Are You Online...?

You decide what information you reveal, when, why, and to whom!

Tips on password

- Passwords should be difficult for others to guess.
- Don't use the same password for every account.
- Create passwords which are long, unique and use a mix of random numbers, and lower and upper case letters.
- Change passwords regularly and don't share them.

Spotting Fake Emails

- The sender's email address doesn't tally with the trusted organisation's website address.
- The email is sent from a completely different address or a free webmail address.
- The email does not use your proper name, but uses a non-specific greeting like "Dear Customer" or "Dear Winner".
- A sense of urgency; eg the threat that unless you act immediately your account may be closed or someone's livelihood endangered.
- A name of a prominent organisation with a forged or fake website link.
- A request for personal information such as user name, password or bank details.
- The email contains spelling and grammatical errors.
- The email indicates you were expecting an email from the sender.
- The entire text of the email is contained within an image rather than the usual text format, which contains an embedded hyperlink to a bogus site.

Do

- Use anti-virus.
- Keep your software updated.
- Ensure that the link label and web address tallies before clicking on it.
- Ensure that data transmissions are made over secured sites.
- Think before sharing information over social networks.
- Be cautious of public Wifi.
- Lock your gadgets with a passcode.
- Consider wiping out data on a gadget remotely if it is lost.
- Control how information is disclosed as many hacks do not involve hi-tech methods.
- Take time to check that you have the correct email address.
- Do online search.
- Turn on firewall.
- Make sure the link is secure before entering payment card details on a website.
- Be conscious of web security.
- Ensure email settings have the requisite security settings, such as encryption of emails.
- Check "From" field when you receive or before sending an email.

Don't

- Click on unsolicited pop-ups, unknown emails, email attachments.
- Click on a link you did not expect to receive.
- Provide information on the website that may open.
- Click on links you are unfamiliar with.
- Use the same passwords for different websites.
- Disclose information unless you're sure of its intended purpose.
- Accept social media invitation if in doubt.
- Store credit card details online.
- Reveal your username and password to anyone.
- Reply to spammer or the sender, for any reason.