LO3 - ANSWER KEYS:

SELF CHECK 1:

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

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.

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.

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.

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!

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

- **The Free Ride**
- **The “Oceans of Spam" Problem**
- **The Theft of Resources**
- **It's All Garbage**
- **They're Crooks**
- **It Might Be Illegal**

LO3 - ANSWER KEYS:

SELF CHECK 2:

1. List 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. List and explain Spam Media
   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.
3. List and describe 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.

LO3 - ANSWER KEYS:

SELF CHECK 3:

1. List the four broad categories anti-spam techniques:
    - ***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.
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.
    - Discretion
    - Address Munging
    - Avoid Responding to Spam
    - Contact Forms
    - Disable HTML in Email
    - Disposable Email Addresses
    - Ham Passwords
    - Reporting Spam
3. List the techniques that email senders use to try to make sure that they do not send spam.
    - 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