Email

Email, Or Electronic Mail, Is Becoming More And More Popular As People Learn To Communicate Again With Written Words. For Many Purposes It Is Superior To A Phone Call Because You Don't Have To Catch The Person In And You Can Get Straight To The Point. No Time Is Wasted On Casual Conversation. It Also Leaves A Written Record To Refer Back To For A Response Or If You Forget Who Said What. Email Is Superior To The Traditional Office Memo Because It Uses No Paper (Save The Trees!!) And It Can Be Sent To A Whole List Of People Instantly.

Purpose: Transmitting Messages Between Computer Users

Major Advantage: Speed For Communication And The Lower Cost .

Major Disadvantage: You Don't Know If The Receiver Actually Reads It, Though You Can Find Out If They Received It. Of Course In A Phone Conversation You Don't Really Know If The Person Is Actually Listening Either!

With No Body Language Or Vocal Intonations It Is Difficult To Convey The Emotional Tone You Want.

Introduction to Email Security

Today email is so widely used that it has become the default means of communication where the correspondents feel that they can discuss matters that can be kept between them. We analyze below how this might be a dangerous illusion, especially when discussing matters with legal, business or political content and I but may comment to use email safety .

Email borne viruses

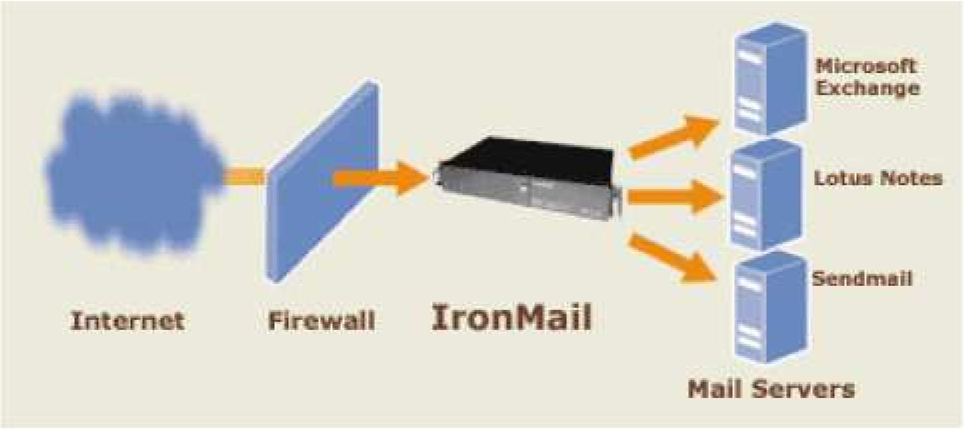
Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs.

Secure Your Communications email

Once your gateway is secure, the next step is securing your communications beyond the gateway to include your external users, partners, clients and others.

IronMail achieves this with our Mail-VPN feature.

Mail-VPN secures messages while they are in transit over the Internet, with no client interaction, using SSL technology. Mail-VPN can create secure tunnels to other mail servers or other IronMail units as well as end-users such as remote employees and telecommuters. Mail-VPN capabilities include:



The Only Comprehensive Security Solution For Email Systems

IronMail, an all-inclusive email security appliance, sits at the mail gateway between your network firewall and mail servers. Every connection to your mail server(s) passes through IronMail.

IronMail is the first product designed to provide application-level security for email.

What does this mean? It means that IronMail will not allow exploitation of vulnerabilities in your email systems or allow your email system to be used as a delivery vehicle for attacks.

Securing Email Using SSL

SSL is widely known as the technology that allows companies like E*Trade to conduct millions of dollars a day in transactions securely over the Internet However, SSL is not specifically tied to web traffic (HTTP).

SSL is a transport-layer protocol developed to secure TCP/IP-based protocols such as Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and, of course, HTTP.

By applying SSL technology to email, secure email becomes as easy to secure as web browsing.

Email Security Guidelines

1) Receiving Email With Attachments

a) Unsafe File Types. Never Open Any Email Attachment With Any Of The Following File Extensions:

File .Bat

File.Com

File.Exe

File.Vbs

b) Unknown File Types. Never Open Any Email Attachment Or Internal Email Link With A File-Type Extension You Do Not Recognize.

c) Microsoft Document Types. Never Open Any Email Attachment Or Internal Email Link With A Recognized Microsoft Document Type (E.G., .Doc, .Xls, .Ppt) Even From <u>Someone You Know And Trust</u> Without First Running An Updated Virus Scan Program On It.

d) Ask For Plain Text. If You Receive A .Doc, .Wpd, .Xls Or Or Other Unsafe File Type As An Attachment, Even From Someone You Know, Ask Them If They Will Convert It To .Rtf, .Txt Or .Cvs And Then Resend

It To You. Then Delete The Original Email And Attachment.

e) Apparently Safe File Types. *Apparently Safe* File Types Include:

- .Gif, .Jpg, .Tif, .Bmp, .Mpg, .Mp3, .Avi And Other Recognized Multimedia File Formats
- .Txt, .Pdf, .Rtf

f) Delete Attachments. Make Sure To Configure Your Email Client So That It Always Deletes Email Attachments When You Delete The Email It Came With. Also, Make Sure That If Mail Attachments Are Automatically Moved To A 'Trash' Folder When The Email Is Deleted, That The Folder Is 'Emptied' Each Time You Quit The Program. Otherwise Dangerous Files May Be Left Stored Indefinitely In Your Email Attachments Directory Or And/Or Your Trash Directory.

g) Disable Email 'Executables'. In Eudora, Under Tools / Options / Viewing Mail, Make Sure To Disable (Unclick) "Allow Executables In Html Content."

2) Sending Email With Attachments:

a) Avoid Sending Attachments If The Same Information Can Be Sent As Plain Text Or Rtf.

b) Rather Than Sending A .Doc File As An Attachment, It's Often Best To Cut And Paste The .Doc Content Into Your Email As Text.

c) You Can Also Convert .Xls Files To .Csv (Comma-Delimited Format) Before Sending, Thus Minimizing The Risk Of Spreadsheet Macro And

Script Viruses.

d) Only If It Is *Essential* To Retain Document Formatting, Embedded Objects, Etc., Should You Or Your Correspondents Send Unsafe File Types -- And Then Only If You Have Recently Run An Updated Virus Scanning Program That Includes Protection From Macro Viruses.

e) If You Need To Share Formatted Documents With A Group Or Committee, Consider Converting Them To Html And Posting Them To An Appropriate Location In Swift Or web.

3) Getting security information up to date abut email .

4) Other noting of scurity:

a) Don't run programs of unknown origin

b) Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network

c) Disable Java, JavaScript, and ActiveX if possible.

Make regular backups of critical data: Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store the backup disks somewhere away from the computer.

d) Make a boot disk in case your computer is damaged or compromised

To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk which will help when recovering a computer after such an event has occurred. Remember, however, you must create this disk before you have a security event.

Finally for email security I will remember all to follow the Email Security Guidelines because you don’t know what kind of information will be in you computer and the important of it and don’t know who want the get information for your computer and who will used it.