Safe and responsible computing

Safe and responsible computing is more important today than ever before.
Here is a short list of DO's and DON'Ts with details to follow.

DO:

✓ USE SAFE EMAIL PRACTICES. There are many important suggestions.

✓ Have a current, updated ANTIVIRUS program.

✓ UPDATE your operating system (Windows or Mac) and keep it current.

✓ BACKUP, BACKUP, BACKUP.

✓ Maintain safe and secure PASSWORDS.

✓ Review and specify CONTROLS AND FEATURES for all services and programs.

DON'T:

✓ DO NOT CLICK ON A LINK unless you are 100% sure it is safe.

✓ DO NOT REPLY TO EMAILS unless you are 100% sure it is safe.

✓ DO NOT CLICK ON AN ATTACHMENT unless you are 100% sure it is safe.

✓ DO NOT GIVE OUT PERSONAL INFORMATION unless you are 100% sure it is safe.

✓ DO NOT STORE PERSONAL INFORMATION ONLINE.

Important procedures and details follow.
The guidelines are implemented somewhat differently depending on your hardware and software tools used.

E-MAIL

Settings: Discern and choose settings with awareness of the results of your choices.
- •Every email service has a set of option settings that deserve to be reviewed and selected.

Filters: Choose if you want to accept html formatted mail, attachments or links.
- •Strong filters may reject some wanted mail. Lower filters require a watchful eye.

Address files: Do all received and sent email belong in your email address file?
- •Unsolicited or advertising contacts may not deserve to be saved in your contact collection.

Copies: Is it necessary to save all copies of sent mail or on a selective basis?
- •Consider saving only essential and important communications.

Folders: Categorize retained messages.
- •Group folders can greatly assist finding and tracking sist necessary communications.

Reply: If you receive mail with additional copied persons, use care to select whether you intend to reply to one or to all.
- •Do you want everyone in the message to read your response?
- •Consider not including the original message or include only selected portions in your reply.

Groups: When sending or replying to multiple email addresses, consider placing the additional or even all email addresses in BCC rather than in visible addresses.
- •Blind Carbon Copy (BCC) does not expose all the email addresses to all recipients. It may not be necessary for all to see who else receives the same message.
- •Open lists of recipients may also be used for others to contact the same addresses.

Identity: Introduce and sign your emails. Fully explain insertions, attachments and links.
- •Your email address is not enough for the recipients to validate the sender.
- •If you receive unexplained or untrusted signed emails, do not click on links or attachments.

Junk: Tag suspicious emails as "junk" or "blocked."
- •Do not reply to extraordinary offers, awards, promises or invitations.
- •If you are offered a large inheritance from an unknown relative, it's a hoax. Delete it.

Protect: Set your Antivirus options to scan both incoming and outgoing mails.
- •Scan what you receive but also check that outgoing mail and addresses are secure.

Accounts: Consider different email addresses for different services.
- •Different emails could be used for personal, financial, software services, registrations, etc.

Clean up: Empty and clear out your mailbox and deleted folders regularly.
- •Mailboxes fill up and become unwieldy to organize. Copy important mail to holding folders.
- •Deleted or Trash folders also hold old mail files. So don't forget to throw out the trash.

SYSTEM PRACTICES

A good Google guide: **https://safety.google**

AntiVirus: Extended features of Antivirus and Internet security services.
- •Some free services are as effective as paid services, including: Avast, Avira, AVG, etc.
- •Settings will check viruses, internet, email, malware, scripting, file security and more.
- •Either let the software schedule regular updates of the virus lists or apply them yourself.

Preferences: For any software choose security and options appropriately.
- •To control, protect and secure a Google account, use **https://myaccount.google.com.**

Alerts: Do not ignore or override warnings.
- •Blocks or alerts from official software security should be taken seriously before ignoring.

Hoax: Be aware of internet "hoax" warnings with offers to clean your system.
- •Identify if the warning is from your own security software. Others are not official.
- •Microsoft or legitimate sites do not alert and offer to fix your system from the internet.
- •Even credible web sites may generate a false security warning that can infect your system.
- •Close or leave any hoax invitations.

Updates: Allow Microsoft or Apple to update their software and security.
- •Including other software and core services like Oracle (Java), Adobe (Flash) etc.

Backup: Make regular external copies of necessary computer files.
- •If you cannot keep a full system backup for full restoration, consider copies of essential files.
- •A general rule is to copy everything you would not want to loose in a system failure.

Cloud: Be selective of what you store on public servers (the "cloud").
- •Internet storage and backup services should not be considered as private material.

Clean up: Periodically clear/remove your browsing history and cookies.
- •These leave a long trail for clandestine advertising and unwanted contacts.

Passwords: Do not use the same password for everything.
- •Responding to an option to "remember me" on a site may not be totally private.
- •Catalogue your multiple passwords in a local secure software vault tool like KeePass.

Personal: Do not supply private information without security guarantees.
- •Validate the use of any personal information such as credit cards or bank transfers.

Wireless: (WiFi) Carefully choose between local home or public networks.
- •Local networks allow links between computers. Public networks isolate each computer.

Software: Installing new programs, select only features and services you want.
- •It has become customary to add services and add-on programs unless you decline.

Social Networks: Facebook and more are not private and postings are permanent.
- •Your comments may be gleaned or misused years later. Be discrete and discerning.

Turn off: Don't leave your computer unattended for long periods.
- •Completely shut down daily (not just sleep mode) to refresh software services.