Information Security Facts and Guidance for Volunteers

We all use on-line systems daily to interact with others, access information and complete our tasks. When we use these regularly it can be very easy to overlook the basic information security housekeeping that ensures we keep data and systems secure.

You are a target to hackers. Don't ever say "It won't happen to me". We are all at risk and the stakes are high - to your personal and financial well-being, and to the Institution's standing and reputation.
Keeping IET computing resources & information secure is everyone's responsibility.

By following the tips below and remaining vigilant, you are doing your part to protect yourself and others.

We have therefore put together some simple facts and suggested actions as a reminder to help you keep both yourself and the IET safe and protected.

- **Your username and password is used to identify YOU as YOU** when you login. Others who need access will be given their own login. **Don't share your login** details with anyone.

- **Always create strong passwords** using special characters, numbers, and upper and lower case letters which are difficult for someone to guess.

- **Always use Multi Factor** using a 2nd factor for authentication can prevent others accessing your accounts even if your password is known.

- **Never use a password which is the same as your username or easy to guess** – it makes it far easier for hackers to gain access into your account.

- **Don't reuse your passwords between accounts you have** - hackers love people that do this and they use compromised lists of usernames and passwords all the time - with great success.

- **Think about using a password manager if you don't already**. The browser ones are OK, but a dedicated password manager offers much more, and makes life much more secure, and much easier.

- **Avoid Phishing scams - beware of suspicious emails and phone calls** - Phishing scams are a constant threat - using various social engineering ploys, cyber criminals will attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information.

  Phishing scams can be carried out by phone, text, or through social networking sites - but most commonly by email. Be suspicious of any official-looking email message or phone call that asks for personal or financial information. Do not respond to emails or click links from unknown senders. Always verify the legitimacy of the person asking for information.

- **Be careful what you click** - Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your computer. If attachments or links in email are unexpected or suspicious for any reason, don't click on it.

- **Don't download or print documents** containing personal or commercially sensitive data unless you absolutely have to; and **destroy any downloads or printouts** (using a cross-cutting shredder) as soon as you have finished with them.

- **Protect sensitive information** - Be aware of sensitive information and associated restrictions. In general:
  Keep sensitive data (e.g., SSN's, credit card information, student records, health information, etc.) off of your workstation, laptop, or mobile devices. Securely remove sensitive data files from your system when they are no longer needed. Always use encryption when storing or transmitting sensitive data. Such information should not be stored or sent in plain text over email. Sensitive information should always be encrypted, and password protected.

- **Use mobile devices safely**

  Considering how much we rely on our mobile devices, and how susceptible they are to attack, you'll want to make sure you are protected:

  - Lock your device with a PIN or password - and never leave it unprotected in public.
  - Only install apps from trusted sources.
  - Keep your device's operating system updated.
  - Don't click on links or attachments from unsolicited emails or texts.
  - Avoid transmitting or storing personal information on the device.
  - Most handheld devices are capable of employing data encryption - consult your device's documentation for available options.
  - Use Apple's Find my iPhone or the Android Device Manager tools to help prevent loss or theft.
  - Backup your data.

- **Keep devices and software updated** – smart phones, computers and software all require regular patches in order to prevent newly discovered security vulnerabilities from being exploited. Ensure your devices are kept updated

- **Follow vendor security guidelines** – similarly smart phones, computers and software all have best practice guidelines for how to keep your information secure. Refer to your vendors security documentation for further information. E.g. Microsoft, Google, Apple, etc.

- **Never leave systems or documents unattended** where others can see them. Lock your screen (CTRL+ALT+DEL) and lock away documents containing data while others are around. This is particularly important in public areas.

- **Don't link external applications** - Avoid linking external applications to your IET accounts. Doing so can provide third-parties with access to your information and corporate information.

- **Always dispose of hardware responsibly** – destroy disk drives so they cannot be read by others, especially if you do download documents and store them, even if you have deleted them.

- **Use a Firewall** – Mac and Windows have basic desktop firewalls as part of their operating system that can help protect your computer from external attacks.

- **Be cautious when using public Wi-Fi** – Use a VPN (virtual private network) if possible. Ensure website addresses are legitimate and using “HTTPS” with a valid certificate.

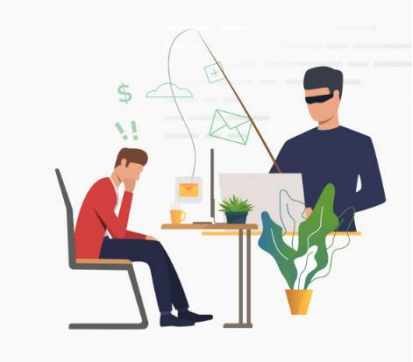
- **Be conscientious of what you plug in to your computer** - flash drives and even smart phones can contain malware.

- **Be careful of what information you share on social networking sites.**

- **Monitor your online accounts for suspicious activity.**

- **Bank or shop online only on trusted devices and networks** - and logout of these sites when you've completed your transactions.

And Remember



- **Email is not considered a secure communication method** for sending sensitive information. Always encrypt & passwords protect sensitive information.

- **Email messages you send** become the property of the recipient.

- **The information you place in an e-mail** can show up anywhere and anytime so think before you send any email message.

- **Check email trails** for personal, sensitive or incriminating data.

- **Do not auto forward or redirect** email to external addresses. Ensure any emails are reviewed manually and sensitive content removed before sending email to external recipients.