The Basics of E-Mail Security

By Felipe Guillen

July 2003

INTRODUCTION. This tutorial discusses the basics of E-mail security for small businesses, and acquaints you with important information such as a few of the more notable hazards associated with the unrestricted or careless use of E-mail. This well used communications portal of todays technology based society, is responsible for countless instances of serious information and financial losses, in almost every segment of business imaginable. The information presented here will help to inform the reader as to just some of the precautions which should be considered before any E-mail is consigned to its unescorted cyber journey.

BACKGROUND. As todays business environment continues to evolve and become yet more competitive and aggressive in the various commercial markets, a greater reliance is being placed on the use of the many offshoots of today's technology sector such as E-mail. This derivative of the computer evolution finds particular application where a fast and convenient mode of communication is desired, especially by todays busy company executives and their secretaries and assistants. This means of communications however carries very serious repercussions if misused (and we are not referring to the well recognized and published hazards involving computer virus' and their E-mail based distribution).

A vital point to remember about this medium is that it is **very susceptible to extensive and undetected interception** and even manipulation (i.e., editing, rerouting, duplication, etc.), by numerous unseen parties once it leaves the confines of your computer! **Never forget that E-mail is as secure as a postcard! In fact, it is truly todays electronic equivalent of a postcard!**

E-mail traffic is open to compromise by numerous elements including (but not limited to); employees of your firm such as the computer system administrator and his/her staff, the counterpart employees of the recipient when mailing to other firms, the employees of the ISP you may be using as your Internet portal, employees of the ISP of the recipients Internet portal, in mid-stream by any of the many Hacker types which infest the Internet, by professional operatives who routinely use this medium as a key modality for the supplemental collection of internal information of targeted firms, by anyone gaining access to unsecured computers and accessing the E-mail archive files, etc. Further, such compromises leave no evidence of their occurrence.

In addition, the wide and still increasing use and availability of wireless internet portals courtesy of such business types as coffee shops, fast food restaurants, café's, etc., (used to increase customer traffic and patronage at their establishments) has served to **significantly** increase the vulnerability of not only E-mail traffic – but also of web surfers. Case histories are already replete with very extensive and wide spread damage to the users of these "convenient" services. As it turns out, not only do the patrons of these establishments find the wireless services convenient and attractive – but so do serious hackers!

Examples of just some of the information losses regularly attributable to the careless use of E-mail include;

Executives movements: Many situations involving the compromise of executives (especially when traveling) owe their success to the careless disclosure of where for example key executives will be checking in when traveling – so efforts may be prearranged for the total compromise of their rooms, conference sites, messages, vehicles, etc., via electronic eavesdropping devices.

Marketing strategies: Many executives and their assistants alike have inadvertently aided in the release of sensitive marketing information such as contact names, contract bid information, scheduled meetings, confidential cost figures, etc., due to careless E-mail practices.

Personnel changes: By simply monitoring the E-mail traffic of targeted firms, supplemental information is easily collected relating to internal company problems and changes such as transferring, departing or newly hired executive personnel and the scheduled dates for such changes. This information has even been used in past operations to actually "hire away" prospective executive candidates which were to be hired by the unwittingly victimized firm!

Personal information: Due to carelessness, personal information about many a firms executives and other such key personnel is routinely compromised due to its inappropriate transmission via this unsecured medium. Even **extensive** instances of credit card fraud and identity theft, owe their glowing success to the careless, widespread use of sensitive information relayed via E-mail and Internet traffic.

Mergers and/or acquisitions: Extensive and quite confidential information pertaining to important mergers and/or acquisitions has been lost by its being inadvertently leaked via E-mail. This is potentially damaging to both privately held companies, as well as publicly traded firms.

Financial problems: Many a firms loss of investors and potential supporters owes the unregulated use of E-mail for its woes. Whether due to the inadvertent discovery and disclosure of critical E-mail traffic, or due to the deliberate efforts of professional operatives retained by less than ethical (but careful) potential investors, E-mail has helped to consign many a teetering firm to the annals of history.

Internal security issues: Professional operatives know full well that by simply compromising a targeted firms E-mail traffic, they will quite readily obtain a very detailed and useful synopsis of the companys internal security problems and vulnerabilities – which are then promptly and completely exploited by the Operative and his/her team. This is a favored and oft used, basic element of the professional operatives "tools of the trade".

"As useful as one may find E-mail to be - business spies appreciate it even more!"
(PS: The Same Applies to VOICEMAIL!!!)

In addition, E-mail may be easily "Spoofed" to give the impression that the sender was someone who in actuality had nothing to do with the message – by falsifying the automatically system placed Sender I.D. As an example; an unethical and ruthless competitor may successfully paint the profile of their closest competitor in a highly negative light to the general public and the industry by sending a highly inflammatory E-mail which is then mysteriously leaked to for example - representatives of the media. The negative publicity can be expected to generate serious credibility and image problems for the hapless victimized firm, while also impeding their potential for future profitability or even casting doubt on their ability to remain in business. The perpetrators thus enjoy increased market share, and may even cause the total failure of a key competitor!

Further, if it is in the profile of the victimized company and its employees to indeed use the E-mail system to conduct serious business via this hazardous medium, they will have an even more difficult time disproving the appearance that a particular E-mail was in fact not prepared and sent by them. On the other hand if it can be dramatically shown by strictly adhered to policy and practice that this firm and its employees in fact never conduct such sensitive business via E-mail, such efforts at sabotage may be more readily and successfully countered since it can be more convincingly shown that it is clearly uncharacteristic of the company to have written and consigned such information to E-mail.

Inbound E-mail poses its own set of serious hazards. More and more instances of virus intrusions, discreet data theft, illicit remote control of computer systems etc., are accomplished via the introduction of malicious code as secreted attachments in messages, documents, etc. When the attachments are opened, the code discreetly executes and delivers its true payload. The victim thus does not realize that they have just unknowingly unleashed serious problems into their system.

E-mail based forms of compromises are quite varied and too extensive to cover in total in this advisory. Suffice it to say that the use of E-mail must be carefully evaluated, and its ramifications understood.

E-mail should ONLY be used for transmitting the simplest and most innocuous of messages. It should never be used for conducting serious or confidential business matters. Remember this rule; If its confidential - keep it off of the Internet and out of the E-mail system, and never open attachments. The following provides a concise set of important considerations for all users of the E-mail system.

TEN TIPS FOR SMALL BUSINESSES. To start, here are ten basic elements to consider before using the E-mail system for conducting business, and before you send your next communiqué;

1. Is the information being sent via E-mail considered to be at all sensitive, confidential or in any way critical to your firms operation and/or well being?

2. Are there any other means of communication which would be more acceptable or secure for transmitting the material in question? Thus, is E-mail being used solely because its convenient?

3. Does the material being considered for transmission via E-mail pass the **"Postcard Test"**? That is – is the material being transmitted so benign and non-sensitive in nature that you would feel just as secure and unconcerned about its confidentiality if were sent via U.S. Mail, written on the back of a Postcard?

4. Is the information to be sent of such a nature that if it were to be broadcast on the radio, TV or in the print media – it would have no effect or be of no consequence or concern to either you or your business?

5. In the broadest sense, does any of the information being considered for transmission via E-mail though not of any importance or criticality now – carry the potential however slight for its being used in any negative or harmful situations directed against you and/or your firm, at anytime in the future (however distant that may be)?

6. Is the material to be sent via E-mail potentially an important "Puzzle Piece"? That is, though by itself in its current form it may be casual or benign in nature, if combined with other sensitive office conversations or stored information (which may at anytime be covertly compromised) – could it then be used as a vital component to confirm or complete a more encompassing or confidential yield of critical internal information?

7. Can any of the contents or details of the pending E-mail be used if illicitly modified or edited by adversarial third parties, to "spoof" or otherwise be manipulated to negatively misrepresent you or your firm to the recipient or others?

8. Is the pending E-mail written so as to clearly and unmistakably convey the intended message, without the potential for the unsecured content to be used to portray you or your firm negatively - if taken out of context?

9. Does the potential exist for the recipient of the E-mail to reply with information which in part or in whole would inadvertently expose sensitive/confidential information to the unsecured realm of cyber space? In other words, does it illicit a potentially hazardous response?

10. Are all of the parties which you send E-mails to, thoroughly versed and acquainted with the security considerations surrounding the proper use of E-mail - or are there any who can be considered the weak link(s) in the chain???

NOTE: These tips are only intended to outline some of the basic and more well exploited vulnerabilities of the E-mail system. Each firm should commission a comprehensive and thorough analysis of THEIR OWN unique security exposures and required solutions. As situations and security risks are fluid and always varying, periodic reappraisals of both risks and security countermeasures should be conducted at regular intervals - incorporating any indicated modifications and/or required security enhancements.

In addition, obtain and regularly use such computer security software programs as; **[1] Encryption Programs** – designed to encode sensitive files and documents (including E-mail) to make it more difficult to make use of confidential material that may be stolen or copied by aggressor parties, **[2] Spyware identification and removal programs** which when run regularly, will identify spy type and other intrusive programs which may be present in your computer(s), and then remove them from your system, and **[3] Internet protection programs**, to provide computers which access the Internet, with a degree of protection from some of the many prevalent hazards including worms, spyware, scanners, scripts, etc.

For an example of a suite of such programs, you can go to: **http://www.itcompany2.com/omega** to see what we recommend to clients who use our services. Regardless from where you obtain the programs, acquire and regularly use effective protective programs for all of your computers – and make a habit of ALWAYS and REGULARLY backing up your data!

When only ashes are left, it's too late to call the fire department!

TAKE THE 15 POINT SECURITY HAZARD PROFILE TEST!

The following quick check profile test will give you a basic appraisal as to your current risk exposure potential, to the various forms of business compromises awaiting the unsuspecting and unprepared business executive. Answer "TRUE" or "FALSE" to the following questions, then grade yourself at the end of the test to see where you stand in todays aggressive business environment.

1. TRUE___ FALSE___ I never use E-mail to send confidential or sensitive messages.
2. TRUE___ FALSE___ None of my employees use E-mail for sending confidential messages to others.
3. TRUE___ FALSE___ We never use Voicemail for leaving confidential or sensitive messages.
4. TRUE___ FALSE___ When offices are unoccupied, all confidential documents are securely locked away.
5. TRUE___ FALSE___ Computer passwords are changed at least once a week, and used by all personnel.
6. TRUE___ FALSE___ Key offices, phones & conference rooms are checked to insure there are no eavesdropping devices.
7. TRUE___ FALSE___ All discarded sensitive/confidential documents are promptly shredded by Crosscut Shredder units.
8. TRUE___ FALSE___ Computers are protected by security programs, firewalls and strong passwording access controls.
9. TRUE___ FALSE___ Traveling executives have all sensitive files in their laptop computers, encrypted in case of theft.
10. TRUE___ FALSE___ Office doors have high level security grade locks installed, instead of the standard office grade types.
11. TRUE___ FALSE___ All executive offices are securely locked after hours, and when otherwise unoccupied.
12. TRUE___ FALSE___ We have a program for identifying, classifying & securing documents considered **CONFIDENTIAL**.
13. TRUE___ FALSE___ When holding meetings away from our offices, we have the area checked for eavesdropping devices.
14. TRUE___ FALSE___ We have "in-house" programs in place to warn us of any attempted business espionage efforts.
15. TRUE___ FALSE___ We thoroughly background check and pre-screen all prospective employees.

If you answered TRUE to all 15, Congratulations! You're an example to others who wish to survive & thrive in today's world!

If you answered TRUE to 11 or more, You're very aware of today's hazards and have been doing your homework. You'll do well!

If you answered TRUE to 8 to 10, You should promptly institute the necessary security corrections - before your luck runs out!

If you answered TRUE to 5 to 8, You're well on the way to being some business spy's "Lunch"! Get serious help QUICK!

If you answered TRUE to less than 5, If you're still in business, it's only because no one's attempted to compromise you – yet!!!

SUMMARY. Just as todays business climate is heavily reliant on technology to function and even to thrive, it should always be remembered that this technological sword is a double edged servant that cuts both ways. Technology can be used constructively or destructively – depending on who is wielding the sword. Be sure that when next you draw the sword – it is not taken away from you and used against you or your firm! Take a lesson from responding police officers, who realize that they are bringing a gun to the scene (their own sidearm). Don't arm your adversaries - practice "Safe E-mail"- and effective communications security.

FOR ADDITIONAL INFORMATION. The author can be contacted at:

Mr. Felipe (Phil) Guillen, President
OMEGA, Inc.
P.O. Box 964
Tinley Park, IL 60477
708-429-1563

OMEGA is a Minority-Owned Business