

Safety Mail

www.aoema.org



Not feeling safe
in the online world?

Use this guide to communicate
safely on the internet.



Safety Mail

Contents

INTRODUCTION

Page 3

THE 2-MIN "SAFETY MAIL" TEST

Page 4

COMMUNICATING ON THE INTERNET

Page 6

GETTING THE MOST FROM BUSINESS E-MAIL

Page 8

SECURITY FIRST AND FOREMOST

Page 13

DOING IT RIGHT

Page 20

POLICY AGENDA

Page 24

RESOURCES

Page 35

The Internet has become an important communication tool for the 21st Century. With more than 300 million people worldwide taking advantage of this exciting phenomenon, the Internet is nothing short of a revolution. It has changed how we relate to each other and the world around us. We now have access to people, places and information never before available. Businesses and governments are streamlining operations, grandparents are staying in touch with grandchildren living half a world away, school children are communicating with astronauts in

outer space – all over the Internet. The Internet has become ubiquitous, permeating all aspects of life. The Internet is literally changing our way of life.

You may, however, have some concerns about venturing into the online frontier. We hear about viruses, Trojans, invasion of privacy, lack of consumer protection, “dot.com scams” and even something called “web bugs” – all reasons to be concerned. However, this is the way of the future and it will become increasingly difficult to ignore the online world. Your best defense against these potential problems is to learn how to **prevent** them from occurring in the first place.



Introduction

3

E-mail has become an indispensable business tool that most of us would find hard to be without. Regardless of the type of work or the size of an organization, e-mail is considered to be the most effective and efficient form of communications today. As a business-critical application, e-mail can deliver great benefits and an improved bottom line. There are, however, potential problems, such as viruses, system hacking, spam, confidential information leaks and copyright infringement. But you can guard your company against these threats by following the advice in this booklet and taking action today.

“SafetyMail” is a companion volume to “SafetyNet” – a practical guide that answers four critical questions everyone needs to know to feel safe in the online world:

- How do I secure my computer?
- How do I protect my personal data?

- How can I trust online transactions?
- How do I avoid Internet trouble, traps and scams?

While “SafetyMail” can be a valuable resource for anyone using e-mail, it is expressly intended for business users of e-mail and includes the following sections:

- MESSAGING STRATEGIES
- MARKETING STRATEGIES
- THREATS
- GUIDELINES
- POLICY CONSIDERATIONS

This booklet targets company executives and senior staff responsible for developing an e-mail policy for their organization. All issues that need to be addressed by a policy document are included, along with recommendations. For the broader business audience, this resource identifies best practice guidelines for realizing the greatest potential from e-mail and provides advice on how to **prevent problems before they happen**.

For more information and updates on all subjects, including specific references for individual APEC economies, refer to www.aoema.org/safetymail.

TAKE THE 2-MINUTE "SAFETY MAIL" TEST AND AVOID ONLINE TROUBLE BEFORE IT HAPPENS.

- | | YES | NO | |
|--|--------------------------|--------------------------|---------|
| Do you have anti-virus software installed? | <input type="checkbox"/> | <input type="checkbox"/> | See p.8 |
| Do you have the most recent version of the anti-virus software? | <input type="checkbox"/> | <input type="checkbox"/> | See p.8 |
| Do you know if your virus definitions up to date? | <input type="checkbox"/> | <input type="checkbox"/> | See p.8 |
| Do you have a firewall installed on your personal computers as well as your internal server? | <input type="checkbox"/> | <input type="checkbox"/> | See p.8 |

Are your Internet communications putting your organization at risk? You may not think so or you may not be aware, but you won't know until you take our 2 minute "Safety Mail" test. Take two minutes out of your busy schedule and save many hours and a lot of money by preventing trouble from happening in the first place. E-mail problems can potentially affect your organization, management and employees.

4

The 2-Min "Safety Mail" Test



- | | | | |
|---|--------------------------|--------------------------|----------|
| Do you have the latest version of the firewall software? | <input type="checkbox"/> | <input type="checkbox"/> | See p.8 |
| Do you have a written policy document for your employees that explains how they should conduct Internet communications? | <input type="checkbox"/> | <input type="checkbox"/> | See p.6 |
| Do you educate your employees on this policy and its ramifications? | <input type="checkbox"/> | <input type="checkbox"/> | See p.28 |
| Do you have a formal method for archiving business e-mails? | <input type="checkbox"/> | <input type="checkbox"/> | See p.27 |
| Do your business messages contain disclaimers and contact details? | <input type="checkbox"/> | <input type="checkbox"/> | See p.22 |
| Are procedures in place for managing e-mail addresses of former employees? | <input type="checkbox"/> | <input type="checkbox"/> | See p.24 |



This test is very simple – if you answer "NO" to any of the following questions, it is highly recommended that you read this booklet and become more familiar with these topics.



Safety Mail

Topics and Policy Considerations

MESSAGING STRATEGIES Page 6

- E-mail
- Instant Messaging
- Short Message Service
- When there is too much of a good thing
- The three “must do’s” for Internet communication

MARKETING STRATEGIES Page 8

- E-mail Address Data Collection
- Message Distribution
- Referral E-mail Marketing
- Full Disclosure
- Customer Satisfaction
- Internal Testing

THREATS Page 13

- Viruses, Trojans and Worms
- “Snooping” and “Spoofing”
- Social Engineering
- Instant Messaging Worms
- Digital Signatures and Encryption
- “Spam”

GUIDELINES Page 20

- Guidelines for file attachments
- Guidelines for sending e-mails
- Guidelines for participating in mailing list

POLICY CONSIDERATIONS Page 24

Email is an official company record

- Disclaimers on messages
- Intellectual Property and Copyright
- Privacy Considerations
- Message Style and Content

Protecting your information assets

- Archiving policies
- E-mail use outside the office
- Keeping organizational information private

Employee rights and responsibilities

- Message Response Times
- Temporary Employees
- Harassment
- Monitoring e-mails
- Participation in e-mail lists
- Personal use of organizational resources
- Training
- Transfer and retirement of employees

Additional messaging strategies

- Instant Messaging
- Short Message Service (SMS)

ADDITIONAL RESOURCES Page 35



Communicating on the Internet



MESSAGING STRATEGIES

E-MAIL

With the proliferation of the Internet, e-mail has become an indispensable business tool, with businesses of all sizes using e-mail today for more effective and efficient communications. E-mail is simple to use, but also simple to abuse. Many companies fail to realize this fact, neglecting to manage and control the environment until something goes terribly wrong.

At minimum, an e-mail problem can reflect poorly on an organization's reputation. In the extreme case, your company could be liable in a multi-million dollar lawsuit. This may sound alarmist, but it does happen and it generally makes headline news when it does. But it doesn't have to happen and almost never does when individuals and companies properly address the issues and put appropriate management controls in place.

The positives of using e-mail far outweigh the negatives, and like other aspects of your business environment, management is the key to success.

INSTANT MESSAGING

Instant messaging is a service that lets users know when designated contacts are on line and allows them to communicate instantly, usually by exchanging typed messages in a separate window. With instant messaging, a list of contacts you wish to communicate with is created; when any of those people come on line, the service alerts you of their availability and if desired, immediate interaction is possible.

Until recently, Instant Messaging (IM) has mainly been used for personal communications. Software packages are now available that let companies set up their own IM service for both internal and external communications.

IM in a business environment can be extremely useful and is fast becoming a popular communications channel for managing internal affairs as well as providing a personal touch when dealing with customers. However, just as with e-mail, IM needs to be managed and policies should be in place to address the unique nature of this exciting form of online communications.

SHORT MESSAGE SERVICE

SMS (Short Message Service) lets you send messages up to 160 characters in length to digital phones (mobile/cell), using either a computer or another digital phone. There are numerous ways businesses are using this facility today, including:

- *Notifying an employee of a voice mail message*
- *Notifying a salesperson of an inquiry and contact details to return the call*
- *Notifying a doctor of a patient with an emergency problem*
- *Notifying a service person of the time and place of their next job*
- *Notifying a driver of the address of an unscheduled pickup*

In some parts of the world, SMS is now an integral part of life. Business people, students and parents have all found ways to use this facility to enhance their communications. Many phone companies now provide services to businesses that enable them to broadcast SMS messages to employees and customers.

With a little bit of creativity, SMS quickly becomes an effective communications channel for business environments, offering efficiency gains and potential dollar savings. Don't think of 160 characters as a limitation – many small businesses around the world have come to rely exclusively on SMS to manage all their business communications. Of course, just like e-mail and IM, SMS requires a management policy.

WHEN THERE IS TOO MUCH OF A GOOD THING

While e-mail, IM and SMS are effective communications strategies and certainly have a place in your organization, they should be used judiciously. There are times when a phone call or face-to-face meeting is far more appropriate. These technological advances should be considered as part of an overall communications

strategy and managers should be alert to any employee with too much dependence on any particular form of communication. As consumers, we all know how frustrating it can be when no one in an organization is available to respond over the phone and voice mail messages go unanswered.

THE THREE “MUST DO’S” FOR INTERNET COMMUNICATION

There are three things that **MUST** be done in any organization that uses the Internet. These three things must be done regardless if you have two employees, two hundred employees or two thousand employees:

must do #1 – Develop a policy for e-mail communications

The first step is to develop a policy and then it must be kept up to date, as changes in technology and usage often dictate changes. A policy needs to be a written document and **MUST** apply to everyone in the organization equally.

must do #2 – Educate everyone in the organization

People can't be expected to follow the rules unless they understand what they are. Make sure that everyone understands that a policy exists and that it **MUST** be adhered to. Many companies now require employees to sign the actual policy document to indicate that they are aware of its existence and promise to follow the rules as stipulated.

must do #3 – Manage and enforce the policy

It may be necessary to take advantage of monitoring software available today to ensure that company policy is being adhered to. While this may seem intrusive and somewhat heavy handed, it is usually the best way to protect the integrity of both company and employees. If monitoring software is installed, all employees **MUST** be made aware of its existence and clearly understand how it works.



Getting the most from business e-mail



MARKETING STRATEGIES

E-mail is often referred to as the “killer application” of the Internet, with nearly 95% of the more than 600 million Internet users worldwide using e-mail in some capacity. Business e-mail has emerged as an efficient, economical and personalized method for companies to reach their most valuable asset, their customers. When compared to traditional direct marketing, e-mail marketing is faster, measurable and far more cost effective. The downside, of course, is the meteoric rise in “spam” and the need for businesses to not be seen as “spammers.” It is a fine line between legitimate e-mail marketing and “spam.”

An effective and responsible e-mail marketing strategy takes a consumer-based approach, where the consumer’s needs are understood and addressed. According to AOL and other Internet Service Providers (ISPs), somewhere around 70% of all e-mails today are classified as “spam.” Is it any wonder the consumer is fed up with unsolicited e-mails? These unwelcome messages are also the most common source of viruses. With these facts in mind, permission and privacy must be the cornerstones of your e-mail marketing program. This is the only way to develop customer loyalty and establish business integrity in the online environment.

There are many e-mail marketing strategies and techniques, too numerous to explain in this booklet. However, there are some basic guidelines and best practice principles with respect to permission and privacy that are extremely important and that is what we will focus on. Use this section to help you design an effective, but responsible, e-mail marketing strategy, one that is based on customer permission.

E-MAIL ADDRESS DATA COLLECTION

Before you can start an e-marketing program, you first need to develop an e-mail database or list of e-mail addresses to mail to. This must be done with customer permission. Gaining permission requires considerable effort, time and money, and you may wonder why it is necessary since permission isn't required before sending advertising through the postal service.



There are two very good reasons. One, it is now law in some jurisdictions. Secondly, many ISPs will terminate service to customers they believe responsible for sending commercial or bulk e-mails without permission. Some key points to keep in mind:

- Never collect e-mail addresses without the owner's consent. Do not, under any circumstances, take addresses from chat rooms, bulletin boards, directories, web sites, or any other publicly available source. This is precisely how spammers create their e-mail databases.
- Don't use "must fill" fields. Many web sites present users with forms that require information they may not wish to divulge. In other words, the "submit" button will not activate until all "must fill" fields are filled in. Not only does this anger users, but you run the risk of collecting garbage data.
- Always send an "opt-in" confirmation. When a user willingly submits his e-mail address for marketing purposes (opt-in), a confirming e-mail should be sent immediately. Usually this is done by auto-responding software. While not foolproof, a confirmation e-mail generally removes the risk of a forged or accidental registration. It is now best practice to not just send an "opt-in" confirmation, but to request that the user re-confirm permission to use his e-mail address. This lets a customer change their mind and helps build goodwill.
- Always log date, time and IP address of each e-mail address collected. This is very important in terms of new legislation in some jurisdictions, as you may be required to prove that a particular customer willingly submitted his e-mail to a marketing database. An audit trail can be very useful should your company need to defend its position in response to legal action.



MESSAGE DISTRIBUTION

It is important to format your e-mail message so it is not thought to be "spam." The following points should be heeded:

- Never falsify header information. Information contained in the header enables a user to determine the origin of an e-mail - domain, IP address, delivery path, etc. Spammers use fake information in the header to avoid detection by

consumers and law enforcement. Legitimate e-mails need to demonstrate credibility and that includes clear and accurate headers.

- Never falsify the subject line. While marketing involves creative and catchy phrases, the basic “truth in advertising” doctrine applies. Never mislead your customers intentionally or unintentionally. Words like “hi” in the subject line are very unprofessional (they are also used by spammers to make recipients think the e-mail is from a known acquaintance).

Always provide an “opt-out” option. Each and every e-mail message must include an unsubscribe option to allow customers to change their mind.

Always honor unsubscribe requests. You must ensure that your system can manage “opt-out” requests and responses should be immediate.

REFERRAL E-MAIL MARKETING

When used in a responsible manner, referral e-mail marketing can be a powerful community-building, brand-building, and list-building tool. However, it doesn’t take much for a legitimate campaign to be perceived as “spam” and this can reflect negatively on your company and your brand. Some important steps to take include:

- Make sure it’s appropriate in the first place. Determine whether you should even mention forwarding at all.
- Remind customers to forward “appropriately.” Ask customers to think twice before submitting a referral. If you end up sending e-mails to individuals who don’t want to receive them, your e-mail campaign will ultimately be perceived as unsolicited. Refrain from offering rewards, as this tends to encourage inappropriate forwarding of names.
- Always include referrer name. Use either the “from” or “subject” line to name the person who requested the message be forwarded. Without the referrer’s name, the recipient can only assume that this is a “spam” e-mail.
- Permission is not transferable. E-mail addresses submitted by referral must not be considered as “permission addresses” and used in future campaigns.
- Always log the date, time and IP location. Again, this is extremely important should your company need to defend against legal charges.

FULL DISCLOSURE

Customers will not remain loyal to your company or brand unless they can trust you. This means honesty and full disclosure on several matters:

- Privacy policy. Privacy of personal information has become a significant issue in the world today. The European Union has developed quite stringent rules with regards to

privacy in the electronic environment. Many others are following their lead. The breadth of information covered by these privacy regulations is quite broad and organizations will need to identify the specific information collected from their customers and how they will be using it before creating an organizational privacy statement. Be specific – the customer needs to understand exactly what information is being collected and what will be done with it.

- Information tracking. If you are doing any kind of tracking of an individual's web behavior – click-through tracking, cookies, bugs, implanted coding – you should disclose this activity to your customers.
- Contact business details. Customers will have a much higher level of confidence in your company if you provide background information and complete contact details, including physical address and phone and fax number. Consumers are often uncomfortable with companies that provide only an e-mail address, causing them to wonder if they are dealing with a legitimate enterprise.

CUSTOMER SATISFACTION

This is a list of general tips for creating better customer satisfaction during e-mail marketing campaigns:

- When sending multiple e-mails, only the sender and recipient addresses should be displayed. Do not show the entire recipient list on each message. If an e-mail is intercepted, the recipient list could be used by spammers.
- Consider the time of day you are sending out your messages – some people have their messages forwarded to mobile/cell phones after hours and certainly will not appreciate advertising at 3am.



- Considering the growing use of digital phones and handheld devices, message length becomes critical.
- If you outsource e-mail marketing services, you must manage all these issues with that company. Don't leave this to chance or assume that outsourcing companies will necessarily do the right thing.
- Make certain you are not including information in your e-mails that is protected by copyright. Get permission.
- E-mails from customers should always be responded to as quickly as possible. You may need to increase staff, particularly during marketing campaigns.

- Make sure that the right person in your organization responds to customer complaints. Training for response teams may be required. It is also important to keep detailed records and a log to record time and date of e-mail exchanges should a complaint escalate in intensity. An audit trail can be very useful and necessary should a complaint end up in the hands of lawyers.
- Remind your customers why they are receiving your e-mail. Tell them right at the beginning of the message that they are receiving this e-mail because they asked to be on a list and remind them they are a valued customer.
- Minimize the number of clicks it takes to respond to your e-mail purpose - a purchase or information regarding new products, etc. If the e-mail redirects customers to your website, have the link take them directly to a customized "landing page," not your homepage. Get right to the point on that page. Don't let potential confusion or frustration set in.
- Make sure the timing of your e-mails fit strategically with your target market.

INTERNAL TESTING

One of the best ways to test your campaign prior to launch is to use your own e-mail and go through each step yourself to test both content and systems:

- Use an assortment of "spam" filters to test your own marketing e-mails.
- Carefully check the "from" and "subject" lines and assess them with your customer hat on.
- Audit your subscription process to ensure that it offers a double check "opt-in" process.
- Check your unsubscribe ("opt-out") process – make sure it works properly and in a timely fashion.
- Test your message and "landing page" carefully. Check every link to ensure it is working properly. There is nothing worse than a broken link.
- Be certain that your web server can deal with increased traffic.
- Make sure you can handle an increase in product fulfillment if the goal of your marketing campaign is new sales.





Security First and Foremost

13

THREATS

VIRUSES, TROJANS AND WORMS

As e-mail continues to grow in popularity with individuals and businesses, it has also come to the attention of those who create viruses and are hoping to spread them far and wide. The criminal element is constantly looking for opportunities to do harm and unfortunately, they have found e-mail and IM to be effective channels for their misdeeds. Again, we must stress that while there is a threat, there is a way to prevent trouble before it happens.

Prevention is the operative word. Take the necessary steps to ensure that viruses can't enter your computer in the first place and become vigilant in following procedures regularly, as new threats and creative methods are discovered daily. We have all read about virus attacks in the newspapers, but if every user on the Internet

were to follow these simple steps, we could actually put these people out of business. They would quickly stop their nefarious activities if they couldn't cause trouble.

One of the "innovations" that virus creators have made recently is to include in the virus program the capability to send e-mails to all parties listed in your e-mail address book, potentially spreading the infection to family, friends and business associates. Just remember, all of this can be prevented and will eventually stop if the following advice is heeded.

RECOMMENDED ACTION

- Anti-virus software must be installed and virus definitions updated regularly, preferably, automatically.
- Be extremely careful when opening file attachments. As mentioned above, virus programs can send messages that appear to come from people you know. Therefore, ensure that the indicated sender of the attachment has actually sent it. This is a very critical point since most of the time it is only when an infected attachment is opened that the virus actually takes effect.
- Even seemingly innocuous files can hide a virus. People are often caught by trying to open files they think contain a picture or joke. Remember the rule - don't open any file until you can confirm what it is and who sent it, and then only open it after you have subjected it to analysis by an up-to-date anti-virus program.
- Some examples of suspicious e-mails include:
 - * e-mails from unknown sender
 - * e-mails with strange or suspicious subject titles
 - * e-mails with names that include non-alphabetic characters
 - * e-mail subject titles in foreign languages (not in your native language) unless you have an established relationship with someone who speaks that language
 - * Unexpected e-mails with attached files
- To protect against viruses capable of sending e-mails to address book entries, install firewall software that automatically checks all outgoing e-mails for suspicious activity.
- For e-mails with suspicious files attachments, both the file itself and the e-mail to which it is attached should be put in your recycle bin and then emptied.
- Before opening any file attachment, it is always best to have your anti-virus software program check it first.
- When sending an attachment in an e-mail, be sure to send information about the file to let the recipient know it is legitimate.
- Don't pass on e-mails reporting virus threats as this is often a hoax and sending it on will just perpetuate the hoax and clog up e-mail servers around the world.
- The latest versions of anti-virus software can check both incoming and outgoing messages for viruses. For the safety of everyone on the Internet, be sure this setting is in fact turned on.



SNOOPING AND SPOOFING

ABOUT SNOOPING AND SPOOFING

(Snooping) If you fail to protect your e-mail password, someone could read your messages. This could be damaging in a corporate environment where e-mails are considered confidential business matters. Even in the home environment, it is best practice to not reveal your passwords.



(Spoofing) It is possible for people to send mail in someone else's name and this is called "spoofing." There is nothing that can be done about this other than to be aware that it can happen and to

report it to your Internet Service Provider (ISP) or IT department if you find that it has occurred. You will know that you have been "spoofed" if you receive a rejection notice for an e-mail that you did not send.

The Internet e-mail system we use today was never meant to be used all over the world in an open environment. It started as a system for academics to easily communicate with each other as a closed community. With this in mind it is easy to understand why it is so insecure and open to abuse.

RECOMMENDED ACTION

- Passwords must be protected. Choose passwords that are at least 8 characters in length and a combination of alphabetical and numeric. No matter how good the password is, however it still needs to be changed frequently (not longer than 45 days).
- There is no reason to share passwords with anyone. In other words, **DO NOT TELL ANYONE** what your password is.
- Passwords must not be written down, as someone could read it and then use it.
- Ensure that employees understand it is forbidden to read a co-workers e-mail without their permission.
- Be alert for evidence of someone "spoofing" your e-mail address and report this activity if it does occur.
- Employees must not spoof the e-mail of other people inside or outside the organization.
- Employees must not try to disguise or hide their identity when using the organization's e-mail system.

WHERE TO GO FOR HELP AND MORE INFORMATION

[www.cert.org/tech_tips/
email_spoofing.html](http://www.cert.org/tech_tips/email_spoofing.html)

SOCIAL ENGINEERING

ABOUT SOCIAL ENGINEERING

Term used to describe the exploitation of weaknesses in people. It is the art of tricking someone into giving out personal information (like passwords) that could compromise system security.

Illicit e-mails are sometimes used in an effort to obtain personal or sensitive information by appearing to be legitimate. This type of attack is commonly referred to as a “social engineering attack,” and more specifically known as “Phishing.” An attack of this nature typically directs unsuspecting users to a bogus web site where people are encouraged to enter sensitive information. What makes this so insidious is that the web site may actually look like the web site of a legitimate company and the initiating

e-mail will have graphics and design familiar to the recipient. The “phisher” then takes the information that has been entered and uses it illegally.



RECOMMENDED ACTION

From the United States Government Federal Trade Commission (FTC) site the following recommendations are made:

- If you get an e-mail that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm billing information, do not reply or click on the link in the e-mail. Instead, contact the company cited in the e-mail using a telephone number or web site address you know to be genuine.
- Avoid e-mailing personal and financial information. Before submitting financial information through a web site, look for the “lock” icon on the browser’s status bar. It signals that your information will be secure during transmission.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Report any “phishing” activities to the FTC (www.ftc.gov) or CERT (www.cert.org)

**WHERE TO GO FOR HELP
AND MORE INFORMATION**

www.kb.cert.org/vuls/id/652278

IM WORMS

ABOUT IM WORMS

Instant Messaging, while useful, is not a private system. Anything written during an Instant Messaging session must be thought of as open to everyone on the Internet. It is possible for people to use Instant Messaging sessions to



harass those involved in the “conversation.” The best way to protect yourself from this intrusion is to select the appropriate “blocking” setting on your IM software.

While Instant Messaging can be a useful application in a business context, it can make you more vulnerable to threats from Trojan programs, worms, viruses and social engineering attacks. If your organization doesn’t intend to use IM for business communications, it is best to specify in your policy document that IM is not permitted. If your organization does not intend to use IM, the following recommendations should be followed.

RECOMMENDED ACTION

- Do not give out personal information during instant messaging sessions.
- Do not download files during instant messaging sessions.
- If you are uncomfortable about the security threats posed by IM worms, it is best to disallow employees from using instant messaging.
- Firewall software must be installed and settings specifically concerned with IM threats need to be selected.
- It is highly recommended that organizations use enterprise-wide Instant Messaging software products for tighter controls and a safer environment.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.cert.org

DIGITAL SIGNATURES AND ENCRYPTION

ABOUT DIGITAL SIGNATURES AND ENCRYPTION

The general rule is not to send sensitive information (e.g. credit card details or employee background information) via e-mail. There are, however, times when this is unavoidable and in those situations you should take advantage of digital signatures and encryption. The Internet e-mail system is completely open to the world and sending sensitive information in an open e-mail is like sending it on a postcard.

Major e-mail software packages have the facility to digitally sign messages and even encrypt them if desired. However, some governments consider encryption to be an illegal technology and consequently you will need to check the laws for both the sending and receiving jurisdiction before encrypting a message.



RECOMMENDED ACTION

- Develop an organizational policy on digital signatures and encryption to identify the circumstances under which they should be used.
- For employees likely to need digital signatures, make sure they fully understand the technology, understand how the company intends to use them and have access to their own company-approved digital signature.
- Identify the most appropriate Public Key Infrastructure to manage your digital signatures in your organization.

WHERE TO GO FOR HELP AND MORE INFORMATION

[www.apectelwg.org/apecdata/
telwg/eaTG/EA-text.pdf](http://www.apectelwg.org/apecdata/telwg/eaTG/EA-text.pdf)
searchsecurity.techtarget.com/

SPAM

ABOUT SPAM

Spam or unsolicited commercial e-mail, has been growing for some years now. Some users report that over 70% of their e-mail is "spam." For businesses today there are several considerations when thinking about "spam" issues, relating to both incoming and outgoing e-mail.



1. Incoming e-mail

To have employees individually deal with their "spam" causes a significant loss in productivity. Another problem is that "spam" is often offensive to the recipient, making it difficult for them to effectively deal with it.

To enhance productivity and to avoid a difficult situation, it is far better to deal with "spam" on a company-wide basis and to keep it out of employee mailboxes. Some employees have already taken legal action against their employers for not taking

appropriate steps to control "spam." To reduce your company's exposure to workplace relations issues, it is important to fully address these issues and consider installing software that can provide the necessary protection for a company-wide e-mail system.

2. Outgoing e-mail

When dealing with customers, companies must be sensitive to the amount of "spam" people receive today and keep e-mail to a minimum. Even with "opt in" e-mail newsletters, recipients can become frustrated with companies who send too many e-mails. It can be a fine line between what is acceptable and what isn't, but a company must learn how to manage the situation if it is to keep customer loyalty.

RECOMMENDED ACTION

- Establish a policy for dealing with "spam" and ensure that all employees follow it.
- Address the issue of "spam" control in your company's e-mail system to prevent offensive e-mails from ever getting into employees' mailboxes.
- Develop a policy and rules for outgoing e-mail to ensure that your organization is not considered to be "spamming" customers.

WHERE TO GO FOR HELP AND MORE INFORMATION

<http://spam.abuse.net>

www.cauce.org



Doing it Right



Guidelines for File Attachments

- Nearly everyone's e-mail box has a size limitation imposed by their ISP or in-house mail system. Therefore, if you try to send a large file to someone, it may be rejected due to an e-mail system overflow.
- You should also be aware that many users don't have access to high speed lines and large files can cause significant delays or problems in the process of receiving these e-mails over dial-up connections.
- Avoid sending large files. A file over 150 Kilobytes is generally considered to be too big.
- When sending a large file, be sure to optimize its size by using compression software. It may be necessary to distribute it over several e-mails by sending it in sections.
- It is important to warn the recipient in advance that you intend to send a large file. The person may be out of the office and you could be unnecessarily clogging their mailbox with large files they won't be able to deal with until they return.
- The best method for sending large files is to upload the file to the Internet and give the recipient an address where they can download the file. This approach allows the recipient to download the file at a time when it is most convenient for them. Contact your ISP or IT department for instructions on how to do this.

- Unless you have installed either a hardware or software encryption device, you should assume that messages exchanged over the Internet are not secure. If it isn't appropriate on a postcard, then it isn't appropriate for email!
- If you are forwarding or re-posting a message you've received, do not change the wording. If the message was a personal message to you and you are forwarding it on to an individual or a group, you should ask permission first.
- Never send chain letters via electronic mail as they are clearly forbidden on the Internet. Your network privileges may be revoked. Should you happen to receive one, notify your Internet Service Provider (ISP) immediately.
- Be careful when addressing a message or when replying to an email address, as some addresses appear to be that of an individual but are actually being distributed to a list of recipients.
- Use both upper and lower case. It has become convention that if you use all upper case, YOU ARE SHOUTING.

- Use the subject line to express some sense of what your message is about. This makes it easier for the recipient to effectively sort through incoming mail, set priorities in terms of critical messages requiring immediate attention and filing of messages for future reference.
- You may not always have time to respond fully to a message at the time you actually receive it. Far better to send a brief email to let the sender know you did receive the message and a quick note to indicate that you will send a longer reply later.
- Unsolicited email advertising is unwelcome and in some contexts illegal.



Guidelines for sending E-mails

21

- Some people like to use "smiley faces" to indicate a tone of voice or an attitude. A happy face is :-) and an unhappy face is :- (and is achieved by combining keyboard symbols. It is best to use them sparingly if you are going to use them at all and keep in mind that some cultures may not understand their meaning.
- For people who routinely have to deal with a heavy load of emails, they appreciate being made aware of any specific emails that are lengthy and might require extra time to deal with them. Generally speaking, a message over 100 lines is considered long and it is a good idea to use the subject line to notify the recipient of this fact.
- Try to be brief with your messages, but at the same time be careful you aren't so brief as to be terse. A terse message can often be considered rude or angry.

- It is possible with today's messaging systems to request "read receipts" or attach "urgent flags" to messages. However, having these facilities turned on all the time dilutes the effectiveness of this strategy. It can also cause annoyance to recipients if used indiscriminately.
- To avoid creating long and unwieldy email recipient lists, use the "blind carbon copy" (BCC) convention when sending messages to large groups.
- Use Urgent flag sparingly.

- Before you actually get involved in a mailing list or newsgroup, it is a good idea to spend one or two months getting to know the group before you post anything.
- Inappropriate behavior by users is not the fault of the system administrator. However, it is the responsibility of the system administrator to take action if someone has overstepped the boundaries of proper behavior.
- Once you press the “send key” it is too late to rescind your comments. Be very careful not to post comments that you might regret later.
- Keep your messages brief and to the point.
- Some lists welcome advertising while others have strongly stated rules against it.
- When replying to a message or posting, it is always best to make sure you include enough of the original text to provide context. Otherwise your response may not make sense.

- Send subscribe and unsubscribe messages to the appropriate address.
- Consider unsubscribing or setting a “no mail” option (if available) when you cannot check your email for an extended period.
- When sending a message to more than one mailing list, especially if the lists are closely related, apologize for cross-posting.
- Never give out your user ID or password. System administrators that need to access your account for maintenance or to correct problems will have full access to your account without having to request information from you.

Guidelines for participating in Mailing Lists



- Be careful when sending personal responses. If you simply click on “reply to sender” you are most likely sending your reply to the entire mailing list and not to a single recipient as intended.
- If by some chance you do accidentally send a personal message to the entire group, be sure to immediately send an apology both to the individual and to the group.
- If you have strong feelings about what someone else has posted, express your feelings in personal emails.
- Don’t get involved in what is often called “flame wars.” Avoid posting or even responding to incendiary material. Leave this type of problem to the list administrator.
- Avoid non-standard fonts, as they will display differently on different systems, making it difficult to read text files.

- If only numbers are used for dates, day and month could be confused. Avoid misunderstandings by using the following date format: 11 Feb 2004.
- Acronyms can be used to abbreviate when possible, however messages that are filled with acronyms can be confusing and annoying to the reader. Some common acronyms are:
 - IMHO** = in my humble/honest opinion
 - FYI** = for your information
 - BTW** = by the way



Safety Mail

Policy Considerations

Email is an official company record

Disclaimers on messages	Page 25
Intellectual Property and Copyright	Page 25
Privacy Considerations	Page 26
Message Style and Content	Page 26

Protecting your information assets

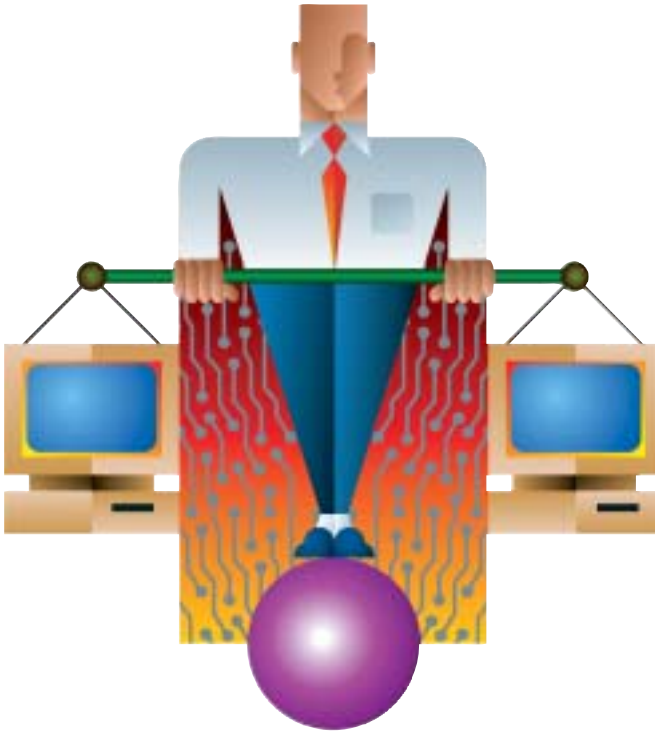
Archiving policies	Page 27
E-mail use outside the office	Page 27
Keeping organizational information private	Page 28

Employee rights and responsibilities

Message Response Times	Page 29
Temporary Employees	Page 29
Harassment	Page 30
Monitoring e-mails	Page 30
Participation in e-mail lists	Page 31
Personal use of organizational resources	Page 32
Training	Page 32
Transfer and retirement of employees	Page 33

Additional messaging strategies

Instant Messaging	Page 33
Short Message Service (SMS)	Page 34



Policy Agenda



POLICY CONSIDERATIONS

This section will help you address the important issues related to an Internet communications policy agenda. All organizations should have a formal, written document, signed and agreed to by all employees. This is the only way to protect the legal rights of both company and employee. While some of the topics covered in this part were discussed in previous sections, it is important that all policy-related considerations be included to ensure a comprehensive and complete resource.

Email is an official company record

DISCLAIMERS ON MESSAGES

Once a message leaves your organization, there is no way to know how the information inside the message will be used or interpreted by the recipient. Additionally, you won't know if the message is ultimately read by people other than the intended recipient.

Policy Considerations

- Ensure that your e-mail policy specifies that a disclaimer must be included on the bottom of all messages sent by the organization.
- Clearly state that the information transmitted is for the use of the intended recipient only and may contain confidential and/or legally privileged material.
- Indicate that the information is not to be re-transmitted, disclosed or disseminated without the consent of the author of the message.
- Indicate an e-mail and phone number so that anyone receiving the message in error can report it or send it back. This has been standard practice with fax cover sheets.

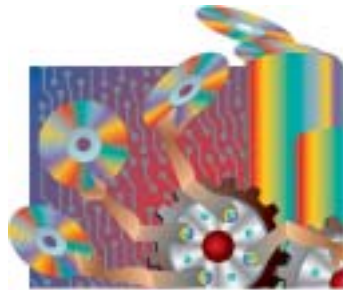
INTELLECTUAL PROPERTY AND COPYRIGHT

The Internet has given us access to more information than ever imagined, and together with computers and word processing, we are able to publish material faster and disseminate it further. Employees of an organization must understand the intellectual property ramifications of publishing material on the Internet or sending it via e-mail.

Liability for any breaches of copyright made by employees rests with the organization. Clearly this issue must be addressed by a policy document and employees need to be instructed on what they can and can't do with respect to using information they find on the Internet.

Policy Considerations

- All employees must understand the concept of intellectual property and copyright and must be educated in these issues. Several lawsuits have resulted in finding companies and individuals liable for infringement of intellectual property rights and copyright. This is a serious matter with serious consequences.
- Instruct employees not to quote information in an e-mail that has been written by someone else unless explicit permission is given and the original author is acknowledged.



PRIVACY CONSIDERATIONS

Again, it is important to stress that e-mail over the Internet is not secure, so any information sent must be considered open to the world. If, without permission, you send personal information about someone to a third party, you could be held liable for invasion of privacy and sued.

You must also be very careful when sending messages to large groups. By including a list of e-mail addresses in the "TO" or "CC" you could be unintentionally providing someone with a list of addresses to "spam."

Policy Considerations

- When sending personal information, either in the e-mail text or within a file attached to the e-mail, you should encrypt the information. (Talk to your e-mail support people to find out how to do this).
- When sending an e-mail to multiple people you should use the blind copy or "BCC" facility for the list of addresses. This way the names are not visible to everyone.

MESSAGE STYLE AND CONTENT

Any correspondence that an organization enters into, whether it is on paper or in electronic form can be considered as a legal commitment by the organization to the contents of the correspondence. Therefore, all correspondence must be taken seriously, including e-mail exchanges, and rules must be in place to protect the company.

Clearly not all correspondence takes the form of a contractual agreement, so correspondence categories will need to be established and appropriate rules defined for each category.

Policy Considerations

- Include procedures that cover the various types of correspondence. Be especially careful when defining the rules of conduct for contractual discussions over e-mail.
- Both content and style are important considerations. Where possible, simply adapt the style used for paper-based documents. In the rare instance when this isn't possible, make sure you seriously consider the legal ramifications of the electronic document in question and review it carefully. You may need to get legal advice.
- It is also important to establish a management approval process for documents sent electronically that commit the organization to a legally-binding course of action.



Protecting your information assets

ARCHIVING POLICIES

E-mail and instant messages are now considered to be company records and it is well known that company records must be retained according to specific laws. Don't confuse back-ups with an archiving process: Back-ups are designed to enable an organization to recover from computer disasters, while archived files preserve business documents for future reference, in accordance with government requirements.



An organization should review the types of messages that are sent both internally and externally and decide how best to deal with each type in terms of archiving requirements. Some of the categories you might need to deal with include:

- Administrative correspondence
- Fiscal correspondence
- General correspondence
- Instant Messaging correspondence
- Encrypted correspondence

It would not be necessary to retain all of this correspondence for the same amount of time and it may be deemed unnecessary to archive all categories.

Be sure to include all electronic communications channels in your archive policy. Keep in mind that communication is a two way process and organizations on the receiving end of your correspondence are likely archiving these documents as well.

Policy Considerations

- Develop a policy on how and when employees should submit messages for retention.
- Establish a central point (usually an internal e-mail address) where messages can be sent or copied if they are to be retained. Make it easy to archive.
- Establish rules and policies on how and what employees should retain on their own computer and for how long.

E-MAIL USE OUTSIDE THE OFFICE

E-mail access is simple and easy today, making it possible for employees to stay in touch from just about anywhere. There are, however, important considerations for an organization with respect to employees accessing their business e-mail accounts from locations other than the office.

Two areas of major concern are passwords and log-out procedures. If passwords are not managed properly, there is always a risk, but even more so when traveling. If an employee fails to complete all steps in the log-out process, company e-mail systems could be at risk and open to hacking. At the very least, the next person to use a public access computer would be able to read the employee's company mail.

You should also be cautious when reading or writing e-mails in public areas such as trains, coffee shops, or wireless “hot spots.” It is quite easy for someone to read the information over your shoulder.

Notebook computers, digital phones, and recorded media (e.g. floppy disks, CDs) are at particular risk if stolen or lost, as e-mails and documents can be read by people outside the organization.

Policy Considerations

- When addressing this issue, keep in mind that this is all about the risks associated with accessing the organization from outside the office. Clearly there are risks, but they can be managed and most companies believe the productivity gains outweigh the potential risks.
- Rules for the use of e-mail outside the office should be based on the assumption that mobile/cell phones and handheld devices can easily be lost or stolen.
- Even if the use of company e-mail is permitted outside the office, sensitive information should never be sent outside the confines of the company.
- Employees must be educated on the risks of using e-mail outside the office.
- Automatic forwarding of company e-mail to non-company mailboxes should be prohibited as this can endanger the security of company information by sending it to unknown entities.

KEEPING ORGANIZATIONAL INFORMATION PRIVATE

It is possible for e-mails to be intercepted and the information compromised as they travel through several networks and servers. With the ease of use of information systems today, it is possible for dishonest or careless employees to copy the organization’s information and send it to competitors or other interested parties.

Sensitive information could be sent to an outside mailing list or electronic bulletin boards by disaffected or careless employees. It is also easy for employees to forward e-mails from their company e-mail account to their personal e-mail account.

Carelessness in dealing with e-mail could result in internal messages being sent outside the organization, with unauthorized addresses accidentally or intentionally added to the message.

Policy Considerations

- Confidentiality agreements must be signed by all employees. This is extremely important for all companies, large and small.
- Institute an “active access control” system to restrict important data to designated senior staff.
- E-mails being sent outside the office should be automatically copied to a designated manager.



- Policies regarding the forwarding of internal e-mail to addresses outside the organization must be set.
- Employees must be taught to check the receiver's address when sending e-mails. This is particularly important when using the "reply to all" facility.

Employee rights and responsibilities

MESSAGE RESPONSE TIMES

If your company website includes an e-mail address, designated as either a general contact or specifically named contact, there is an obligation to respond in a timely manner. Not answering e-mail is the same as not answering the phone and your reputation and profits depend on being responsive to all forms of communications.

There are many things that could stop e-mail from getting through. This includes a full mailbox, a mail server that is not operating properly, or an Internet gateway problem (when two e-mail systems are unable to pass e-mails between them). Businesses must ensure that none of these things stand in the way of receiving e-mails.

Policy Considerations

- Your e-mail policy should include a specification for reading and responding to e-mails. Managers must then ensure that these rules are adhered to.
- Make sure that nothing gets in the way of receiving e-mails from valued customers.

TEMPORARY EMPLOYEES

A temporary employee who is brought in for a couple days is not likely to need access to the company e-mail system. However, for any temporary employee expected to use company e-mail, you will need to make them aware of your policy document and get them to sign it. Any employee, including temporary workers, could create liability issues for the organization and the only way to protect against potential problems is to have all employees read, understand and sign the policy document.

Policy Considerations

- To assist all managers, a policy for allocating e-mail addresses to temporary employees must be defined.
- One of the issues often raised by employers is whether to allocate a department-level address or a personal address for temporary staff. This is a matter of opinion, but both options should be considered when addressing this particular issue.
- Make sure all temporary employees who are expected to use company e-mail accounts have a full understanding of your policy document and have signed it.



HARASSMENT

Nearly everyone with an e-mail account has received a joke from a friend via e-mail. The Internet makes it exceedingly easy for people to share jokes, cartoons, stories and photographs they find funny or interesting. The problem is that not everyone agrees on what is humorous or interesting, and while a sexually explicit joke may be funny to some, it may be offensive or disturbing to others. Personal e-mail sent through personal e-mail accounts is one thing, but employees using company e-mail accounts raises a number of issues, even potential law suits.

Organizations must recognize that inappropriate use of company e-mail systems could result in charges of harassment in the workplace. The best way to deal with this issue is to prohibit the downloading and distribution of any material that doesn't directly relate to company business.

Jokes, stories and pictures should never be sent or received via company e-mail accounts. Employees should exchange such information via personal e-mail accounts only.

Employers need to be aware that if an employee reveals evidence of inappropriate e-mails being distributed in the workplace, but chooses not to take action, this can result in legal action against the employer.

Policy Considerations

- Ensure that the e-mail policy of the organization covers the downloading and/or distribution of potentially offensive material.
- Follow up immediately on all complaints of breaches to this policy.
- All staff, no matter what their level, should be aware of the consequences of breaching this provision of the policy.

MONITORING E-MAILS

Establishing a comprehensive e-mail policy document is only the first step. The next step is to enforce it. This does not mean standing over employees and reading what is on their computer screens. Software is available today that can report and summarize all activity for all employees.

The need for monitoring

Without electronic monitoring it is impossible to know if employees are sending sensitive information to recipients outside the organization.

Employees may be using the Internet and chat rooms for personal purposes during business hours. This can reduce productivity or worse, put the organization at risk legally.

Offensive material could be passing through the internal network.



The Risk in monitoring

Unless employees are informed of the monitoring activities, the organization could be liable for invasion of privacy and could be in breach of the law.

If employee activity is being monitored and it is found that illegal or offensive material is being distributed, but management doesn't take steps to stop the activity, the organization could be held liable in any legal action taken.



Policy Considerations

- Decide if you are going to use monitoring software.
- If monitoring software is in fact deployed, then a policy statement must be included that informs employees that they will be monitored, the reasons why they are being monitored and a clear explanation of the consequences should they violate any of the specified mandates.
- Monitoring is the only way to ensure 100% compliance with company policy.
- Annual notice should be given to employees of the type of monitoring and its purpose.
- Employees must be informed that they have a right of action against an employer for invasion of privacy.

PARTICIPATION IN E-MAIL LISTS

The Internet today offers an enormous number of interesting newsletters that are available via e-mail; the topics are endless, covering every imaginable aspect of business and personal life. E-mail based discussion lists on many subjects are also available and of interest to many individuals and companies.

The equivalent in hard copy would be trade newspapers, magazines and newsletters, and for the most part these are considered valuable resources for employees. Electronic or in hard copy, these information sources can provide a valuable educational resource. However, it is possible to have too much of a good thing, and most organizations would not like their employees sitting at their desk reading all day. Hence, participation in these lists must be managed.



Policy Considerations

- Ensure that your e-mail policy mentions participation in newsletters and e-mail lists; clearly define any restrictions or limits deemed necessary. Again, employees need to be told what is expected of them.
- Educate managers on their role in managing employees' time.

PERSONAL USE OF ORGANIZATIONAL RESOURCES

Companies must decide whether employees are free to use company e-mail addresses for personal use, and to what extent. In other words, a decision will need to be made on whether to place limits or restrictions on employees and if the company will actually monitor activity. It is important for employees to understand that computer time, computer storage capacity and Internet bandwidth are all finite resources and paid for by the organization they work for.

If you decide to use monitoring software to manage employee use of resources, it is extremely important (in some jurisdictions it is now law) that all employees be advised of that fact.

E-mail records are now routinely used in legal cases the world over. Therefore, organizations need to understand their information flows and teach their employees about the potential risks of inappropriate e-mail activities.

Policy Considerations

- Employees must clearly understand that all e-mail exchanged over organizational systems belongs to the organization and inappropriate activity could result in legal action.
- Clearly stipulate the rules and responsibilities for the use of personal e-mail on organizational systems. If monitoring software is put in place, make certain all employees are informed of this decision and they agree to it by signing a policy document that specifically mentions this point.

TRAINING

A policy document is worthless to an organization if employees don't fully understand what they are reading. In fact, if employees and senior management don't understand each other, a policy document could actually create more problems. Make sure you back up your policy with an appropriate training program. It is well worth the time and effort, and is far less trouble than dealing with the potential problems associated with the issues raised in this booklet.

Everyone in the organization will need to be involved in the training process – from senior managers to all levels of employees, even temporary workers. Senior managers need to know what is expected of them in managing the process and employees need to know what the restrictions and limitations are.



Policy Considerations

- Develop training programs for all employees and managers to ensure that everyone knows and understands the ramifications of the company e-mail policy.
- Ensure that new employees are trained on the policy before they begin using e-mail.

TRANSFER AND RETIREMENT OF EMPLOYEES

When employees retire, leave the organization, or transfer to another division, their old e-mail address should not be deleted. Customers and suppliers could be using this address as their only way to communicate with your organization. Therefore, it is important for continuity of communications to monitor defunct e-mail addresses for a period of time. The employee could also have been using this address as a contact point for information or services vital to the organization. The critical point is that the mailbox of the ex-employee needs to be monitored and steps taken to ensure a smooth transition to the person taking over that position.

Policy Considerations

- Rules on how to deal with ex-employees' addresses need to be established and adhered to.
- If another person in the organization is assigned the obsolete e-mail address, the ex-employee should be informed.
- The address could be discontinued when all activity in the e-mail box has been attended to and a smooth transition has been completed.
- When the employee leaves the organization, the password for that e-mail account should be changed immediately.

Additional messaging strategies

INSTANT MESSAGING

Instant Messaging services can provide an organization with real time access to their customers and suppliers. It can be a key differentiator with any support strategy that employs the methodology. However, if Instant Messaging is used in the workplace by employees for non-business reasons it can be a significant drain on enterprise productivity.

Users of Instant Messaging services should also be aware that these services may open an organization to additional security threats. It can be difficult to protect against these threats unless your anti-virus programs can specifically examine Instant Messaging traffic.

Policy Considerations

- Examine Instant Messaging technologies to determine if they can be used to enhance your company's communications capabilities.
- If Instant Messaging is used within your organization, be sure to address the issue of what is acceptable and what isn't during an IM exchange between employees and business associates. While it might seem obvious to some, it is always best to explicitly inform all employees that bad language and unprofessional behavior will not be tolerated. Remember, the Internet represents your "window to the world" and it is important to take the necessary steps to ensure that your organization's reputation is maintained and enhanced.

- You should specifically address the issue of employees using Instant Messaging for their private use in the work place or after hours.
- To address the security concerns related to Instant Messaging, make certain you have anti-virus software programs installed at both the desktop and server level, and all relevant settings have been selected.

SHORT MESSAGE SERVICE (SMS)

SMS provides an easy, simple and inexpensive way to communicate instantly with employees, customers and suppliers immediately, wherever they may be. Systems are available today that will allow organizations to instantaneously broadcast SMS messages from a computer in the office to one or more mobile/cell phones in the field.



If an organization decides to use SMS with its customers, it should only send this type of message when regular e-mail isn't effective. For example, it is quite appropriate to send SMS updates on scheduled deliveries, but it is most inappropriate to use SMS for advertising. If not used properly, SMS messages can often create resentment with customers. On the other hand, if used appropriately, it can become an unsurpassed and welcomed customer service tool.

Policy Considerations

- Determine if SMS should be part of your communications strategy. Keep in mind that digital phones are fast becoming a ubiquitous tool for most consumers. This creates an opportunity for businesses to differentiate themselves in terms of customer service. However, don't make the mistake of using SMS too much or under the wrong circumstances.
- When deploying SMS, make sure that customers and suppliers are given the choice to receive or decline any SMS service you may offer. This means you must specifically ask potential recipients if they wish to "opt in" and you should also provide an "opt out" option should they change their mind in the future.
- Consider the use of SMS for maintaining internal communications with employees. This could be particularly important when dealing with a sales force that spends much of its time out of the office.
- Don't take it for granted that employees understand SMS. Provide training on the effective and professional use of SMS.
- Decisions have to be made regarding the use of personal mobile/cell phones and SMS during business hours. While most organizations already have a policy in place regarding the use of company phones, they may not have included rules about personal phones that come to work every day with the employee. From an employer's perspective, too much time spent on personal calls or personal SMS messages (even if it is on the employee's own phone) means a loss of productivity.

ADDITIONAL RESOURCES

Companies offering services to help you develop an email policy document can be found by entering "email policy" into a search engine.

The following is a list of global sites to provide more on the various topics covered in this booklet. For information about the privacy laws, regulations regarding the sending of spam and any other issues relating to e-mail use, visit your government's regulatory agency website or visit www.aoema.org for APEC member websites.

GOVERNMENT RECOMMENDATIONS

www.oecd.org/sti/cultureofsecurity

VIRUS INFORMATION

www.f-secure.com
www.mcafee.com
www.symantec.com

SPAM

www.cauce.org

PRIVACY

<http://epic.org>
www.privacy.net

CONSUMER PROTECTION

www.econsumer.org

NETIQUETTE GUIDELINES

Considered to be the original "Netiquette Guidelines"
www.ietf.org/rfc/rfc1855.txt.



Asia-Pacific
Economic Cooperation

APEC Publication #204-TC-01.1

www.apec.org



www.aoema.org



E-Japan Forum
www.ejf.gr.jp



Funded by FMMC (Japan)
www.fmmc.or.jp

Disclaimer and Copyright

The information and URLs contained in this guide book are accurate at the time of printing.

© Copyright is jointly held by APEC, AOEMA and the E-Japan Forum, with AOEMA managing all rights and permissions. This guide book may not be reproduced, translated, or published in any electronic or machine readable form in whole or in part and is prohibited from commercial use such as sales and publication without prior written approval of the APEC Secretariat, Asia Oceania Electronic Marketplace Association. APEC, AOEMA and the E-Japan Forum and members who are involved in the

development of the guide book are accept no liabilities for any losses and damages caused directly and indirectly through the use of this guide book. When using this guide book for any purposes, you should explicitly stipulate the source of quotation or reference from "Safety Mail" by APEC, AOEMA and the E-Japan forum". Nisso 22 Building 5th Floor, 1-11-10 Azabudai, Minato-ku, Tokyo 106-0041 JAPAN

Please email us at info@aoema.org for feedback, comments or more information.

March, 2004.



Safety Mail

Messaging Strategies

Marketing Strategies

Threats

Guidelines

Policy Considerations

Safety Net a companion to Safety Mail. A practical guide for beginners as well as experienced Internet users for creating your own “safety net” to safeguard against fraud and threats in the online world.

- Consumer Protection • Cookies • Digital Signatures • Firewalls • Identity Theft • Instant Messaging, Chat Rooms, etc
- Intellectual Property Rights • Internet Dumping • Internet Scams • Legal Issues • Monitoring Internet Usage
- Online Defamation • Online Dispute Resolution • Online Stalking • Passwords • Privacy of Personal Information
- Public Access • Secure Web Pages • Spam • Software Updates • Spoofing • Spyware • Trojan Programs • Viruses
- Guidelines for Email Messages • Guidelines for Mailing Lists • Guidelines for Consumer-friendly Websites
- Guidelines for Safe Online Buying • Guidelines for Online Auctions

ISBN: XXXX-XXXX