Safety on the Internet

The more we use our computer, the more information we store about ourselves on it. We type up our CV with our personal information, we use online banking with our bank account information, we buy online with our credit card. Every time we use the computer in this way, information about us is stored on it. It is important that this information is secure both physically and virtually.

What should you do?

1. **Install and Use Anti-Virus Programs**

Anti-virus software protects your computer from viruses by scanning your computer and your incoming email and deleting anything that is infected.

Viruses can destroy your data, slow your computer's performance, cause a crash, or allow spammers to send email through your account.

Examples of anti-virus software are Norton, McAfee, AVG (free software) or Symantec.

A **virus** is a malicious program written specifically to attack your computer. The most common way of receiving a virus is online.

Spyware is a form of malicious software that monitors your online activities and can potentially collect your personal information.

2. **Use Care When Reading Email with Attachments**

Email has become a critical way to communicate with friends and families and conduct business - it's quick, convenient, and effective.

Many email messages contain attachments, such as documents, photos, or links to Web sites that senders think might be of interest.

However, cyber criminals often use email to trick people into opening attachments and visiting Web sites that collect personal information (phishing) or download malicious software (spyware). They overload our email inboxes with messages we didn't ask for and don't want (spam).

To protect yourself against these types of emails follow these tips:

- Don’t open an email from someone you have never heard of. Delete it immediately. If you do open it by accident, don’t click on any links. Never reply to a SPAM email
- You can put a block on unwanted SPAM email on your email account – this will also block most fraudulent emails too
- Use an up-to-date web browser as these can warn you against sites that may try to gain your information fraudulently
- Don’t give away your password or any personal information. No legitimate company will ever ask you for your password

Spam

Left unchecked, any email account will quickly become overloaded with junk, some of which will contain viruses and scams. Most email programs contain options for filtering out what you don't want. Learn how to use those tools properly to make your email experience faster, safer and simpler.

Phishing

Phishing attacks use email or malicious Web sites to collect personal and financial information. Attackers may send urgent emails that request account information, seemingly from a reputable credit card company or financial institution. When users respond with the requested information, attackers can use it to gain access to the accounts.

3. **Use Care When Downloading and Installing Programs**

Sometimes when we are online and we click on a link another window opens and before we know it we are downloading a new program. Most times it is no big deal but every time we add a new program to our computer it has the potential to contain a virus or just slow the computer down at Startup because another program now has to start.

It is important to ensure only necessary programs are installed & only necessary updates to these programs are allowed to run. Always check what is requesting an update before allowing it to happen. Ensure children are restricted users on the computer to avoid unnecessary downloads of games etc. which could slow down your computer.

4. Security considerations that should be taken into account when using the internet:

- When accessing websites that require logging in, always keep information such as username and password secure and private, for example, for on-line banking
- Select No when asked by a website that requires logging in whether the user wishes the website to remember the user's password for the next time s/he logs in
- Don't ever share personal information with a third party over the internet, for example, when an email is received requesting personal information
- Give some consideration to the web sites being accessed and the content contained in them
- Only give credit/laser card details on secure, legitimate, well known websites
- Consider using Paypal as a means of transferring payment through the internet
- When using self generated passwords, ensure that the learner uses a combination of lowercase, upper-case, and punctuation characters to make up the password

5. Passwords

Privacy considerations to be taken into account when using the internet, for example:

Some guidelines for Passwords:

- Combine capital & lowercase letters and use numbers and symbols to make your password more secure e.g. B0no567 (using a capital B and a zero instead of an O makes it harder to guess).
- Try to use a minimum of 6 characters in your password.
- Avoid using family or pets names.
- Use separate passwords for every account or at least for important accounts like online banking.
- Don't make loads of private information public on the internet – exercise caution at all times
- Consider the websites where the learner is filling out forms or purchasing goods or services as the personal information given may be used to send spam or to advertise products or services
- Be cautious of photos or videos that the learner posts on websites such as youtube and that have the potential to be viewed by people all over the world
- Be aware of the privacy settings the learner has applied on social networking sites

Applicable usage policy considerations to be taken into account when using the internet, for example:

- If using the internet at work or in the centre/school, be aware of websites that should not be accessed, such as those considered pornographic, immoral or unethical
- When writing or forwarding emails, consider the content of the emails and who will be receiving them, in line with the work or school policy
- Ensure that any website or email content viewed or forwarded to others is not considered discriminatory on the grounds of race, gender, nationality, religion etc.