Safety tips for using Email

- ✓ **Avoid exposure of E-Mail account details such as user name and password to unknown /unauthorized persons while using E-Mail.**
- ✓ **Avoid unauthorised disclosure of email contents to protect privacy of information**
- ✓ **Avoid clicking of web-links provided in email messages to prevent secretly installation of a malware (e.g., virus) on your computer**
- ✓ **Install latest Anti-virus/Anti-Spyware software and keep them up-to-date.**
- ✓ **Install personnel (Desktop/user level) Firewall on the system.**
- ✓ **Keep Operating System and application software updated with latest security updates / patches in the computer system used for email to prevent the exploitation of the weakness in the system.**
- ✓ **Be suspicious while opening unexpected emails.**
- ✓ **Do not open suspicious email Attachments.**
- ✓ **Scan an email attachment before opening/downloading to minimize the risk of downloading malware (e.g., virus).**
- ✓ **Use encryption for sending and receiving confidential email to ensure that message can only be read by the intended recipients.**
- ✓ **Do not respond suspicious/banking-related (Phishing)/ winning lottery / fund transfer emails to avoid becoming a victim of financial frauds.**
- ✓ **Do not open untrusted/unknown emails (spam)**
- ✓ **Enable spam filter to reduce amount of spam/junk emails**
- ✓ **Keep strong password with minimum of eight characters, comprising a combination of alphabets (both upper and lowercase), numbers and special-characters.**
- ✓ **Do not keep your computer unattended to avoid misuse**

To minimize the risk of information leakage and account hacking, there are some recommendations to be followed by an user for using email in a secure way. These recommendations are as follows.

1. Avoid Exposer of email account details

While opening an email account, do not expose your account details such as name and password to unauthorised/unknown persons. Ensure that nobody is watching you behind while entering your password. Exposing email account details (such as name or password or both or part of the password) may give way to intruders to hack the email account by guessing password or some password cracking tools.

2. Avoid Unauthorised Disclosure of email contents

Read email only when it is necessary to avoid exposure to third party or unauthorised persons. Many times the content of an email will contain private or confidential data, so to avoid any type of invasion of privacy, be sure to be cautious of your surroundings and never leave a computer unattended. Lock the computer if having to leave it for any length of time.

3. Avoid Clinking web Links in email messages

Avoid clicking or opening web links or program unchecked in email messages. Following the web links or programs that may be part of an email message may lead to secretly installation a malware (e.g., virus) on the computer.

4. Install Anti-virus software

User should Install latest Anti-virus software and Anti-spyware, and keep them updating time to time. Anti-virus software helps to protect computer against known viruses. User can detect and remove the virus before it can do any damage to the computer. Attackers are continually writing new viruses, it is important to keep anti-virus software up-to-date. Anti-virus software such as AVG, Norton Internet Security, Trendmicro, Quick Heal etc are good options. User should not install multiple (more than one) different anti-virus software, as multiple installations may give scanning results against each other.

5. Cautious with email Attachments

Use caution when opening email attachments, even if they appear to have been sent by a known person. Email attachments are a common source of spreading malware such as Virus, Worm and Trojan Horse. Some malware can "spoof" the return address, making it look like the message came from some known source. Take the following precautions:

- Do not open an email attachment If it seems suspicious, even if the scanning result indicates that the attachment is clean because that anti-virus software may not have the signature as new viruses are constantly being released.
- Open attachments that come from a trusted source only (not unsolicited email) as many viruses, worms, and Trojan Horses have been known to attach themselves on to them. Opening an infected email attachment may damage or harm the computer.

6. Scan an email attachment before opening/downloading

Scanning email attachment before opening or downloading minimizes the risk of downloading malware (e.g., virus). Opening or Downloading attachment without scanning may damage the computer if it is infected.

Disable the option to automatically download attachments, if this option is already enabled in the email software.

7. Use Encryption for Sending and Receiving Confidential email

Send and receive confidential or sensitive messages using encryption to ensure that message can only be read by the intended recipients.

Some messages are too sensitive and confidential. User should use encryption for sending sensitive messages. Email Encryption is used to ensure that both sensitive and personal information cannot be seen by anyone other than the intended recipient.

Email encryption is a process where the actual body is coded using an encryption key. An e-mail message appears either blank or with a block random combination of integers and alphabets. It is intended for confidential information between the sender and recipient.

There are few tools and techniques of encryption. Pretty Good Privacy (PGP) is one of the tools to encrypt email messages. The other tools/techniques include public-key encryption like the Secure Sockets Layer (SSL) to encrypt data and PEM (Privacy Enhanced Mail) for encryption, authentication, and certificate-based key management.

The encryption process is as follows. There are two keys: Private Key and Public Key. The sender and the recipient both need to have Private Key and Publick Key in the form of a Digital Signature, a PGP key, or the open version of PGP (Open GPG) key. Both sender and recipient need Public key in each other's repository. The repository is like a key-chain. First step is to exchange each other's public keys between sender and recipient through a signed (but not encrypted) e-mail and import keys into repository. After getting the each other's public keys and putting into repository, create an e-mail as usual and select Encrypt ("Encrypt this to myself,") from the security options and then send the email. The email is encrypted (using a combination of sender's Private key and recipient 's Public key) and then sent to the recipient. When recipient gets the email, the indicator at the recipient's email shows whether or not the e-mail has been tampered with or the certificate is valid (typically a green or red icon in the header). As long as the recipient has the sender's Public key in repository, the e-mail will appear normal, otherwise it will be blank page.

8. Do Not respond Suspicious/Banking-related emails

Many suspicious emails are being sent and forwarded to many email accounts for collecting information. Do not respond or follow such emails.
Emails regarding updation of bank account details or winning lottery or emails from persons (e.g, Nigerians) requesting bank account details for transferring a big amount of money (million dollars) to your account. These are **phishing emails** and are sent from malicious people with intent of collecting bank account details to transfer money from your account to their account. Do not respond/follow such email messages, instead delete them. Keep in mind that bank never sends email messages to any customers/clients asking updatation of account details.

9. Do Not Open Unknown emails

Lot of emails are received from unknown sources/people for advertising, marketing or any other purpose. They are all junk and often frustrating, unsolicited and unwanted emails called **Spam**. Do not open/respond such emails, instead delete them.

10. Enable Spam Filter

Set a Spam filter to reduce "junk" emails that could be part of a potential phishing scam or malware. Enabling spam filter can automatically eliminate a large portion of the risk.

11. Keep Strong Password

Keep a strong password so that it is difficult to guess or memorise by a third party. A strong password should have a minimum of eight characters, comprising a combination of alphabets (both upper and lowercase), numbers and symbols/special-characters, and be as meaningless as possible.

12. Do not keep Computer Unattended

Never keep computer system unattended so that unauthorised persons will not have an opportunity to alter any file or information or do mischievous. Always lock/shut-down the computer when not in use.