# INFORMATION TECHNOLOGY SUPPORT SERVICE

## Level - I

# LEARNING GUIDE 35

| | |
|---|---|
| **Unit of Competence:** | **Protect Application or System Software** |
| **Module Title:** | **Protecting Application or System Software** |
| **LG Code:** | **ICT ITS1 M09 LO3 – LG35** |
| **TTLM Code:** | **ICT ITS1 TTLM 1019v1** |

## LO 3: Identify and Take Action to Stop Spam

| Instruction Sheet | Learning Guide 35 |
|---|---|

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics –

- Define and Identify common types of spam
- Spam Control and combat
- Configure and use spam filters
- Report spam

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Define and Identify common types of ***spam***
- Take ***appropriate action*** in order to protect unauthorized access of spammers
- Configure and use spam filters
- Report and document spam to identify the security threats and be able to perform recommended action

Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 6.
3. Read the information written in the information “Sheet 1 and Sheet 2” in page 3 and 9 respectively.
4. Accomplish the “Self-check 1and Self-check 2” in page 7 and 12 respectively
5. If you earned a satisfactory evaluation from the “Self-check” proceed to “Operation Sheet 1, Operation Sheet 2 and Operation Sheet 3” in page 23
6. Do the “LAP test” in page

| Information Sheet - 1 | Define and Identify Common Types of Spam |
|---|---|

## 1.1. Definition of Spam

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. It is the electronic equivalent of receiving “junk” mail in your letter box. While the most widely recognized form of spam is ***e-mail spam***, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam and file sharing network spam.

Spamming is economically viable to advertisers because their operating costs are so low, and it is difficult to hold senders accountable for their mass mailings. Spam can be used to spread computer viruses, Trojan horses or other malicious software. The objective may be identity theft, or worse. Some spam attempts to capitalize on human greed whilst other attempts to use the victims' inexperience with computer technology to trick them (phishing).

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.

Most spam is **commercial advertising**, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

## 1.2. Types of Spam

There are **four common types of spam**, and they have different effects on users.

### 1.2.1. Cancellable Usenet spam

Cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. (Through long experience, Usenet users have found that any message posted to so many newsgroups is often not relevant to most or all of them.) Usenet spam is aimed at "**lurkers**", people who read newsgroups but rarely or never post and give their address away. Usenet spam robs users of the utility of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts. Furthermore, Usenet spam subverts the ability of system administrators and owners to manage the topics they accept on their systems.

### 1.2.2. Email Spam

Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Email spams typically cost users money out-of-pocket to receive. Many people - anyone with measured phone service - read or receive their mail while the meter is running, so to speak. Spam costs them

additional money. On top of that, it costs money for ISPs and online services to transmit spam, and these costs are transmitted directly to subscribers.

One particularly **nasty variant of email spam is sending spam to mailing lists (public or private email discussion forums.)** Because many mailing lists limit activity to their subscribers, spammers will use automated tools to subscribe to as many mailing lists as possible, so that they can grab the lists of addresses, or use the mailing list as a direct target for their attacks.

### 1.2.3. Instant Messaging Spam

Some examples of instant messengers are Yahoo! Messenger, AIM, Windows Live Messenger, Tencent QQ, ICQ, XMPP and Myspace chat rooms. All are targets for spammers. Many IM systems offer a directory of users, including demographic information such as age and sex. Advertisers can gather this information, sign on to the system, and send unsolicited messages, which could include commercial scam-ware, viruses, and links to paid links for the purpose of **click fraud**. Microsoft announced that the Windows Live Messenger version 9.0 would support specialized features to combat messaging spam. In most systems users can already block the vast majority of spam through the use of a **whitelist**. Whitelisting is the act of authorising contact.

### 1.2.4. SMS & MMS Spam

SMS (Short Messaging Service) is a mechanism which allows brief text messages to be sent to a mobile phone. MMS (Multimedia Messaging Service) can include including videos, pictures, text pages and sound.

Mobile phone spam is a form of spamming directed at these messaging services of mobile telephony. It is described as mobile spamming, SMS spam, text spam, or SpaSMS but is most frequently referred to as m-spam. These types of spam can be particularly annoying for the recipient because, unlike email, some recipients may be charged a fee for every message received, including spam!

## 1.3. Reasons Make Spam Bad

Why do we get so upset when we receive E-mail which was not requested?

There are several reasons:

- **The Free Ride.** E-mail spam is unique in that the receiver pays so much more for it than the sender does. For example, AOL has said that they were receiving 1.8 million spams from Cyber Promotions per day until they got a court injunction to stop it. Assuming that it takes the typical AOL user only 10 seconds to identify and discard a message, that's still 5,000 hours per day of connect time per day spent discarding their spam, just on AOL. By contrast, the spammer probably has a T1 line that costs him about $100/day. No other kind of advertising costs the advertiser so little and the recipient so much. The

closest analogy I can think of would be auto-dialing junk phone calls to cellular users (in the US, cell phone users pay to receive as well as originate calls); you can imagine how favorably that might be received.

- **The “Oceans of Spam" Problem.** Many spam messages say “please send a REMOVE message to get off our list." Even disregarding the question of why you should have to do anything to get off a list you never asked to join, this becomes completely impossible if the volume grows. At the moment, most of us only get a few spams per day. But imagine if only 1/10 of 1 % of the users on the Internet decided to send out spam at a moderate rate of 100,000 per day, a rate easily achievable with a dial-up account and a PC. Then everyone would be receiving 100 spams every day. If 1% of users were spamming at that rate, we'd all be getting 1,000 spams per day. Is it reasonable to ask people to send out 100 “remove" messages per day? Hardly. **If spam grows, it will crowd our mailboxes to the point that they're not useful for real mail**. Users on AOL, which has a lot of trouble with internal spammers, report that they're already nearing this point.

- **The Theft of Resources.** An increasing number of spammers, such as **Quantum Communications**, send most or all of their mail via innocent intermediate systems, to avoid blocks that many systems have placed against mail coming directly from the spammers' systems. (Due to a historical quirk, most mail systems on the Internet will deliver mail to anyone, not just their own users.) This fills the intermediate systems' networks and disks with unwanted spam messages, takes up their managers' time dealing with all the undeliverable spam messages, and subjects them to complaints from recipients who conclude that since the intermediate system delivered the mail, they must be in league with the spammers.

  Many other spammers use **“hit and run"** spamming in which they **get a trial dial-up account at an Internet provider for a few days, send tens of thousands of messages, then abandon the account** (unless the provider notices what they're doing and cancels it first), leaving the unsuspecting provider to clean up the mess. Many spammers have done these tens or dozens of times, forcing the providers to waste staff time both on the cleanup and on monitoring their trial accounts for abuse.

- **It's All Garbage.** The spam messages I've seen have almost without exception advertised stuff that's **worthless**, deceptive, and partly or entirely fraudulent. (I include the many MLMs in here, even though the MLM-ers rarely understand why there's no such thing as a good MLM). It is spam software, funky miracle cures, off-brand computer parts, vaguely described get rich quick schemes, dial-a-porn, and so on downhill from there. It's all stuff that's too cruddy to be worth advertising in any medium where they'd actually have to pay the cost of the ads. Also, since the cost of spamming is so low, there's no point in targeting

your ads, when for the same low price you can send the ads to everyone, increasing the noise level the rest of us have to deal with.

- **They're Crooks.** Spam software invariably comes with a list of names falsely claimed to be of people who've said they want to receive ads, but actually consisting of **unwilling victims culled at random from usenet or mailing lists**. Spam software often promises to run on a provider's system in a way designed to be hard for the provider to detect so they can't tell what the spammer is doing. Spams invariably say they'll remove names on request, but they almost never do. Indeed, people report that when they send a test “remove" request from a newly created account, they usually start to receive spam at that address.

  Spammers know that **people don't want to hear from them,** and generally **put fake return addresses** on their messages so that they don't have to bear the cost of receiving responses from people to whom they've send messages. Whenever possible, they use the **“disposable" trial ISP accounts** mentioned above so the ISP bears the cost of cleaning up after them. It's hard to think of **another line** of business where the **general ethical level is so low**.

- **It Might Be Illegal.** Some kinds of spam are illegal in some countries on the Internet. Especially with **pornography**, mere possession of such material can be enough to put the recipient in jail. In the United States, child pornography is highly illegal and we've already seen spammed child porn offers.

| Self-Check - 1 | Written Test |
|---|---|

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. _____ is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately.
2. List and explain the four common types of spam

   **1.** _____

   _____

   _____

   _____.

   **2.** _____

   _____

   _____

   _____.

   **3.** _____

   _____

   _____

   _____.

   **4.** _____

   _____

   _____

   _____.

3. Why do we get so upset when we receive E-mail which was not requested?

   - _____
   - _____
   - _____
   - _____
   - _____
   - _____

**Answer Sheet**

| |
|---|
| **Score = _____** |
| **Rating: _____** |

Name: _____ Date: _____

**Short Answer Questions**

| Information Sheet - 2 | Spam Control and Combating |
|---|---|

## 2.1. Spam Control

**Spam** is flooding the Internet with many copies of the same message, in a Spam now constitutes an overwhelming majority of **email traffic**.

### 2.1.1. The Effects of Spam

The never-ending onslaught of junk messages:

- Strains networks
- Erodes user productivity
- Propagates dangerous malware and costs business millions of dollars.

### 2.1.2. Types of Spam

Though all junk email might look the same, spam continues to arrive in a seemingly endless number of configurations, ranging from the innocuous to the lethal. The major spam types include:

- **Advertising Spam**: is used to promote an entire spectrum of products and services, from software to real estate to questionable medical and nutritional offerings.
- **Malware Delivery**: Spam is one of the main distribution channels for delivering viruses and other types of malware. Targeted individuals, believing they have received an important document or media file, are often tricked into opening a malware attachment.
- **Scams**: Posing as Nigerian princes, Swiss bankers, tragically ill children and other stock types, scammers prey on recipients' sympathy and greed.
- **Phishing**: Hiding behind the names of respected retailers, financial institutions, businesses, charities and government bodies. **Phishers** attempt to lure unsuspecting recipients to bogus Web sites where they steal personal financial or identity information.
- **Nonsense**: A significant chunk of junk-mail text is pure gibberish. Some of this material is generated in an effort to trick **spam-filtering technologies** into passing an attached message onto recipients. Many nonsensical messages seem to exist for no purpose at all.

### 2.1.3. Spam Media

Spam is overwhelmingly an email problem. Yet as Internet technology advances, junk content is rapidly spilling over to many other types of IP media, including:

- **IM (instant messaging)** : Spam is a growing problem on IM networks, where the threats closely parallel those of email spam.

- **VoIP** Voice over IP: SPIT (Spam over Internet Telephony) is a rare but potentially dangerous form of spam that threatens to annoy users and jam voice-mail inboxes.
- **Search Engines**: Using techniques such as hidden text, doorway pages and mirror sites, a search-engine spammer attempts to boost a Web site's ranking by redirecting traffic to the site. This practice is also known as "spamdexing."
- **Web Message Boards**: Spammers like to use Web message boards and Usenet.com groups to promote products and services that are usually unrelated to the site's content focus.
- **Blogs**: Junk advertising is inserted into a blog's reader-comment area.
- **Online Video**: YouTube LLC and other video-sharing sites are plagued by video spam, which consists of thinly disguised commercials for products and services of dubious value.

### 2.2. Combating Spam

It sometimes seems as if **anti-spam technologies** and methodologies are proliferating as rapidly as spam itself. These are the main tools that can keep spam under control:

- **Spam Filters**: A growing number of technology vendors are targeting spam with products that are designed to block and quarantine suspected spam. These offerings use sophisticated algorithms to scan each incoming message for signs that it may contain spam.
- **Firewalls**: **Spam firewalls** offload message filtering from the email server, freeing up network resources and bandwidth. Spam-firewall appliances usually come preconfigured and can be set up in minutes. Maintenance is usually minimal.
- **Anti-Malware Technologies**: Hardware- and software-based anti-malware products can block dangerous attachments from reaching employees' inboxes.
- **Client Control**: Leading email clients, such as Microsoft Outlook and Outlook Express, as well as Mozilla Foundation's Thunderbird , offer built-in controls that are designed to minimize inbox spam.
- **White Lists/Black Lists**: This feature is found in many spam filters and client controls. White lists of trusted email addresses allow messages to proceed to the user's inbox unimpeded by any filter or client settings. Black lists work in the opposite way, routinely blocking incoming email from known offenders.
- **Disposable Email Addresses**: Many businesses and individuals routinely distribute different email addresses to every external contact, then funnel all incoming messages into a single account. This way, if one address begins spamming, it can be safely eradicated without affecting the flow of messages originating from other contacts.

- **Legal Action** : While it's rare for an individual business to sue a junk-mail sender, a growing number of law-enforcement bodies are targeting spammers, particularly organized crime rings that use the technology for financial and identity theft.
- **Policies**: All businesses need a comprehensive anti-spam policy. Besides mandating the use of filtering and other good spam-fighting technologies, the policy should cover routine workplace practices. **Business Web sites, for example, should never publish visible email addresses that can be "harvested" by spammer software.** Employees should also be encouraged not to post business email addresses on message boards, social-network sites and personal Web pages.
- **Education**: The simple task of teaching employees to be wary of phishing messages, and not to open unknown attachments, can help any business minimize spam's impact.

### 2.3. 12 Tips for Fighting Spam

Fighting spam involves diligence in using anti-malware applications and keeping them, your operating system and applications updated, as you will see:-

- Use filtering software - Most e-mail programs have an automatic spam filtering function. Internet service providers can also install mail filters in their mail transfer agents as a service to all of their customers. Due to the growing threat of fraudulent websites, Internet service providers filter URLs in email messages to remove the threat before users click. Corporations often use filters to protect their employees and their information technology assets. There are 3rd party spam filters available as well – among them SpamAssassin and Norton Internet Security.
- Install anti-virus software and keep it updated
- Use a personal firewall – available in Windows and Mac Operating Systems
- Download security patches – these address known issues as they come to hand
- Choose long and random passwords that involve letters, numbers and symbols
- Protect your email address
  - ✓ Be careful about to whom you give your email address.
  - ✓ When it is necessary to forward messages to bulk recipients who don't know one another, it is good practice to list the recipient names in the "BCC:" field instead of after "TO:". Unscrupulous recipients will not be able to see or copy that list of email addresses.
  - ✓ Avoid responding to spam; even be careful about “unsubscribing” in a suspect email.
  - ✓ Beware of contact forms on websites, they may be harvesting your details, nor can you see the address you are sending to in some cases.

- ✓ Using HTML in email allows web browser functionality such as the display of html, URLs and images. Mail clients which do not automatically download and display HTML, images or attachments, have fewer risks, as do clients who have been configured to not display these by default.

- Protect your mobile phone number
  - ✓ A helpful SMS spam-reduction technique is guarding one's mobile phone number. One of the biggest sources of SMS spam is number harvesting carried out by Internet sites offering "free" ring tone downloads. In order to facilitate the download, users must provide their phones' numbers; which in turn are used to send frequent advertising messages to the phone.
  - ✓ Another countermeasure is to use a service that provides a public phone number and publishes the SMS messages received at that number to a publicly accessible website. Google Voice can be used in this way, but with numbers and messages kept private. (At the time of writing Google Voice is not fully operational in Australia.
- Read terms and conditions carefully - Often the terms and conditions will contain a clause that reveals the intent to put a user's contact details into a mailing list.
- Beware of email scams and fraud –
- Don't open suspicious attachments
- Don't "unsubscribe" if the source seems dubious. Just delete it. The unsubscribe link or button may simply confirm the validity of your contact details.
- Report any email, instant messaging, SMS and MMS spam to the concerned body

| Self-Check - 2 | Written Test |
|---|---|

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. List The Effects of Spam

_____

_____

_____

2. List and explain Spam Media

_____

_____

_____

_____

_____

_____

3. list and describe the main tools that can keep spam under control:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

**Answer Sheet**

| |
|---|
| **Score = _____** |
| **Rating: _____** |

Name: _____ Date: _____

**Short Answer Questions**

| Information Sheet - 3 | Configuring and Using Spam Filters |
|---|---|

## 3.1. Anti-Spam Techniques

Various anti-spam techniques are used to prevent email spam (unsolicited bulk email).

No technique is a complete solution to the spam problem, and each has trade-offs between incorrectly rejecting legitimate email (false positives) as opposed to not rejecting all spam (false negatives) – and the associated costs in time, effort, and cost of wrongfully obstructing good mail.

Anti-spam techniques can be broken into four broad categories:

- ***End-User Techniques***: those that require actions by individuals,
- ***Automated techniques for email administrators***: those that can be automated by email administrators,
- ***Automated techniques for email senders***: those that can be automated by email senders and
- Those employed by researchers and law enforcement officials.

### 3.1.1. End-User Techniques

There are a number of techniques that individuals use to restrict the availability of their email addresses, with the goal of reducing their chance of receiving spam.

- Discretion
- Address Munging
- Avoid Responding to Spam
- Contact Forms
- Disable HTML in Email
- Disposable Email Addresses
- Ham Passwords
- Reporting Spam

### 3.1.2. Automated Techniques for Email Administrators

There are now a large number of applications, appliances, services, and software systems that email administrators can use to reduce the load of spam on their systems and mailboxes. In general these attempt to reject (or "block"), the majority of spam email outright at the SMTP connection stage. If they do accept a message, they will typically then analyze the content further – and may decide to "quarantine" any categorized as spam.

- Authentication
- Challenge/Response Systems
- Checksum-Based Filtering
- Country-Based Filtering
- DNS-Based Blacklists

- URL Filtering
- Strict Enforcement of RFC Standards
  - ✓ *Greeting delay*.
  - ✓ *Temporary rejection*
  - ✓ *HELO/EHLO checking*
  - ✓ *Invalid pipelining*
  - ✓ *Nolisting*
  - ✓ *Quit detection*
- Honeypots
- Hybrid Filtering
- Outbound Spam Protection
- PTR/Reverse DNS Checks
- Rule-Based Filtering
- SMTP Callback Verification
- SMTP Proxy
- Spamtrapping
- Statistical Content Filtering
- Tarpits

### 3.1.3. Automated Techniques for Email Senders

There are a variety of techniques that email senders use to try to make sure that they do not send spam. Failure to control the amount of spam sent, as judged by email receivers, can often cause even legitimate email to be blocked and for the sender to be put on DNSBLs.

- Background Checks on New Users and Customers
- Confirmed Opt-In for Mailing Lists
- Egress Spam Filtering
- Limit Email Backscatter
- Port 25 Blocking
- Port 25 Interception
- Rate Limiting
- Spam Report Feedback Loops
- FROM Field Control
- Strong AUP and TOS Agreements

## 3.2. Managing SPAM

There are a number of ways that SPAM and other email threats can be managed. Most anti-virus software programs contain some sort of SPAM management functionality as well as most Email programs. In the following pages, we will demonstrate the email management processes of Microsoft Outlook 2010.

### 3.2.1. Managing Junk Email

As SPAM or other unsolicited Emails are received, Outlook 2010 allows us to block or quarantine the sender so as to remove our exposure to risk or annoyance in future.

### 3.2.2. Automatic blocking

Unfortunately, the lovely folk who like to send us message after message about cheap pharmaceuticals do not always use the same address. So we block one, another appears in our inbox. To counter this, we can set up some automatic blocking processes to block emails by type rather than sender.

| Self-Check - 3 | Written Test |
|---|---|

**Directions:** Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. List the four broad categories anti-spam techniques:

_____

_____

_____

_____

2. List the techniques that individuals use to restrict the availability of their email addresses, with the goal of reducing their chance of receiving spam.

_____

_____

_____

_____

_____

_____

_____

_____

3. List the techniques that email senders use to try to make sure that they do not send spam.

_____

_____

_____

_____

_____

_____

_____

_____

**Answer Sheet**

| |
|---|
| **Score = _____** |
| **Rating: _____** |

Name: _____ Date: _____

**Short Answer Questions**

| Information Sheet - 4 | Reporting SPAM |
|---|---|

### 4.1. Junk Email

Like everything, there are a number of risks that go with having your own email address. As you give your email address to others, use it online to purchase items or use it as a contact point for entry into competitions, you open yourself up to a bombardment of "Junk" email.

Junk email can include:

- Subscriptions to company information sites and online brochures (the online version of junk mail).
- Spam - A process for sending unsolicited messages (usually for cheap online pharmaceuticals, scams or x rated sites) to many recipients at once. SPAM covers emails, instant messaging, SMS and other mobile phone messaging.
- Distribution of malicious software such as viruses.
- Hoax emails (such as emails requesting online banking details etc.).

### 4.2. Legal Countermeasures

If an individual or organization can identify harm done to them by spam, and identify who sent it; then they may be able to sue for a legal remedy, e.g on the basis of trespass to chattels. A number of large civil settlements have been won in this way, although others have been mostly unsuccessful in collecting damages.

Criminal prosecution of spammers under fraud or computer crime statutes is also common, particularly if they illegally accessed other computers to create botnets, or the emails were phishing or other forms of criminal fraud.

Finally, in most countries specific legislation is in place to make certain forms of spamming a criminal offence, as outlined below:

- **European Union**

  Article 13 of the European Union Directive on Privacy and Electronic Communications (2002/58/EC) provides that the EU member states shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

  In the United Kingdom, for example, unsolicited emails cannot be sent to an individual subscriber unless prior permission has been obtained or unless there is a pre-existing commercial relationship between the parties.

- **United States**

  In the United States, many states enacted anti-spam laws during the late 1990s and early 2000s. All of these were subsequently superseded by the CAN-SPAM

Act of 2003, which was in many cases less restrictive; and any further potential state laws preempted. However, CAN-SPAM leaves intact laws not specific to e-mail. Courts have ruled that spam is, e.g., Trespass to Chattel.

Bulk commercial email does not violate CAN-SPAM, provided that it meets certain criteria, e.g., a truthful subject line, no forged information in the headers. If it fails to comply with any of these requirements it is illegal. Those opposing spam greeted the new law with dismay and disappointment, almost immediately dubbing it the "You Can Spam" Act.

In practice it had little positive impact. In 2004, less than one percent of spam complied with CAN-SPAM, although a 2005 review by the Federal Trade Commission claimed that the amount of sexually explicit spam had significantly decreased since 2003 and the total volume had begun to level off. Many other observers viewed it as having failed, although there have been several high-profile prosecutions.

- **Australia SPAM Act 2003**

As a result of increasing instances of unsolicited bulk email flooding company and personal networks, the Australian Federal Government introduced the SPAM Act. The Spam Act became law on 12 December 2003 and, after a grace period; all provisions of the Spam Act came into effect from 10 April 2004 and covers the following message types:

- Email
- Short message service (SMS)
- Multimedia message service (MMS)
- Instant messaging (IM)

In simple terms, the SPAM Act covers the following:

1. Unsolicited commercial electronic messages must not be sent. Messages should only be sent to an address when it is known that the person responsible for that address has consented to receive it.
2. Businesses must not use electronic address harvesting software. or lists which have been generated using such software, for the purpose of sending unsolicited commercial electronic messages.
3. Commercial electronic messages must contain
    - Accurate information about the sender of the message;
    - A functional way for the message's recipients to indicate that they do not wish to receive such messages in the future - that they wish to unsubscribe.

The maximum penalties under the Spam Act include a range of warning and breach options up to a Court imposed penalty of up to $220,000 for a single day's contraventions up to $1.1 million for a second offence.

### 4.3. Reporting SPAM

Tracking down a spammer's ISP and reporting the offense can lead to the spammer's service being terminated and criminal prosecution. Unfortunately, it can be difficult to track down the spammer, and while there are some online tools such as Spam Cop and Network Abuse Clearinghouse to assist, they are not always accurate. Historically, reporting spam in this way has not played a large part in abating spam, since the spammers simply move their operation to another URL, ISP or network of IP addresses.

In many countries consumers may also forward unwanted and deceptive commercial email to the authorities, e.g. in the US to the email address (spam at uce.gov) maintained by the US Federal Trade Commission (FTC), or similar agencies in other countries.

Emails inundated with SPAM or other unsolicited messages such hoax emails, they can report it to the Australian Communications and Media Authority by undertaking any of the following

Users forward spam to the ACMA's Spam Intelligence Database using report@submit.spam.acma.gov.au email address.

Note: When forwarding an email message, please do not change the subject line of the message or add additional text. The ACMA will only contact you in relation to a report if it requires further information to assist it in its anti-spam activities.

- Organizations, such as Internet Service Providers or universities, which collect large amounts of spam associated with the management of their email systems can be report to the ACMA via command-line or batch reporting.
- Spam SMS messages can be forwarded to a dedicated telephone number 0429 999 888 to report it directly to the ACMA. Your report will be recorded in the ACMA's database and used to monitor SMS spam activity.

| Operation Sheet - 1 | Filter Incoming Messages in Windows Live |
|---|---|

To organize your Inbox by creating filters to direct incoming messages to specific folders, follow these steps:

1. Sign in to the ***Windows Live Hotmail*** website with your ***Windows Live Hotmail account.***
2. In the upper-right corner of the page, click ***Options***, and then click ***More options***.
3. Under Customize your mail, Click ***Automatically sort e-mail into folders***.
4. Perform one of the actions as per your requirement:
5. Click ***New filter*** to Create a new filter
6. Click ***Edit*** next to the filter that you want to edit.
7. Click ***Delete*** next to the filter that you want to delete.
8. Follow the ***on-screen instructions*** to specify which messages you want to filter and where you want to filter them, and then click ***Save***.

## List of Reference Materials


http://www.bukisa.com/articles/345103_how-to-configure-spam-filter-in-microsoft-outlook#ixzz1CfEcieYW

www.acma.gov.au

http://www.google.com/googlevoice/about.html

www.scamwatch.gov.au