Interested in learning more about security?

SANS Institute InfoSec Reading Room

Fighting Spam in the Academic Arena

For the business and educational environments, spam has become a security issue. Junk e-mail has gone from just being annoying to being expensive and risky. The enigma is that spam is difficult to define. What is spam to one person isn't necessarily spam to another. Fortunately or unfortunately, spam is here to stay and destined to increase its impact around the world. Unsolicited junk e-mail steals system resources and reduces employee productivity for every company with electronic mail. It has become an issue that ca...

Bev Weidmann
GSEC Practical, Version 1.4b

Abstract

For the business and educational environments, spam has become a security issue. Junk e-mail has gone from just being annoying to being expensive and risky. The enigma is that spam is difficult to define. What is spam to one person isn't necessarily spam to another. Fortunately or unfortunately, spam is here to stay and destined to increase its impact around the world. Unsolicited junk e-mail steals system resources and reduces employee productivity for every company with electronic mail. It has become an issue that can no longer be ignored; an issue that needs to be addressed in a multi-layered approach: at the source, on the network, and with the end-user.

To keep ahead of the growing problem, each organization must analyze the tools available to determine how best to counter spam in its environment. Tools, such as the corporate e-mail system (in this case, Microsoft Exchange), e-mail filtering gateways, contracted anti-spam services, and end-user training provide important arsenal for any organization. But, different from the corporate world, academic institutions stress the importance of free flowing information of all types. This fact may influence battle tactics, but still the battle must be fought. If you do nothing, Spam will inundate network systems, kill employee productivity, steal bandwidth, and still be there tomorrow!

Fighting Spam in the Academic Arena

Dealing with spam is akin to fighting squirrels around your birdfeeder. If you feed the birds in your backyard, you do it because you want birds. You periodically add bird food to the feeder in the hope that birds will come to eat and you can benefit from their visit. Enter squirrels!! Squirrels are intelligent and adaptable, and they love bird food! I have seen a whole feeder full of birdseed disappear in hours-- devoured by just a few squirrels. I don't really want squirrels, although I don't mind one occasionally. But squirrels are such persistent creatures that it's hard to find a birdfeeder that is truly squirrel-proof. In my mind, squirrels at my birdfeeder waste my resources. I need to buy a lot more birdseed, find a place to keep it, and spend more time taking care of the birdfeeders.

Now this analogy can go just so far, but spam is like the squirrels. Spam steals our system resources, requiring us to purchase additional storage space. It stretches our network bandwidth, which can affect the operations of our internal network. It reduces the productivity of individuals who must deal with the junk mail in their e-mailboxes, and it increasingly requires system administrators to provide and maintain the counter-measures needed in fighting spam.

"DEFINITION" OF SPAM

Spam is difficult to define. In fact, there is no clear definition. Generally accepted is the definition that spam is like junk mail; you get it whether you want it or not. Does that make it spam? Is it spam if it tries to sell you something? Is pornography spam? Are personal jokes from friends considered spam? What about unsolicited political messages? We all recognize spam when we see it, but the truth is that what is spam to one person may not be spam to another. An e-mail that is considered spam at work may not be considered spam at home.

The most prevalent definition seems to be "unsolicited commercial e-mail" or UCE, but there is no definition that is universally accepted (ePrivacy). Spam is unsolicited because you didn't ask for it, you may not want it, or you aren't interested in it. Spam usually advertises something—get-rich-quick schemes or get-something-for-free. Perhaps it presents an investment opportunity or business deal or hypes some health and diet scam. It attempts to sell something, sometimes fraudulently, and it comes through electronic mail.

SO WHAT'S THE PROBLEM?

"Left unchecked, spam will undoubtedly cost corporations billions of dollars in lost productivity and squandered IT resources." According to J. William Gurley, spam is becoming an epidemic (Gurley).

For the user, spam is annoying, distracting, and often downright irritating. Many consider it an invasion of privacy. Time is wasted in checking the e-mails for relevancy and interest before deleting. Often junk e-mail sits unopened, hogging valuable mailbox space, and resulting in requests for additional server storage space. For the enterprise, spam lowers individual and corporate productivity through wasted time. For the e-mail system administrator, spam has become a security issue. Spam steals the resources of the recipient network system by using needed bandwidth and by taking up hard drive space on the mail servers.

"Spam: Has it become a stalemate?" August 4, 2002: CNN.com/SCI-TECH

Junk e-mail is increasing exponentially, and it is also expanding its reach. Spam affects us wherever we have e-mail. Pornography is delivered, boldly and in full view, disregarding the reader's preferences. Even wireless phones that have text capability are becoming targets of unsolicited advertising—especially expensive for the receiver. Spam can be the carrier for computer viruses and malicious code, intentional or not. In some cases, JavaScript embedded in e-mails is flawed and crashes your e-mail program, or worse, your system, requiring time spent recovering. During routine mail server backups, e-mail, including any junk mail left in the message

store, is copied, taking even more space. Spam can also produce an effect like a Denial of Service attack, where the spam blankets a domain address not knowing if addresses are real or not. The Message Transfer Agent (MTA) must use system resources to process the e-mail and send a nondelivery receipt (NDR) for each false address. This can so occupy the MTA that it delays delivery of legitimate mail.

Concern was expressed at the recent Global Internet Project Seminar, which the author attended on June 18, 2002, that the growth in spam would outpace the growth of Internet use. "76 billion…spam e-mails…will be delivered in 2003, according to eMarketer." (ITAA) Vincent J. Schiavone, CEO for ePrivacy Group, reported that we can expect the per-user volume of spam to increase forty-fold by the year 2005 (ePrivacy). Brightmail reported that 36% of all e-mail that traveled the Internet in July 2002 was unsolicited junk e-mail (Lemos). In a Brightmail Study, commissioned by Gartner, "lost productivity due to spam costs US $1 billion a year." (Graff) Japan and Europe report that spam is increasingly becoming a problem for users with wireless connections using I-Mode and SMS messaging systems. All of these factors could likely decrease user confidence in e-mail (ITAA).
In July, according to

Vinton Cert, Senior Vice President of Architecture and Technology at WorldCom, Inc. warned, during the GIP seminar, that "Spammers will always take advantage of the latest technology to optimize their outreach, so that in the future, we may be bombarded by huge amounts of high resolution video and graphics." (ITAA) Technological advances will never outgrow the negative effects of spam.

We cannot eliminate all commercial e-mail; nor would we necessarily want to. In the academic world, as in the corporate world, a wide variety of e-mail has value, when it is wanted. Unfortunately, we don't have reliable technological tools to separate the good e-mail from the bad e-mail. We can stop a lot of the junk. In fact, millions of spam e-mails are stopped every day, but too many pieces get delivered. It's hard enough to come up with a definition of spam. If we can't all agree on a universal definition, how can we expect to stop the junk e-mail while letting through the desirable e-mail?


Wissenswertes über Spam

Let's face it. Spam works. The spammer's goal is to get around any counter measures. Mailing lists are often built from Usenet postings, by stealing Internet mailing lists, or by searching the web for addresses. The cost to the spammer to send the e-mail is negligible.

There are web sites offering software for harvesting e-mail addresses intended for bulk mailings. One such demo, downloaded while researching this paper, was run by searching on a community college domain address. Over 69,000 e-mail addresses from various educational institutions were collected! And this was done using a free demo address harvester in just 3 hours, running in the background, while working on this paper on the same computer!

New techniques are continually being developed to aid advertisers, such as software robots that set up free e-mail accounts, e.g., "jsmith3241." Filters may fail to recognize and screen e-mail from these addresses. Snappy subject lines and inviting messages strive to catch a reader's attention.

According to the Postini Corporation, spammers look for corporate e-mail directories found on e-mail servers. These are called Directory Harvest Attacks (DHA) and are a "theft of e-mail directory information." Postini reports that, in one 24-hour period, 14, 351 DHA's were identified by Postini, with 24,684,670 invalid e-mail delivery attempts. (PostiniCorp). Before the Simple Mail Transfer Protocol (SMTP) delivers an e-mail to a server, it must first check to see if the address is valid. It does this by sending a "delivery attempt" request. If the server sends a "yes" response, then the harvester knows that the address is valid. From this harvesting, huge mailing lists are compiled. "Up to 25% of corporate e-mail server resources are spent processing attacks intended to gather fresh, valid, corporate e-mail addresses." (Postini Corporation).

It's so easy and the potential rewards are so great for the spammer. He or she signs up for a free mailbox, uses his free trial CD, or hires a mass-mailing service, and then sends e-mail to hundreds of thousands, even millions, of potential customers. The potential profit for each successful hit is relatively high. If the spammer sends out one million unsolicited e-mails at virtually no cost and just 5% of the recipients open the e-mail, that's 50,000 potential customers. Add this to the reality that many people think sometimes you can get something for nothing. If the e-mail promises that they will receive $10 credit toward the purchase of a Honda for each copy forwarded to friends, well, why not send it to everyone you know? E-mail is "free" and think of the $$$.

The answer to spam is not an easy one, but it is an evolving one. Fighting spam needs to be done as a multi-layered effort. Legislation won't stop spam, however improving and enforcing laws that deal with fraud and deceptive advertising may help. High-profile prosecution will help. Internet Service Providers can do more filtering of their networks. Software companies can incorporate more tools into their e-mail software. Advertisers can develop a code of ethics for advertising through electronic mail. Employers can use such tools as filtering and blacklists. E-mail users can learn how to handle junk mail better and be given the technological tools to enforce their own definition of spam.

SPECIAL PROBLEMS FOR ACADEMIA

Educational institutions that want to limit the amount of spam coming into their networks have special issues to consider in balancing security and functionality. Such institutions traditionally have been considered more "open" with free access to all types of information without regard to content. "It's the mission of colleges to share information," says Hossein Shahrokhi, Director of Information Technology at the University of Houston's downtown campus (Olsen). E-mail addresses and campus directories are often posted on college web pages. Information is freely shared. The general rule has been to "allow all access unless explicitly prohibited" rather than to "prohibit all access unless explicitly allowed." Certainly the latter is a much more secure environment, but not always appropriate for the educational arena. Because of the wide variety of information handled by educators, the system administrator has a harder time implementing restrictions in order to avoid the consequences of spam on networks and employee productivity.

Educational institutions must also consider freedom of speech issues when deciding whether or not to fight spam, except in cases of fraudulent advertising and nuisance e-mails, which are a theft of service rather than a speech issue. One of the most fundamental rights cited by the US Constitution is the "freedom of speech." Everyone has the right to express him/herself without interference or constraint from the government, unless there is substantial justification for interference. Part of this freedom of speech is the freedom of the press, which gives the freedom to express oneself through publication and dissemination (LII). Concerns in support of academic freedom, privacy, and First Amendment rights make colleges and universities hesitant to use such tools as e-mail filtering or blacklists. The protection of this freedom causes much debate and delay in fighting spam in the educational environment.

Institutions of higher learning must find a balance between possibly violating the principles of academic freedom, privacy, and First Amendment rights with the security concerns of vital networks.

THE SECURITY RISKS OF UNPROTECTED E-MAIL (Borderware)

"E-mail is the most important single service on the Internet. It is also the number one source of security risk." (Borderware) This is especially true in the educational environment where every mail server is vulnerable to a growing list of attacks.

1. Electronic mail comes through the perimeter defenses directly, with firewalls providing only partial protection. Open ports on SMTP servers may have vulnerabilities that expose the server to exploitation by hackers who find entry.

2. Windows, IIS, and Exchange are three components of Outlook Web Access (OWA) and each must be installed and secured separately. It's easy to make security mistakes with complex installations, especially if accepting the default

installations. Transmissions must pass through the firewall requiring additional security measures.

3. Computer viruses often spread through the use of e-mail attachments. Anti-virus software on the workstation may not be current or may even have been disabled by the user. Users often open infected attachments without knowing or considering the consequences, thus causing the virus to activate. This can result in mass spreading of the computer virus within the enterprise.

4. The default configuration for a mail server may allow relaying of third party mail. (Fortunately, Exchange 2000's default is off.) The mail server then gets blacklisted, and many organizations will not deliver e-mail to these servers.

5. The e-mail addresses "leak" onto the Internet.

6. E-mail can be sniffed while traveling cyberspace, exposing confidential institutional information.

7. Poorly written JavaScript in an e-mail may crash your e-mail program, or maybe the workstation. HTML messages can carry computer viruses.

8. A spammer may blanket-mail a domain hoping to hit on valid addresses. This can clog the Message Transport Agent (MTA) with spam if it sends non-delivery messages. Responding to the influx of spam takes time away from processing valid messages.

THE ARENA

There is one sure way to end the spam problem. That is to turn off the SMTP, POP3, and IMAP services! But who wants to do that when e-mail, which uses these protocols, has become such a productive tool to the corporate and educational world? Doing this would be like removing the telephone. Business nearly stops! Communication is critical to business.

Barring something so final, there are a variety of ways to reduce spam in the enterprise. But, because spammers take advantage of every new technology in reaching the masses, a multi-layered approach is the most promising. According to Patrick Cain, there are three primary places to deal with spam: **at the source, in the network, and at the end-user** (Cain). The multi-layered approach is necessary because some strategies only work at particular levels.

Fighting Spam at the Source

- Dollar costs can be added to spamming through improved and enforced federal laws, and even international laws.

- Tier 1 ISP's can require their downstream customers to prohibit open relays and police accounts more.

Fighting Spam Through the Network

- Corporations can use blacklists developed specifically to identify systems that allow open relay. They can use SMTP header analysis to filter e-mail based on specific characteristics. They can use content filtering to look for inappropriate or illegal images or words in a message, both inbound and outbound.
- E-mail gateways can stop spam, as well as viruses, before they enter the e-mail server.
- Enterprises can develop corporate e-mail security policies that define what is acceptable in the organization. Strategies against spam should become part of the overall network protection strategies.

Fighting Spam at the Workstation

- The user should be educated so that they can help manage their own spam.
- Recipients of fraudulent spam can complain to the Federal Trade Commission, Bureau of Consumer Protection to help the agency investigate fraudulent e-mail scams and illegal practices. The address is UCE@FTC.GOV. (FTC).

Strategies Aimed at the Source of the Spam: Legislative Action

Earlier this year, Computerworld reported that anti-spam laws were on the books in 18 states (Thibodeau). In September, The Chronicle of Higher Education reported that there are now 26 states that have laws regulating spam (Olsen). State laws typically ban the use of false headers or routing information. California requires specific labeling on the subject line to alert the recipient that the e-mail is advertising or has adult content, but this law is considered to be the exception (Thibodeau).

Many states allow spammers to be sued by their ISP's if they ignore the ISP's e-mail policies. Iowa requires that opt-out instructions be provided in commercial e-mail (Thibodeau). Many states are considering laws dealing with unsolicited e-mail, but state laws cannot be enforced beyond state boundaries. Spam is just as likely to be sent from many hundreds of miles away.

In Maryland, a law was passed in May 2002, which is to take effect in October 2002. In this law, commercial e-mail messages that use third party domain names without permission, that contain false or missing routing information, or have false or misleading subject lines are illegal. The law applies if messages are sent from Maryland, if the sender knows that the recipient is a Maryland resident, or if the owner of the domain name found in the recipient's address will confirm that the recipient is a Maryland resident (Sorkin). Many other states are considering legislation; however First Amendment rights have slowed progress.

According to the Diamondback, a University of Maryland newspaper, one argument for legislating junk mail is that US Code, Title 47, Section 27, concerning unsolicited faxes, could apply to e-mail (Warner).

> …The term 'telephone facsimile machine' means equipment which has the capacity (A) to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or (B) to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper.

Federal laws may be more effective because they can be enforced throughout the United States. There are no currently enacted federal laws against spam (Sorkin), although there are numerous bills that have been introduced and are in committee. Anti-spam bills are currently under consideration in Congress, but federal laws cannot be enforced outside of the United States. Spam is just as likely to be sent from many thousands of miles away.

Strategies Aimed at the Network Level

General Strategies

In fighting spam, the following strategies may be useful:

1. Develop corporate e-mail policies that define what is acceptable in the organization and communicate these to employees.
2. Use header filtering and content analysis. Messages and graphics are scanned and filtered based on a set of pre-defined rules developed from e-mail policies. Maintaining such filters require vigilance and frequent modification. Consider filtering out e-mail with:
    a. Blank Subject lines.
    b. No address on the From line.
    c. Bulk mailings
    d. Large number of Blind Carbon Copies.
3. Validate sender addresses in the DNS to block inbound mail with invalid or irresolvable addresses.
4. Filter both inbound and outbound mail to avoid the institution becoming part of the problem.
5. Automatically remove HTML script from messages to avoid HTML computer viruses that may be present in junk e-mail.
6. Quarantines filtered messages to watch for false positives. This allows the administrator to scan the messages and forward legitimate mail to the intended recipient or users to access the quarantined mail to decide for themselves.
7. Disable open relay.
8. Use troll boxes or honeypot mailboxes to capture spam that is a result of targeting entire domains hoping for valid addresses.
9. Utilize blacklists, such as RRS and ORBS.

10. Use automatic disclaimers placed on outbound messages that state the e-mail policy of the organization. These may be helpful in defining how e-mail is used and in fighting legal battles.

Rules-based Filtering

In rules-based filtering, messages are examined according to specific rules looking for patterns often used in spam. Invalid source domain names, forged header information, messages containing such characters as $$$$ or !!!!, all capitals, etc., are common characteristics of spam, and delivery of such e-mails can be prevented. Messages can be returned, tagged with a warning, or directed to quarantine folders. Rules can be modified, as needed. Often, users can specify filtering rules for controlling their own spam. This ability for the user to customize filters is called opt-in. Filtering can be at the server or e-mail gateway and/or at the desktop. The advantage of filtering at the gateway server is that the capabilities are greater and the spam is blocked before it even reaches the mail server. The disadvantage of filtering at the gateway server is that the rules are global and false positives can cause desirable advertising to be blocked. Institutions of higher education are made up of a very diverse group of people who need a great variety of information for developing coursework and providing the assorted programs typical of educational institutions.

"Spam: uma 'mala' direta e cada vez mais pesada"
Sabor, 10/26/2000

Reverse DNS Look-up

In reverse look-up, a server receives a request for services from a remote computer and validates the identity of the remote computer. It uses the "bedrock" of the Internet, Domain Name Services (DNS), to determine the Internet numerical address (IP). The IP address is essential for servers providing and offering services, such as FTP or SMTP. In order for this to work, ISP's provide the name services by putting two pieces of information, known as Berkeley Internet Name Daemon data records, into tables on its Internet domain name servers.

Type	Function	Explanation
"PTR" (pointer) record	IP-addr ---> name	Returns an internet name when given a numeric IP address
"A" (address) record	name ---> IP address	Returns a numeric IP address when given an internet name (i.e., a host name, "mx" mail-exchange record, etc.)

(UMD)

If the information isn't there, reverse lookups done on that computer will not work. If reverse lookup fails, the server will not be able to gain the service of the other server. The failure can happen if an Internet Service Provider fails to enter both records in the DNS table for any server it services. IP spoofing is easily foiled by reverse look up

because of the way name lookup works. This can be effective in stopping spam that comes from spoofed addresses on the Internet. This can be a very useful spam-fighting tool, because legitimate advertisers do not hide behind false addresses. (UMD)

Disable Open Relay

Until recently, the default installation for Microsoft Exchange was to allow open relay, which allows one server to use another server to send e-mail. Open relay is sometimes useful for educational institutions, because it facilitates users who are not directly connected within their e-mail systems to still use the resources of their e-mail server to send mail. They may be on sabbatical halfway around the world, but they can log onto their Internet Service Provider accounts with their web browser configured to use their corporate SMTP outbound mail service, and the ISP forwards the e-mail through the corporate system, maintaining the header of the corporate mail. Spammers take advantage of this to mask their identity and host ISPs, by using your server information in their headers.

Spammers have robots and search engines that search the Internet for servers that are open to relay. Unfortunately, servers that are configured to allow open relay expose themselves to being blacklisted for allowing spammers access to their resources. Some companies block e-mail received from servers on the blacklists, so legitimate mail may not get delivered. (University)

Microsoft Exchange 2000

Exchange 2000 Server

For those corporations and educational institutions that use Microsoft Exchange 2000, some filtering is possible at the server level. Exchange 2000 has incorporated the ability to stop the delivery of messages sent from a particular user or domain plus those with blank From lines., To do this, filtering must be enabled on the Default SMTP Virtual Server in the System Manager.

Senders on the message filter list cannot send e-mail to specified IP addresses within your electronic mail system. Filtering can be enabled for select IP addresses, ignoring other IP addresses. You can also accept messages without notifying the sender that the message has been filtered through a non-delivery (NDR) response. This option can improve network and server performance if you have a lot of filtered mail.

Individual e-mail addresses can be specified, as can domain names using wildcard characters, e.g., *@domain.com. This is also configured in System Manager. Messages can be kept in an archive, but old messages are not automatically deleted.

Unfortunately, Exchange 2000 filters by the address of the sender and most spammers use invalid addresses. Often, the reply address is abandoned as soon as the mailing is done. Exchange really doesn't have sufficient tools to fight spam. Plus,

relying on the server to process and filter out junk mail and computer viruses takes system resources better spent processing valid e-mail. To improve its capabilities, the enterprise may opt to purchase an add-on software package, like MailEssentials, which is a content filtering management package, or to implement an e-mail gateway.

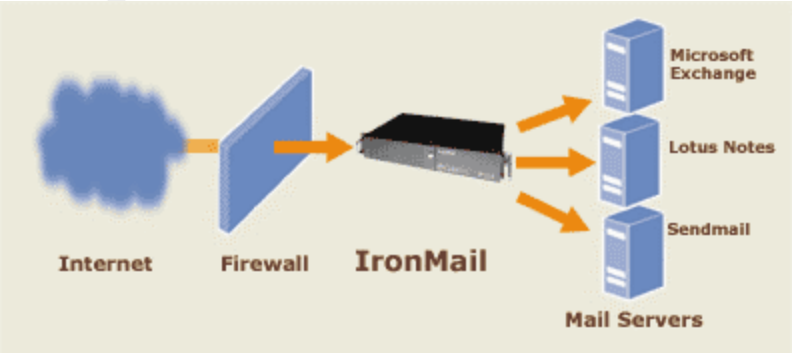
INTEGRATED SYSTEM ANTI-SPAM "SOLUTIONS" FOR THE NETWORK

There is a growing number of integrated system "solutions" (quotes used because there is no sure-fire solution available against spam). Examples of such solutions are CipherTrust's IronMail, by CipherTrust; McAfee's e500; and Symantec SMTP Gateway. These, with some variations, provide a pseudo or e-mail firewall for the filtering of messaging protocols, SMTP, HTTP, FTP, and POP3. Each has developed their own methodology for handling junk mail, as part of the overall protection against other vulnerabilities inherent to these protocols. These solutions combine hardware and software that are purchased and maintained by the institution.

E-mail filtering gateways incorporate a great variety of rule sets governing what data can pass through the gateway and also provide a great deal of flexibility. They can be automated but require frequent maintenance by system administrators. They protect the enterprise by preventing undesirable transmissions, including spam, virus-infected e-mails, and backdoors from reaching the e-mail server. They are usually placed at the outer perimeter, just inside the corporate firewall(s). Generally, firewalls do not impede communications, such as e-mail, from entry. Data that is not specifically stopped at the outer firewall is then filtered by the e-mail filtering gateway.

CipherTrust IronMail

As an e-mail gateway, IronMail's emphasis is on protecting the e-mail system both from spam and malicious code. It combines traditional approaches (such as domain blocking lists and content analysis), with "cutting-edge" approaches (such as distributed signature-based detection, heuristics-based anomaly detection, as well as rules-based header analysis).



(CipherTrust)

IronMail includes a hardened mail gateway that acts as an application-specific firewall, allowing only valid connections to the e-mail server. It protects against e-mail

attacks, including buffer overflow, denial of service, malformed MIME headers directed at the internal servers.

The enterprise can apply flexible policy management to determine how to handle spam, which can be deleted or quarantined at the gateway. The Subject line can be changed or appended to facilitate user-defined filtering. Many of its processes are automated, thus removing some of the burden from system administrators.

Technologies Used in IronMail to Detect Spam:

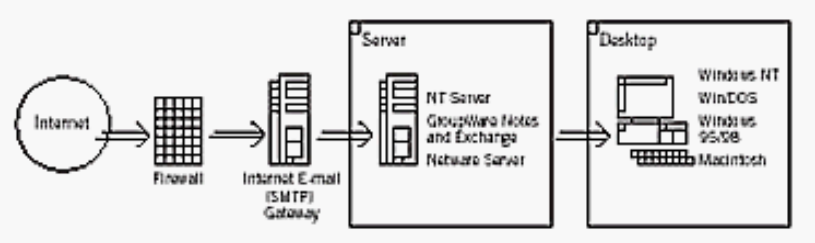
1. **Distributed signature-based spam detection** provides immediate protection against spam floods identified on the Internet. It does this by creating a signature and then uses it to compare against messages received. It incorporates two signature-based spam networks: Vipul's Razor (detection and filtering network) and Distributed Checksum Clearinghouse, DCC, (utilizes fuzzy signatures that use fuzzy logic algorithms that score messages based on signatures found in headers and message body).
2. **Anomaly Detection Engine** identifies patterns of spam propagation (patent pending). It monitors e-mail traffic flows, both inbound and outbound, and makes decisions based on heuristics to identify malicious behavior.
3. **Rules-based header analysis** applies a set of heuristic test to mail headers, looking for specific characteristics or attempts to hide identities. This also uses weighted scoring based on fuzzy logic.
4. **Automated spam-abuse management** proactively protects while it minimizes the administrative work. It can monitor the abuse@domain.com e-mailbox, which receives reports of spam, and parses messages, extracting key information and route traveled. In automatic mode, it automatically creates and enforces a new policy rule that acts on future mailings of type, based on header information. In manual mode, it creates the policy but waits for direction from the system administrator.
5. **Black List Services,** which are based on the sender's IP address, are utilized, such as MAPS, RBL, RSS, and ORBS.
6. **Local deny lists** allow the system manager to build a locally managed list of known spammers based on IP addresses, e-mail addresses, or domain names.
7. **Content analysis** by which messages are scanned for words and phrases.
8. **Reverse DNS** to authenticate incoming connections.

Other options included in IronMail:

1. Messages can be stopped either at the gateway or at the desktop.
2. Messages can be deleted or quarantined. Deleting messages reduces drain on internal networks and mail systems.
3. Labeling mail by modifying the Subject line to warn recipient, thus allowing the user to help manage his own Inbox.
4. Administrator can develop white lists of acceptable commercial e-mails to bypass filters.

Symantec SMTP Gateway

This solution combines virus scanning, filtering, and blocking with remote management, alerts, and reports. As with other e-mail gateways, the SMTP Gateway is hardware placed between the outer corporate firewall(s) and the network server(s). Protection for new and known computer viruses is provided through Symantec Anti-Virus. The Gateway also blocks spam based on specific characters typical of spam. SMTP Gateway provides policy management for scheduling updates and for system and virus alerts.



(Symantec)

Features:

1. **Virus detection** is provided against computer viruses that move amazingly fast through e-mail. It is desirable to stop these at the network level. The SMTP Gateway has the ability to rapidly scan compressed and encoded attachments for viruses. Virus signatures and other updates on the server are updated automatically.
2. **Spam control** is accomplished by utilizing anti-spam lists from Mail Abuse Prevention Systems (MAPS). These lists identify bulk e-mails and stop them from reaching the e-mail servers. System administrators can filter e-mail by sender address and domain, by the subject line, by the attachment, and by the maximum message size.
3. The **secure gateway** provides protection against vulnerability attacks, denial of service attacks, password sniffing, and unauthorized access.
4. **Support** through Symantec Security Response team.

McAfee WebShield e500

McAfee's integrated solution is in their WebShield e500 and e250 appliances combined with McAfee Anti-Virus and content management software. They form an Internet gateway that scans SMTP, FTP, POP3, and HTTP messaging protocols for viruses, malicious code, including ActiveX and JavaScript. Inline scanning requires no configuration at the client workstation. During installation, the system administrator assigns the IP address of the existing firewall to the appliance. The firewall is given a

different IP address. The appliance can also run in proxy mode for scanning so that only the SMTP, HTTP, FTP, and POP3 protocol transmissions pass through WebShield.

Features:

1. **Content scanning and filtering** for viruses and spam with little or no impact on the performance of e-mail servers or firewalls. Filtering can block e-mails containing specific words or phrases, both inbound and outbound. Can prevent transmission of specified types of attachments, e-mails larger than the limit, or e-mails with too many, or too large, attachments, thus conserving bandwidth. Specific spam words and phrases can be blocked.
2. **Support for web browsing**.
3. **Automatic updates** for updating virus signature files.
4. **Spam blocking**. Support for DNS-based black hole lists, such as ORBS. Anti-relay prevents spammers from using your servers and system resources to relay e-mails.
5. Insert **Spam disclaimers** to inbound and outbound e-mails.
6. **Remote manageability**.
7. **Alert notification**.
8. **Reporting**.
9. **Support** through AVERT.
10. Works in concert with McAfee's ePolicy Orchestrator for **graphical reporting** on virus activity at the gateway. Detailed reports provide information on where filtering rules have been triggered and unauthorized attempts to URLs have been made.

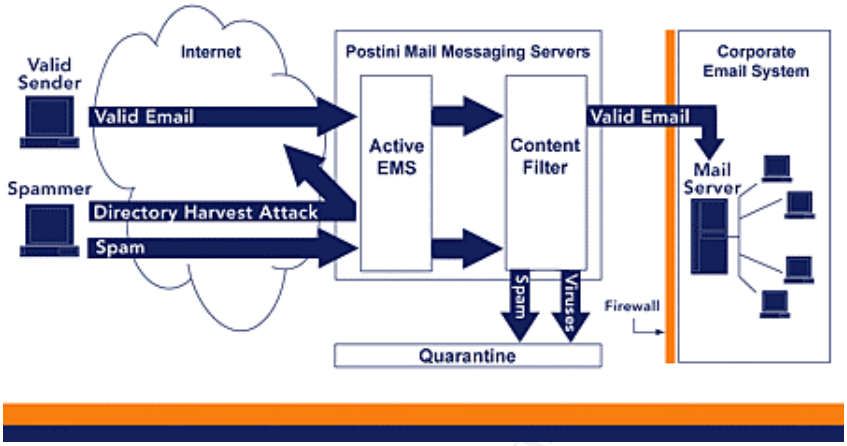
CONTRACTED ANTI-SPAM SERVICES

Another means of countering spam is through real-time services that sit on the SMTP stream outside of the enterprise firewall and are administered by an outside agent. All messages bound for the e-mail server pass through the filtering service. For these, the enterprise can often either sign up on a month-by-month basis or contract for a year or more. Filtering, blocking, and quarantining are done by the service. Total cost of ownership may be less than that of e-mail gateways. Installation is simpler, as is administration, but there are also fewer spam-fighting measures available.

Postini: Integrated E-Mail System Perimeter Service

Postini is an integrated e-mail system perimeter service that provides real-time anti-spam, anti-virus and e-mail system monitoring. The service secures the SMTP connections and content and is platform independent. The service captures spam and quarantines it in the Message Center for later action by the intended recipient. Users can review quarantined messages to determine if they should be delivered or deleted. Postini sits between the Internet and e-mail servers to process messages before they reach the e-mail server. It provides administrative control over e-mail traffic and applications. This service allows system administrators to control global configurations

and user options, but then allows a user to control the degree of filtering applied to spam destined for the Inbox. This allows the user to be part of his/her own solution.



(Postini Corporation)

Features:

- Requires no new hardware of software.
- Identifies and isolates virus-infected messages before they reach your server.
- Processes you messages with minimal latency.
- Infected message are quarantined in a secure, web-based Message Center for access by end-user. The e-mail administrator controls the options available to the user.
- Dedicated connection to McAfee AVERT virus definition servers.
- Works with any e-mail server.
- Detects and diverts junk e-mail before it reaches your e-mail system.
- Real-time heuristics engine analyzes message content, IP header information, envelope information, and source domain.
- Centralized database—no need to maintain or update spam databases
- Requires no new hardware or software.
- Immediate detection and automatic response to directory harvest attacks and other threats.
- Manually blocks known threats and repeat offenders.
- E-mail system load balancing and failover capabilities.
- Detailed usage reports available hourly, daily, or weekly.
- Graphically displays traffic and system activity
- System-wide alerts.
- Web-based remote management through an SSL connection.
- Monitoring and reporting capabilities.
- Trend analysis, usage monitoring, and capacity planning

Brightmail

BrightMail also provides a solution through software and servers with real-time services. It sells its anti-spam service, which includes three components: Probe Network, Bright Light Operations (BLOC), and the Spam Wall.

The **Probe Network** is a collection of 35 million e-mail addresses used as honeypots to attract and receive spam. Messages are delivered to the **BLOC**, which is staffed by real people 24/7. This human involvement minimizes false positives often encountered when filtering e-mail for spam. **Spam Wall** is server-side software residing within the corporate site that is continually updated by the BLOC.

BrightMail will block known spammers, false headers, and unauthorized relays. Filtering rules are constantly and automatically updated. It doesn't require administrative management. E-mail users choose categories for toggling filters off and on.

COMPARISON OF ANTI-SPAM TOOLS & TECHNIQUES

Anti-Spam Techniques	Exchange/ Outlook	IronMail	Symantec/ SMTP	WebShield E500	Postini	Bright-mail
Action Within Perimeter	Yes	Yes	Yes	Yes	No	Yes
E-Mail Filtering Gateway	-	Yes	Yes	Yes		Yes
Application-specific appliance inside enterprise firewalls	Yes	Yes	Yes	Yes		Yes
Hardened operating system	No	Yes	Yes	Yes		
Load balancing and fault tolerance		Yes	Yes	Yes	Yes	
Inbound messages pass through in-house appliance to mail servers		Yes	Yes	Yes	No	Yes
Action Outside Perimeter	No	No	No	No	Yes	
Custom filtering rules pushed to in-house server						Yes
Service-owned servers	-	-	-	-	Yes	Yes
Anti-spam services outside enterprise firewalls	-	-	-	-	Yes	
Integrates Service with Existing E-Mail MTA	-	No	No	No	No	Yes
Human, at service, define spam (less false positives)						Yes
Messages go directly in-house	Yes	Yes	Yes	Yes	No	Yes
Less time commitment from IT staff					Yes	Yes

Anti-Spam Techniques	Exchange/ Outlook	IronMail	Symantec/ SMTP	WebShield E500	Postini	Bright-mail
Protocols Scanned						
SMTP	Yes	Yes	Yes	Yes	Yes	
HTTP	No	Yes	Yes	Yes	No	
FTP	No	Yes	Yes	Yes	No	
POP3	No	Yes	Yes	Yes	No	
Virus/Malware						
Disinfecting/Deleting	Software purchase	Sophos	Symantec	McAfee	McAfee	Symantec
Attachment scanning	Software purchase	Sophos	Symantec	McAfee	McAfee	Symantec
Protection against malicious code/behavior	Software purchase	Sophos	Symantec	McAfee	McAfee	Symantec
Protects against buffer overflows		Yes	Yes	Yes		
Protects against sniffer attacks		Yes	Yes		Yes	
Automatic AV updates	Software purchase	Yes	Yes	Yes	Yes	Yes
Anti-Spam						
Accept messages without notifying sender of filtering (550)	Yes *				Yes	
Anti-open relay	Yes	Yes	Yes	Yes	Yes	
Reverse DNS lookup		Yes	Yes	Yes		
Protects against e-mail denial of service attack		Yes	Yes	Yes		
Labeling spam by modifying subject line		Yes				
Rules-Based Filtering:						
Attachments	Some	Yes	Yes	Yes	Yes	
Block bulk mailings		Yes	Yes		Yes	Yes
Rule-sets developed and maintained by human interaction	Little				User	Service/ User
Automated rule-sets	-	Yes	Yes	Yes	Yes	No
IP address		Yes	Yes	Yes		
Blind carbon copy		Yes				
Domain name	Some	Yes	Yes	Yes		
Sender	Yes	Yes	Yes	Yes		
Subject	Little	Yes	Yes	Yes		
Content filtering or header/ body	Little	Yes	Yes	Yes	Yes	
Alerts & Notifications		Yes	Yes	Yes	Yes	
Allows White Lists		Yes			Yes	
Black Hole List Support		Yes	Yes	Yes	Yes	
Disclaimer Support		Yes		Yes	Yes	
E-Mail Policy Management		Yes	Yes	Yes	Yes	
End-User Configurable	Little				Yes	Yes
Logging		Yes	Yes	Yes	Yes	
Management Reporting		Yes	Yes	Yes	Yes	
Monitors Inbound Messages		Yes	Yes	Yes	Yes	
Monitors Outbound Messages		Yes	Yes	Yes	Yes	
OWA Protection		Yes		Yes	Yes	
Quarantine Messages		Yes		Yes	Yes	Yes

Anti-Spam Techniques	Exchange/ Outlook	IronMail	Symantec/ SMTP	WebShield E500	Postini	Bright-mail
User has Remote Access to Quarantined Messages					Yes	
Remote Manageability		Yes	Yes	Yes	Yes	

* Microsoft claims "yes" but Postini technician reports that Exchange doesn't allow 550 error coding but sends NDR's.
Information based on findings in research. Blanks indicate no reference found.

ANTI-SPAM STRATEGIES FOR THE END-USER

User-Configured Filtering Add-ons: GFI MailEssentials/MailSecurity Bundle

There are a few software add-ons for Microsoft Exchange, which provide some degree of protection from spam. **MailEssentials**, by Gfi, installs on the corporate Exchange server, and provides basic anti-spam defense, disclaimers on all outbound messages, blocking of specified attachments, and other anti-spam measures. It is transparent to the user. **MailSecurity** can be bundled with MailEssentials to provide additional protection, such as content checking, exploit detection, threats analysis, and an anti-virus solution. MailSecurity, gateway version, is deployed at the perimeter of the network as a mail relay server. It scans both inbound and outbound e-mail.

Training the User

Developing Acceptable Use e-mail policies and making sure the e-mail user knows the appropriate use of e-mail can also be valuable tools. Important training will teach the user how to identify spam and how to handle and/or complain about it. It's important to provide an abuse@domain.edu mailbox to receive complaints of junk mail. Providing the user with a list of Do's and Don'ts for dealing with spam is helpful regardless of what strategies are used against spam. The following list is a compilation from various sources:

- **Do** use the delete key.
- **Do Not** buy anything from spammers.
- **Do** capture the full header for reporting spam. Full headers are necessary in determining the route and source of the spam.
- **Do** report spam to the proper place and tell them where.
- **Do Not** reply to spam e-mail, even to use an unsubscribe option in the e-mail. This confirms an address to a spammer and often results in more spam.
- **Do Not** shop online at work or register on websites unless the site is related to work.
- **Do** read Privacy Statements on web pages to learn how the business plans to use your information.
- **Do Not** sign up with special web sites that say that they will get you removed from mailing lists. They are just as likely to be collecting addresses.
- **Do** learn to use filters available through your e-mail software.
- **Do Not** publish your e-mail address on a website.
- **Do** be cautious of the listservs and newsgroups to which you subscribe. Spammers troll these lists for addresses.

- **Do** report spam to the proper places.
- If it sounds too good to be true, it probably is.

CONCLUSION

Keeping ahead of spam (or at least trying to) can be an expensive and time-consuming proposition; a little like outsmarting the squirrels. But the action is essential in order to protect expensive system resources and valuable employee productivity. Spam will never decrease as long as the benefits from spamming far outweigh the costs of spamming. Without action, the impact of spam on educational institutions will continue to increase; just like it will everywhere else. First Amendment rights will continue to be argued, and governmental agencies will continue to discuss legislation. But, tomorrow, spam will still be here. Spammers will get more sophisticated and technologically astute, just as fast as computer technology advances. Yet computer technology has given so much to institutions of higher learning that it's imperative that a balance be found-- one that protects computer systems and productivity, yet allows the free flow of information that the Internet and e-mail offer.

Incidentally, I finally found a squirrel-proof birdfeeder. And it works**!** ☺

LIST OF REFERENCES

Borderware Technologies, Inc. "Thirty Six Email Security Risks." URL: http://www.mxtreme.com/. (1 October 2002).

Brightmail, Inc. "The Brightmail Anti-Spam Solution;" "The Spam Problem and Brightmail's Solution; E-Mail for the Twenty-First Century: The Mailwall Solution." Data Sheets. (26 September 2002). URL: http://www.brightmail.com/pdfs/antivirusDatasheet.pdf
http://www.brightmail.com/pdfs/Mailwall_Whitepaper-Jan02.pdf
http://www.brightmail.com/pdfs/Spam_Problem_Whitepaper.pdf
http://www.brightmail.com/press-vpk.html
http://www.brightmail.com/products-as.html
http://www.brightmail.com/index.html

Burton, Tina. Global Internet Project (GIP) Internet Press Release. "Group Says Spam Threatens the Internet." 25 June 2002.
URL: http://www.gip.org/releases/release.asp?PRESS_RELEASE_ID=29.
(7 September 2002).

CipherTrust . White Paper. "IronMail: The Security Appliance for Email." URL: http://www.ciphertrust.com/ironmail/anti-spam.htm. (9 September 2002).

CipherTrust. "IronMail Tech Paper: Anti-Spam Solution." "IronMail Solution: Anti-spam" June 6, 2002.

Cole, Eric. HACKERS BEWARE. New Riders Publishing. New York. 2002. pp114-119.

Cain, Patrick. "Spam: A Service Provider's Prospective." Presentation. 18 June 2002. URL: http://www.gip.org/publications/papers/PatCain-SPAM.ppt. (27 September 2002).

Lemos, Robert. "Spam hits 36 percent of e-mail traffic." eBusiness. 29 August 2002. URL: http://zdnet.com.com/2100-1106-955842.html (3 October 2002).

ePrivacy Group. Publication: "Spam: Are We Still Asking the Wrong Questions?" http://www.gip.org/publications/papers/StephenCobbSPAM_VS_061802a.ppt
(30 September 30, 2002).

FTC, Federal Trade Commission: Facts for Consumers. "You've Got Spam: How to 'Can' Unwanted Email." April 2002. URL: http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm. (30 September 2002).

GFi. MailEssentials/MailSecurity for Exchange/SMTP 7. 28 September 2002. URL:
http://www.gfi.com/mes/index.html
http://www.gfi.com/mailsecurity/index.html

Graff, Joyce. "Controlling Spam: An Introduction." Gartner. 12 May 2000.

Gurley, J. William. CNET Tech News. "Time to put a stop to spam." 3 April 2002. URL: http://news.com.com/2010-1072-874374.html. (30 September 2002).

LII, legal information institute. "first amendment: an overview." 27 September 2002. URL: http://www.law.cornell.edu/topics/first_amendment.html. (24 August 26 2002).

ITAA, Information Technology Association of America. Press Release. "Internet Group Says Spam Threatens the Internet." 25 June 2002. URL:http://www.gip.org/releases/release.asp?PRESS_RELEASE_ID=29. (30 September 2002).

Microsoft Corporation. "XADM: How to Filter Junk Mail in Exchange 2000." Microsoft Knowledge Base Article - Q276321. 12 October 2000. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;q276321. (23 August 2002).

Microsoft Corporation. Microsoft. "XADM: How to Modify Global Settings in Exchange System Manager." Knowledge Base Article - Q258696. 29 March 2000. URL: http://support.microsoft.com/default.aspx?scid=kb;[LN];Q258696. (23 August 2002).

Microsoft Corporation. "OL2000: How to Filter Junk and Adult Content E-mail." Microsoft Knowledge Base Article - Q195398. 6 November 1998. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;q195398. (23 August 2002).

Mueller, Scott Hazen, Editor-in-Chief. "What is Spam?." URL: http://spam.abuse.net/overview/whatisspam.shtml. (27 September 2002).

McAfee. "McAfee WebShield Appliances". Data Sheet. McAfee, Inc. URL: http://download.nai.com/products/media/mcafeeb2b/pdf/webshield-appliances.pdf. (27 September 2002).

Olsen, Florence. "Fed Up With Spam." The Chronicle of Higher Education. Issue Date: 27 September 2002.

Patrick, John. "The Spam Has Got To Go." 15 June 2002. URL: http://patrickweb.com/weblog/stories/2002/06/15/theSpamHasGotToGo.html. (23 August 2002).

Petersen, Rodney. University of Maryland OutlookOnline. "Junk E-Mail Hits University." 7 April 1998.

Postini Corporation. "Enhanced Messaging." Postini Corporation. URL: http://www.postini.com/services/messaging.pdf. (29 September 2002).

Postini Corporation. "Directory Harvest Attacks: Email's Silent Security Killer." White Paper. URL: http://www.postini.com/services/dha_wp.pdf (13 September 2002). URL: http://www.postini.com/services/ems/how_it_works.html (3 October 2002)

Postini Corporation. "Postini Email Stat Track." 3 October 2002. URL: http://www.postini.com/stats/index.html

Sorkin, David E. Spam Laws. http://www.spamlaws.com/ 25 September 2002.

URL: http://www.spamlaws.com/state/summary.html#md: (22 September 2002).
URL: http://www.spamlaws.com/federal/index.html (22 September 2002).

Symantec, Inc. "Symantec AntiVirus™ for SMTP Gateways." Fact Sheet. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=164 (27 September 2002).

The Anti-Spam Home Page. "Spam Do's and Dont's." 28 September 2002.
URL: http://www.arachnoid.com/lutusp/antispam.html#overview_dos_donts

Thibodeau, Patrick. ComputerWorld: "FTC launches antispam attack, but critics skeptical." 12 February 2002. URL:
http://www.computerworld.com/softwaretopics/software/story/0,10801,68241,00.html. (27 August 2002).

UMD, University of Maryland. Helpdesk. Office of Information Technology. "About Reverse Lookup." 29 March 2002.

University of Maryland. Helpdesk. Office of Information Technology. "Open Relaying Background." 20 August 2002.

Warner, Brianne. UMD Diamondback. "You've got Spam: Dealing with unwanted e-mail." 30 November 1999.

Graphics

ClickArt:125,000 Deluxe Image Pak. Broderbund.

http://www.cnn.com/TECH/computing/9809/22/spamcontrol.idg/
http://www.cnn.com/TECH/computing/9806/30/diy.spam.idg/
http://www.cnn.com/TECH/computing/9806/30/diy.spam.idg/index.html

http://www.polen-scout.de/intern/spam.html

http://www.jfservice.com.br/arquivo/informatica/dicas/2000/10/26-Spam/

Useful Sites:

Mail Abuse Prevention System (MAPS) http://mail-abuse.org/.
Open Relay Behaviour-modification System (ORBS) http://www.ordb.org/.

Last Updated: July 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
Security Awareness Summit & Training 2017	OnlineTNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced