Unit 4: Society, Law and Ethics (SLE-1) - Cyber safety

Cyber safety

Cyber safety is trying to be safe on the internet and is the knowledge of maximizing the user's personal safety and security risks to private information and property associated with using the internet, and the self-protection from computer crime in general.

Safely browsing the web: Protecting yourself by securing your devices, software and connections is important, but making the right choices when doing things on the web can make a huge difference to your safety online. There are potential risks involved in doing things online, but by making smart choices you can reduce that risk.

By using a combination of preventative measures and making good choices online you can stay safe when browsing the web.

Before you start – Update your software: Exploiting email and web browsing applications is the most common way hackers and malware try to gain access to devices and your information. Protect yourself before you start browsing the web by making sure that your operating system, web browser, security software, browser plugins (like Java or Adobe products) and other applications are up-to-date.

Protect your web browser: You can adjust the settings in your web browser to work in a more or less secure way. Some functionality might be limited when using the most secure settings, but they can provide the best protection from malicious content. Most web browsers will give you warnings when they detect you visiting a malicious website or possibly being exposed to malicious content. Pay attention to these warnings – they can help protect you from malware, phishing and identity theft.

Use safe behaviour:

Use the following advice when browsing the web to significantly reduce your risk of being a victim of cybercrime:

- Use strong unique passwords online.
- Only download files and applications from websites that you trust, such as from official app stores or legitimate organisations, such as your bank.
- Pause and think carefully before clicking on links in email, messages or on social networking sites. Don't click on links in messages if you don't know the sender or if the message is unexpected.
- If you think a link looks suspicious or you can't tell where it leads to, before you click hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognize or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video, or webpage without directly clicking on the suspicious link.
- Expand shortened URLS to check if they are safe. Short URLs are often used in social media. There are a number of services that create short links - such as goo.gl, bit.ly, tinyurl.com, ow.ly and youtu.be. To check if these links are safe you can use an 'expand link' facility to get the original URL from a shortened link without having to click through to the destination. Look for a short URL expander that is recommended by your anti-virus software or a reputable software company.
- Be wary of offers that seem too good to be true. Leave websites that ask for your personal or banking details in return for money – these are scams.
- Don't agree to friend requests from people you don't know on social media networks - people are not always who they say they are.

Identity protection: Your personal identity is important as it defines who you are. Your identity includes your personal information; information such as name, address, contact information, bank account, credit card numbers, and social security numbers should all be kept private.

Confidentiality: Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Sometimes safeguarding data confidentiality may involve special training for those privy to such documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods, to prevent them from bending data-handling rules with good intentions and potentially disastrous results.
A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm. Other options include biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, precautions such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy form only.

Social networks: Social networking is playing a huge role in our life. Now a days businesses heavily rely on social media for their promotions and sale of their products. But on the other hand lot of frauds are being done using social media. Person shouldn't accept any random request. There are lot of fake accounts on social media which might be hackers they might intrude in your PC.

Cyber Trolling: Trolling is internet slang for a person who intentionally starts arguments or upsets others by posting inflammatory remarks. The sole purpose of trolling is angering people. It has been compared to flaming in cyber bullying. Plus, many people who troll think what they do is an "art". They frequently hide behind a cloak of anonymity. The symbol for trolling is a black and white drawing of a face with a mischievous grin, which is symbolic of the expression someone is making while trolling victims.

Purpose of trolling is To be a source of entertainment for the troller, To be offensive and argumentative, To derive pleasure from annoying the hell out of others, To scour the internet for bait (a.k.a. you), To get attention, To feel powerful, To gain recognition, To upset the victim

Cyber bullying: Cyber bullying is deliberate and repeated harm inflicted through using the Internet, interactive and digital technologies, or mobile phones.

Purpose

- To get revenge
- To feel empowered
- To gain popularity
- To harass and threaten
- To be offensive
- To humiliate
- To intimidate
- To upset the victim