



Professional Development

September/October 2008

The Essential Guide to Email Security

What you need to know about protecting incoming and outgoing email.

Over the past couple of decades, email has become one of the world's leading communication mediums, perhaps even outpacing the telephone and traditional mail service.

Unfortunately, over this same time span, email has proven itself to be highly vulnerable to outside influences, including individuals and organizations that seek to cause some form of technological damage or hope to make money in an illegal fashion. As a result, security has become an increasingly important issue for email users.

Email Threats

Although email security is often viewed as a single issue, it is actually a conglomeration of several different threats that work to damage computers and defraud recipients, as well as to undermine the effectiveness, reliability and trust of email systems. Email threats can be divided into several distinct categories:

Viruses, Worms and Trojan Horses: Delivered as email attachments, destructive code can devastate a host system's data, turn computers into remote control slaves known as [botnets](#) and cause recipients to lose serious money. [Trojan horse](#) key loggers, for example, can surreptitiously record system activities, giving unauthorized external parties access to corporate bank accounts, internal business websites and other private resources.

Phishing: According to the Anti-Phishing Working Group — a trade organization that consists of financial organizations, software publishers and other concerned parties — [phishing](#) attacks utilize social engineering to steal consumers' personal and financial data. The attacks rely on "spoofed" emails that direct recipients to bogus websites that are designed to trick them into revealing confidential financial data such as credit-card numbers, usernames, passwords and social security numbers. Phishing perpetrators typically operate by hiding under phony identities that they have stolen from banks, online merchants and credit-card companies.

Spam: Although not an overt threat like a virus-infected attachment, junk email can quickly overwhelm an inbox, making it difficult to view legitimate messages. The [spam](#) problem has gotten so bad that it is commonplace for users to abandon email accounts that are overrun with spam rather than try to fight the problem. Spam is also the delivery medium of choice for both phishers and virus attackers. So just how bad is the problem in terms of numbers? Tens of billions of spam messages are sent every day.

Email Safeguards

Protecting email users and their systems from attackers is a 24/7 job that requires the use of multiple security tools. Some of these include:

Client Security: Virtually all major email clients offer security settings, anti-spam tools, phishing filters and other features that are designed to snare and isolate dangerous messages before they can inflict harm. Email users should investigate these features and use them as their first line of defense.

Firewall: A [firewall](#) can bolster email security by filtering out malware-laden attachments and other types of unwanted material that don't meet pre-configured rules.

Encryption: Rendering messages indecipherable to unauthorized recipients is a popular way of protecting outbound emails. [Encryption](#) software isn't perfect, however, since even the best products consume both processor speed and storage space. Users can also lose or forget passwords. Encryption can be handled by firewalls or additional software.

Anti-Virus Tools: Leading [anti-virus products](#) and services generally do a good job of spotting and removing viruses, worms and Trojan horses from incoming email messages.

Spam Filters: A good spam filter can differentiate between legitimate email and spam, freeing a user's inbox from mounds of digital debris. A drawback to this technology is that a poor spam filter, or one that has not been properly tuned, will remove a certain number of legitimate emails from a user's view while letting some spam pass through untouched. Improved spam-recognition technologies are making spam filters more accurate. Most vendors now promise 99 percent-plus accuracy rates — but even the best spam filter will incorrectly categorize some emails.

Education: One primary email-defense tool is education. Users who are aware of email threats are less likely to open potentially virus-infected attachments, click phishing links or perform other risky actions.

Email threats will continue to exist for as long as there are people and organizations that thrive on the misery they inflict upon others. Therefore, the practices and tools that constitute email security are likely to exist for as long as email itself.

Article from IT Security by John Edwards; September 19, 2008, <http://www.itsecurity.com/>