AntiSpam Etc – Email Safeguards in a Nutshell

by Bonnie D. Huval

There is no single product on the market, even at the high end, with a 100% perfect capability for intercepting every threat to your email. However, if you are willing to look beyond the ordinary, it is possible to get an extremely high level of protection for your email without excessive hassle or cost.

Initial Strategic Decisions

Your email strategies have implications for the vulnerability of your email. If you have ever suffered the embarrassment of apologizing to angry customers, colleagues and friends about a virus that spread to them through your email, you are concerned about more than your own computer. You also want to avoid letting anything misuse your email to spread itself.

Many people use server based email accounts and access their email only through a web browser. This is especially common for personal accounts and free email services. Some businesses do it too, hosting email on their own servers, so that traveling workers need not carry their own PC with them. PCs with a standard software configuration can then be rotated among the workers as needed. If you use server based email, a virus that relies upon an email address list on the PC to propagate itself cannot find any such list. It may infect your PC, but that type of infection cannot spread itself from your PC.

Many users prefer to run an email client on the PC so they can compose messages offline, download incoming messages, and keep message archives for offline reference. Hackers target the most popular email clients more often than other clients. As a result, simply choosing a less common email client can help you dodge some bullets.

Basic Protection

Even if you always leave your email on a server and get to it through a web browser, and even if the server attempts to block viruses, the bare minimum level of protection is antivirus software. Remember, just one infection is enough to give you a nasty headache. A few websites offer antivirus scans free of charge, but you are safer with antivirus software that runs on each PC, especially if you choose to download email to your PC. Antivirus software on your computer can not only scan for infections, it can screen incoming email to intercept infections before they become established.

When combined with a subscription for frequent online updates, this is a good first line of defense. It often comes in a bundle with a personal firewall program and software that blocks specific behavior from websites. If you have only "pocket money" to spend on email protection for each PC each year, this is probably what you will buy. To be safe, you will probably continue to use it even if you add heftier protection elsewhere. Symantec and McAfee sell two of the most widespread lines of

software for this purpose, and issue security updates quickly as new malware appears in the Internet.

Add Spam Filtration

Shielding against viruses does not reduce the amount of spam. Published estimates say that up to 90% of email is spam. Wading through 100 messages to find 10 that are legitimate is a waste of time and capacity.
You can get antispam filters that run on your PC. Some email clients come with such a filter. It is likely to do a poor job of distinguishing spam from legitimate messages and may not allow tuning of its sensitivity. "Pocket money" can buy a more accurate filter, although it will still make a lot of incorrect decisions and its ability to "learn" greater accuracy is generally limited.

The next step up is a filter on your email server--the larger computer that initially receives email from the Internet and from which your email client downloads messages. If you are using email service provided by someone else, including one of the major free services, they are likely to run such a filter. Some hosting services offer a server based filter bundled into their hosting packages. They choose software priced so that with volume discounts, they can afford to cover the cost with part of their hosting fees. Alternatively, if you have your own email server, you can buy the antispam software of your choice. That gives you greater accuracy and better ability to tune the filtering.

Unfortunately, for spam filters up to this level of sophistication, the primary method used to detect spam can be defeated by a clever spammer. These filters look at contents of the subject line and body for each message, seeking words and phrases frequently found in spam. Have you ever wondered why a lot of spam contains an advertisement in a picture instead of text? It's easy to analyze text. It's hard for software to discern words embedded in a picture. Server based filters do more sophisticated analysis than PC based filters, but mistakes still occur.

These spam filters also check the sender against one or more commercial blacklists. In theory, blacklist providers know which domains have been sending spam. In practice, some blacklists are too easily tricked by "spoofed" headers in spam messages, or they blacklist the entire network location that sent the spam even if the IP address is shared by several unrelated domains. That causes some innocent domains to be blacklisted. Spam filters using the blacklist block delivery of legitimate messages from those domains.

One of my clients nearly lost an important customer because their server based antispam system routinely segregated his messages as spam. Even though they are using one of the leading enterprise class filters, for six months the customer was unable to get through. A more accurate solution is available, and it provides more than antispam and antivirus filtering.

Sophisticated Gateways

The next step upward is to subscribe to an email protection gateway. You can do this only if your email is on a domain where you manage the email server. To use a gateway, change the MX records for your domain to point to the gateway. This tells the Internet to send all your email to the gateway instead of to your email server. The gateway removes viruses, segregates spam into quarantine, then sends your server only the messages that it considers legitimate.

This goes beyond sending viruses and spam into quarantine. It reduces the email load your server has to handle, because quarantine is at the data center that provides the gateway instead of your equipment. One of the largest nationwide real estate firms in the USA, with about 40,000 email accounts, was planning to upgrade its computers and communication lines when it began using an email protection gateway. The gateway reduced the amount of traffic to its computers so much, the upgrade was no longer needed.

The best email gateways (not all of them, only the best) detect spam differently from other antispam filters. Instead of watching for key words or phrases used in previous spam, they analyze the attack patterns suffered by wide-open email accounts, tracing them back to specific source computer systems. Software analysis is augmented by round-the-clock human monitoring and analysis. This type of system can detect and begin responding to a new spam campaign within a few minutes, even when the campaign is executed through many hijacked PCs (a botnet). Accuracy is higher than when you run and perform frequent tuning on your own server based antispam system, and can easily be above 95% with hardly any tuning. Legitimate messages rarely get quarantined by the best of these systems, and little spam sneaks through.

The best gateways go a couple of steps beyond filtering, too. Some organizations need to prevent confidential or proprietary information from being sent to inappropriate recipients. Depending on the gateway you choose and the level of service you subscribe to, the service can filter *outbound* email in accordance with rules set by you. Without a gateway, this would need to occur separately on your email server.

Last and certainly not least, the gateway can provide disaster redundancy for your email. If your email server goes down, the gateway can store your email until the server is up again, then deliver all the email you would otherwise have lost. Some gateways allow you to access email through a web browser while your server is down, keeping you in business throughout even the worst disaster.

This type of system is used by the state college campus that hosts emergency responders after disasters in Port Arthur, Texas. They did not have it when a 2005 hurricane shut the town to all residents for about a month. Lack of communication made it hard to support for emergency workers, and especially hard to coordinate re-opening of the campus. The next time the town was shut for weeks by a hurricane, the campus relied on this system to help it keep going. Between emergencies, it has cut their incoming spam volume to a small trickle.

Cost Need Not Be High

That brings up the subject of cost. The college is able to afford the best available gateway service on its tight budget. Using the gateway allows the college to use less expensive arrangements for disaster recovery of its computer center, since email is always safe. Finally, the gateway helps the college avoid upgrades of its email capacity, since spam is almost completely eliminated from its incoming email.

Most small companies with just a few email accounts cannot afford a reasonably good server based system. Subscription to an email protection gateway for a company with five email accounts costs about as much as a monthly dinner out for one or two people at a modest restaurant. The more email accounts a business has,

the lower the monthly cost per user. For businesses large enough to use their own server based system, a gateway is often either about the same price, or cheaper.

Although outbound filtering and email disaster redundancy may cost extra, at least one gateway includes those services at no extra charge and without binding customers into long term contracts. It is not just a highly reliable and scalable option, it is also surprisingly affordable and accessible for small organizations.

About the Author: Bonnie D. Huval has been a consultant since 1992 helping companies make more money, especially with their automation and transaction systems. Successful projects by her USA and UK firms include cutting time to ship product from two days to two hours, cutting downtime for product introduction by 40%, and getting the right email gateway for the college mentioned in this article. Go to http://www.seneschal.biz for your own free 30 day trial of the same email gateway for any size company. Go to http://www.makesureyougetpaid.com for her materials to help small businesses be more successful.

Article Source: http://EzineArticles.com/?expert=Bonnie_Huval