-mail messages can help protect your privacy. Pictures in HTML e-mail can require Outlook to download the pictures from a server. Communicating to an external server in this way can verify to the sender that your e-mail address is valid, possibly making you the target of more junk mailings.

☑ Don't download pictures automatically in HTML e-mail messages or RSS items

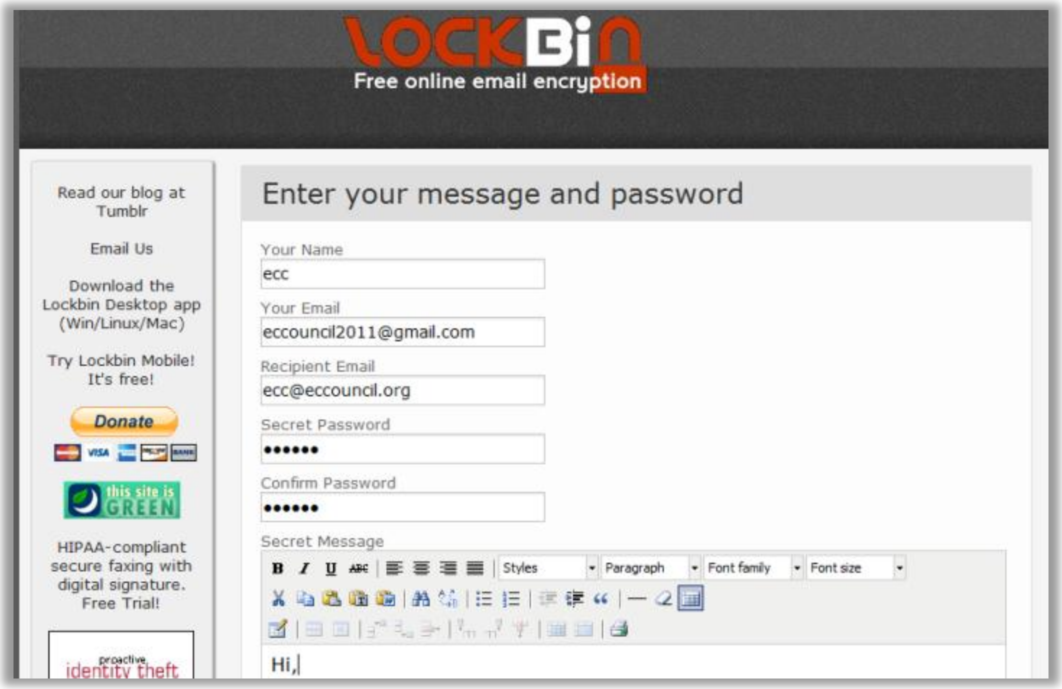
- ☑ Permit downloads in e-mail messages from senders and to recipients defined in the Safe Senders and Safe Recipients Lists used by the Junk E-mail filter
- ☑ Permit downloads from Web sites in this security zone: Trusted Zone
- ☑ Permit downloads in RSS items
- ☑ Permit downloads in SharePoint Discussion Boards
- ☑ Warn me before downloading content when editing, forwarding, or replying to e-mail

Figure 09-18: Downloading Settings Microsoft Outlook 2010

Online Email Encryption Service: Lockbin

Source: https://lockbin.com

Lockbin is a free online email encryption service. It can be used to encrypt emails containing personal/confidential information such as credit card information.



LOCKBIN
Free online email encryption
Read our blog at Tumblr
Email Us
Download the Lockbin Desktop app (Win/Linux/Mac)
Try Lockbin Mobile! It's free!
Donate
this site is GREEN
HIPAA-compliant secure faxing with digital signature. Free Trial!
proactive identity theft
Styles
Paragraph
Font family
Font size

Enter your message and password

Your Name: ecc

Your Email: eccouncil2011@gmail.com

Recipient Email: ecc@eccouncil.org

Secret Password: ••••••

Confirm Password: ••••••

Secret Message:

Hi,

Figure 09-19: Sending Private Message Using Lockbin

Email Security Tools

Comodo AntiSpam

Source: http://www.comodoantispam.com

Comodo AntiSpam is an intuitive, easy-to-use, client-based software product that eliminates spam forever from your computer's email system. It uses 'Passcode Authentication' technology, a patent-pending, active-filtering algorithm, to authenticate the sender of each incoming email message. Comodo AntiSpam works with all current Windows operating systems and supports email programs such as Outlook, Outlook Express, and Eudora, Netscape or any other POP3 email application. Comodo AntiSpam is guaranteed to eliminate all spam from your computer.

Netcraft Toolbar

Source: http://toolbar.netcraft.com

It is browser toolbar to report and block phishing sites identified by the toolbar user community. It provides Internet security services, including anti-fraud and anti-phishing services, application testing, code reviews, and automated penetration testing.

PhishTank SiteChecker

Source: https://addons.mozilla.org

PhishTank SiteChecker gives Firefox users a way to bring the community judgment of PhishTank into their browser, for extra protection against phishing.

Spamihilator

Source: http://www.spamihilator.com

Spamihilator works between E-Mail client and the Internet and examines every incoming E-Mail. Useless spam mails (Junk) will be filtered out. This process runs completely in the background. The Learning Filter (Bayesian Filter) uses the rules of Thomas Bayes (English mathematician, 18th century) and calculates a certain Spam-Probability for every E-Mail. In addition Spamihilator uses a Word-Filter that searches messages for known keywords. User-defined words and regular expression can also be added.

McAfee SpamKiller

Source: http://us.mcafee.com

SpamKiller can filter any number of e-mail accounts. When SpamKiller is running, an envelope icon is displayed in the system tray. SpamKiller automatically run programs and play sounds, depending on the type of messages you receive. For example, it can automatically start your e-mail program when new mail arrives.

Comodo Email Certificate

Source: http://www.comodo.com

Secure Certificates let you digitally sign emails to prove that the attachments and email content actually came from you. Secure Email Certificates allow you to easily encrypt your emails and ensure that the attachments and messages may only be read by the intended recipients. Digitally signing email with a digital Certificate means that it is impossible for anyone to edit the content of your mail without the recipient being alerted. Comodo's digital Certificates are fully trusted by 99 percent of email clients.

Mirramail Secure Email

Source: http://www.mirrasoft.com

Mirramai is a fully featured email program, like Outlook or Outlook Express, except the emails you send can be easily secured with 256 bit AES Encryption at the click of a button. The security provided by Mirramail is not just for sending or receiving messages - the messages stored on your computer are also secured with 256-bit AES encryption.

Encryptomatic MessageLock

Source: http://www.encryptomatic.com

MessageLock is an add-in for Microsoft Outlook that allows the sender to protect email messages using strong AES-256 bit encryption (exceeds HIPAA's minimum strength requirements). To use MessageLock, just open a new email message in Microsoft Outlook, and click the "Encrypt Email" button in the Outlook email toolbar.

Module Summary

Email is a method of exchanging digital messages with one or more recipients.

Attachments can contain malicious programs; opening such attachments can infect the computer.

Spamming is the process of populating the user’s inbox with unsolicited or junk email.

Hoaxes are false alarms that claim reports of a nonexistent virus.

Do not forget to delete your browser cache, passwords, and history.

Consider setting mobile phones to download only headers of emails, not the full email.

Digital signatures are used to authenticate the sender of a message or the signer of a document.

Email security tools protect passwords and automatically logs users off their email accounts.

Email Communication Checklist

The following is a list of Don’ts that users should follow for secure email communications:

- □ **DON’T USE** just one email account for all purposes.
- □ **DON’T CLOSE** the browser without properly logging out.
- □ **DON’T FORGET** to delete your browser cache, passwords, and history.
- □ **DON’T SEND** personal and financial information via email.
- □ **DON’T TRUST** emails from your friends to be secure.
- □ **DON’T DELETE** spam instead of blacklisting it.
- □ **DON’T FAIL** to scan all email attachments.
- □ **DON’T FAIL** to enable the email spam filter.
- □ **DON’T SHARE** your email account information with others.
- □ **DON’T USE** simple and easy-to-guess passwords.

Email Security Checklist

It is impossible to avoid using email, and the user, therefore, has to be aware of the threats that unsolicited emails can pose and how to secure email communications. The following is a list of the best practices a user should follow for safer email communications:

- □ Create strong passwords for logging into mail accounts.
- □ Enable “**https**” for secure communications/transactions.
- □ Be diligent while opening email attachments.
- □ Do not click the links provided in email messages.
- □ Follow email etiquette when forwarding messages.
- □ Do not forward or reply to spam and suspicious emails; delete them.
- □ Avoid accessing email via an unsecured public wireless connection.
- □ Avoid accessing email accounts on shared computers.
- □ Avoid sending large attachments in emails.
- □ Use the **BCC:** option when sending mail to bulk recipients.

□ Never save your password in the web browser.

□ Sort messages by priority, subject, date, sender, and other options.

□ Avoid sending confidential, sensitive, personal, and classified information in emails.

□ Clean your inbox regularly.

□ Create folders and move emails accordingly (Family, Friends, Work, etc.).

□ Digitally sign your outgoing mails.

□ Send attachments in PDF format rather than Microsoft Word or Excel formats.

Security Checklist for Checking Emails on Mobile

Mobile phones and other portable devices are not used just for making calls now. Accessing email from mobile devices is common today. The access of email on mobile devices has also brought in considerable security concerns. Some security tips to help mobile users send/receive email safely over their devices include:

□ Consider setting mobile phones to download only email headers, not the full email.

□ Configure the device to only offer attachment notifications, not attachments.

□ Do not open/send large attachments from mobile devices.

□ Do not follow links sent in email or text messages.

□ Install mobile anti-virus and keep it up to date.

□ Users should understand how their email client handles emails accessed from mobile devices.

□ Some clients may delete the email from the server when the user accesses that email from a mobile device. Users, therefore, may have to make a copy of the email.

□ Turn off the option **Show Pictures** in Internet Explorer (Go to **Tools** → **Internet Options** → **Advanced** and uncheck the **Show Pictures** option).

□ To reduce the size zip and send any important files and send emails as plaintext.