Digital Skills

Deep drive into digital world…..

(Participant Guide)

Welcome Note

Dear Participant,

Welcome to the training program titled as “Digital Literacy”. With this training, participants can use digital technology to become more productive at work.

For example, digital documents can be created, stored and accessed more efficiently than printed versions, but only if employees know how to locate them, use them and share them confidently. If they struggle with this, it has a knock-on-effect on how employee time is used in the workplace – with consequences for business productivity.

Your role in the activities of this course is of great importance. Through activity-based training, you will understand digital industry in detail. When engaged in active, deep learning, you are not passively taking in information from instructors but are reading, writing, discussing and problem-solving.

You as participants are expected to follow the training course as directed by our efficient trainers and ensure to complete the assignments religiously.

Please remember, you are adults now and trying to step into the corporate sector; hence it is crucial for you to interact with your trainer and acquire the knowledge of accounting.

We hope that you will gain from this programme and will be able to inspire for you future self.

All the best!

Table of Content

General Instructions to Trainee

As a participant/ trainee, keep in mind the following guidelines

1. Greet your instructor and the other participants when you enter class
2. Always be punctual for every class
3. Be regular. Candidates who fall short of the required attendance will not be certified
4. Inform your instructor if, for any reason, you need to miss class
5. Pay careful attention to what your instructor is saying or showing
6. In case you do not understand something do not hesitate to put up your hand and seek clarification
7. Make sure you do all the exercises in your workbook. It will help you understand the concept better
8. Practice any new skills you have learnt as many times as possible. Seek the help of your Trainer or co-participant for practice
9. Take all necessary precautions, as instructed by your Trainer, when using machinery and tools
10. Make sure you are neatly attired and presentable at all times
11. Participate actively in all the activities, discussions and games during training. It will make you more confident and help in the learning process.

Digital Literacy
At the end of this module, you will be able to: ❖ Know the actual meaning of Digital Skills ❖ Understand CyberSecurity and different threats ❖ Learn different trending application in IoT ❖ Understand basics of AI, ML, Blockchain and Robotic Process Automation ❖ Learn about mobile and web development techniques

Module 1- Computer Fundamentals

Module Overview

This module will aim at introducing you to the concepts of computer. This also will cover about computer security which is used for saving data and information for different attacks.

Module Objective

At the end of the module, you will be able,

- To understand Computer network
- To understand the meaning of computer security and privacy
- To learn about different sets of threats to your data in the computer and how to save it

Computer Network

A computer network or data network is a telecommunications network which allows nodes to share resources. In computer networks, networked computing devices exchange data with each other using a data link.

Types of Computer Network

A network can be classified by its capacity or its purpose, mainly it is classified under following types:

1. PAN (Personal Area Network)
2. LAN (Local Area Network)
3. MAN (Metropolitan Area Network)
4. WAN (Wide Area Network)

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants.

Local Area Network

A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment.

Metropolitan Area Network

A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN)

Wide Area Network

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

Internet Area Network

An Internet area network (IAN) is a concept for a communications network that connects voice and data endpoints within a cloud environment over IP, replacing an existing local area network (LAN), wide area network (WAN) or the public switched telephone network

Cloud Networking

Cloud networking (and Cloud based networking) is a term describing the access of networking resources from a centralized third-party provider using Wide Area Networking (WAN) or Internet-based access technologies.

Computer Security

Computer Security is the protection of computing systems and the data that individual stores or access.

Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.

Why is Computer Security Important?

Computer Security allows individual to carry out its mission by:

- Enabling people to carry out their jobs, education , and research
- Supporting critical business process

Computer Privacy

In order to safeguard your information, it is important to fully understand the visibility of data on a computer.

Privacy is extremely important when multiple users access the same computer and when a computer is often used on the Internet. It is easy to protect your sensitive information in these cases of computer use.

Computer privacy has become a huge concern as we increasingly use portable computers and share public computers or Internet access points for personal and business purposes.

Natural Threats to Computer

Natural disasters, such as earthquakes, floods and hurricanes, can damage your computer. Fires, extreme temperatures and lightning strikes can cause major physical damage and lead to loss of data.

Protection against Natural Threats to Computer

- Create Backup of the data
- Install computer in proper location.
- Install an Uninterruptible Power Supply (UPS)

Threats from Human Action

This can be further divided as intentional threat and unintentional threat

Intentional Threats: Computer crimes are the best examples of intentional threats, or when someone purposely damages property or information. Computer crimes include espionage, identity theft, child pornography, and credit card crime.

Unintentional Threats: These threats basically include the unauthorized or accidental modification of software. Have you ever accidentally deleted an important file, or tripped over a power cord?

Protection against Human Threats

- Create Backup of the data
- Encrypt the data at the drive level
- Install Antivirus and anti-spyware programs
- Block junk e-mail messages
- Install Firewall

In this world of ubiquitous computers and persistent threats from hackers, protecting your computer is a must. The key pathway through which malware attacks the system is the Internet and its popular service, the Web.

There are numerous ways to protect and remove malware from our computers. No one method is enough to ensure your computer is secure. The more layers of defense, the harder for hackers to use your computer. Here are five simple, but critical steps to protect your computer,

- Install Firewall
- Install Antivirus Software
- Install Anti-Spyware Software
- Use Complex and Secure Passwords
- Check on the Security Settings of the Browser

1. Install Firewall

A **firewall** enacts the role of a security guard. There are of two types of firewalls: a software firewall and hardware firewall. Each serves similar, but different purposes. A firewall is the first step to provide security to the computer. It creates a barrier between the computer and any unauthorized program trying to come in through the Internet. If you are using a system at home, turn on the firewall permanently. It makes you aware if there are any unauthorized efforts to use your system.

2. Install Antivirus Software:

Antivirus is one other means to protect the computer. It is software that helps to protect the computer from any unauthorized code or software that creates a threat to the system. Unauthorized software includes viruses, keyloggers, trojans etc. This might slow down the processing speed of your computer, delete important files and access personal information. Even if your system is virus free, you must install an antivirus software to prevent the system from further attack of virus.

Antivirus software plays a major role in real time protection, its added advantage of detecting threats helps computer and the information in it to be safe. Some advanced antivirus programs provide automatic updates, this further helps to protect the PC from newly created viruses.

3. Install Anti-Spyware Software:

Spyware is a software program that collects personal information or information about an organization without their approval. This information is redirected to a third party website. Spyware are designed in such a way that they are not easy to be removed. Anti-Spyware software is solely dedicated to combat spyware. Similar to antivirus software, anti-spyware software offers real time protection. It scans all the incoming information and helps in blocking the threat once detected. Comodo Free Antivirus comes with spyware protection built in.

4. Use Complex and Secure Passwords:

The first line of defence in maintaining system security is to have strong and complex passwords. Complex passwords are difficult for the hackers to find. Use a password that is at least 8 characters in length and include a combination of numbers, letters that are both upper and lower case and a special character. Hackers use certain tools to break easy passwords in few minutes. One recent study showed that a 6 character password with all lower case letters can be broken in under 6 minutes!

5. Check on the Security Settings of the Browser:

Browsers have various security and privacy settings that you should review and set to the level you desire. Recent browsers give you ability to tell web sites to not track your movements, increasing your privacy and security.

Computer Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are almost identical to the legitimate one. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that are infected with malware.

Types of Computer Phishing

- Deceptive Phishing
- Spear Phishing
- CEO Fraud
- Pharming
- Dropbox Phishing
- Google Docs Phishing

Deceptive Phishing

The most common type of phishing scam, deceptive phishing refers to any attack by which fraudsters impersonate a legitimate company and attempt to steal people's personal information or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing the attackers' bidding.

For example, PayPal scammers might send out an attack email that instructs them to click on a link in order to rectify a discrepancy with their account. In actuality, the link leads to a fake PayPal login page that collects a user's login credentials and delivers them to the attackers.

Spear Phishing

Not all phishing scams lack personalization – some use it quite heavily.

For instance, in spear phishing scams, fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender.

The goal is the same as deceptive phishing: lure the victim into clicking on a malicious URL or email attachment, so that they will hand over their personal data.

CEO Fraud

Spear phishers can target anyone in an organization, even top executives. That's the logic behind a "whaling" attack, where fraudsters attempt to harpoon an executive and steal their login credentials.

In the event their attack proves successful, fraudsters can choose to conduct CEO fraud, the second phase of a business email compromise (BEC) scam where attackers impersonate an executive and abuse that individual's email to authorize fraudulent wire transfers to a financial institution of their choice.

Pharming

As users become more savvy to traditional phishing scams, some fraudsters are abandoning the idea of "baiting" their victims entirely. Instead, they are resorting to pharming – a method of attack which stems from domain name system (DNS) cache poisoning.

The Internet's naming system uses DNS servers to convert alphabetical website names, such as "www.microsoft.com," to numerical IP addresses used for locating computer services and devices.

Under a DNS cache poisoning attack, a pharmer targets a DNS server and changes the IP address

Malicious website of their choice even if the victims entered in the correct website name.

Google Docs Phishing

Fraudsters could choose to target Google Drive similar to the way they might prey upon Dropbox users.

Specifically, as Google Drive supports documents, spreadsheets, presentations, photos and even entire websites, phishers can abuse the service to create a web page that mimics the Google account log-in screen and harvests user credentials.

If you do not take measures to keep your computer safe, your computer -- and you -- could become the target of a cybercrime.

Cybercrimes are those instances when criminals, known as hackers or attackers, access your computer for malicious reasons. You can fall victim any time you are on an unprotected computer, receive a deceptive email claiming there is an “urgent matter” regarding your Monster account or just surfing the Web. They might be seeking sensitive, personal identification information stored on your computer, like credit card numbers or private account logins they use for financial gain or to access your online services for criminal purposes. Or they could want your computer’s resources, including your Internet connection, to increase their bandwidth for infecting other computers. This also allows them to hide their true location as they launch attacks.

Computer Ethics

Computer ethics is a part of practical philosophy which concerns with how computing professionals should make decisions regarding professional and social conduct.

- You shall not use a computer to harm other people.
- You shall not interfere with other people's computer work.
- You shall not snoop around in other people's computer files.
- You shall not use a computer to steal.
- You shall not use a computer to bear false witness.