Evaluate the state of performance and possible causes of failures

ICT Tools

Information and Communicating Technology (ICT) tools are computer-based equipment used for processing data and communication. Some ICT tools are;

- Television
- Public Address System
- Radio
- Mobile Phone
- Computer

Uses of ICT tools

ICT tools are very useful in many other ways. We watch television programs for entertainment, education and information.

The Public Address System is used for making community announcements by amplifying the voice of the user.

The radio presents programs, music and discussions that keep us informed and entertained.

The Mobile phone helps us to stay in touch with our friends, family and colleagues and finally the computer enables us to surf the Internet and communicate with other people online, it is also a form of entertainment because we can use it to watch movies and listen to music as well.

Computers can also be used in businesses for communicating, desktop publication, sound editing.

Although it is unlikely that using ICT equipment will be dangerous in itself, it can be used in ways which can be a hazard to our health.

Health and safety using ICT Tools

In this lesson you will learn about the possible long-term health hazards associated with the use of ICT equipment and ways to avoid these health problems.

It is important to note that although ICT makes our lives easier, long term exposure to ICT equipment without precaution may lead to possible health hazards in future. Here are some of the possible health hazards.

Safety precautions for the use of ICT Tools.

What are the negative effects of long term exposure to television?

Your eyes are not suited for staring into the television set for hours.

Staring into the television set for hours can be dangerous and harmful to the eye.

By staring continuously you cause the eye to overwork itself and this may lead to eye irritation, such as dry eye, red, itchy, and watery eyes, fatigue, including heaviness of the eyelids or forehead; and difficulty in focusing the eyes.

Negative effects of improperly using the Computer.

Eye irritation and Eye fatigue.

The negative effects of using a computer do not differ greatly from that of the television. Staring at the monitor for more than two hours a day can lead to eye irritation, such as watery eyes, heaviness of the eyelids or forehead, difficulty in focusing the eyes and fatigue of the eye structures etc. It is therefore important to keep a distance of 20 to 26 inches away from the monitor and arrange your lights sources in order to prevent reflections or glare on the monitor screen.

Lower Back Pain

Sitting behind the computer for long periods or using the wrong kind of chair can also lead to problems in the future. It can lead to pain in the lumbar region of the back.

Wrist Pain

People may also experience wrist pains usually because their hands are not positioned properly when typing. Pains in the back, wrists or fingers often occur when you are not able to reach the keyboard and mouse whilst bending your elbows at 90 degrees, with your shoulders relaxed.

Cold and Flu

People who work for many hours in air-conditioned rooms may suffer from cold and flu.

Mobile phones and our Health

It is believed that mobile phones can affect the health of people who use them.

Research from Finland suggests that mobile phone radiation causes changes in the brain and even low level emissions from headsets are still damaging.

However, there has not been any major research that provides scientific evidence of the danger of using mobile phones.

It is therefore too soon to reach a definitive verdict on health risk from mobile phones. Nevertheless there are some effects that you can have when you do not use the mobile phone properly.

Some of the long-term health effects of using mobile phones are:

1. Headaches and tiredness.

Using the mobile phone for hours can be very stressful and may lead to mild or severe headaches.

2. Creates joint pain.

Holding the mobile phone to your ear for more than 15 minutes can lead to a strain of your wrist and ligaments in the back of the hand.

3. Mobile phone battery explosion.

It is not advisable to use your mobile phone whilst charging it. Sometimes mobile phone batteries over heat and explode in such cases. You can be seriously injured if this happens to you.

4. Induced ringing In the ears.

You can overwork your ear-drum when you hold the mobile phone very close to your ear. Keeping the mobile phone close to your ear for long periods of time may weaken your eardrums, induce ringing in your ears and eventually damage your hearing abilities in future.

5. Increased Cancer Risk

Some studies have examined the potential link between mobile phone use and the development of certain types of cancer, particularly brain tumors. However, the overall scientific consensus remains inconclusive, with some studies suggesting a possible association and others finding no significant evidence of increased risk.

6. Effects on Brain Function

Research has explored the impact of mobile phone radiation on cognitive function, sleep quality, and brain activity. While some studies have reported changes in brain activity, memory, and attention, the clinical significance and long-term consequences of these findings are still under investigation.

7. Electromagnetic Hypersensitivity (EHS)

Some individuals claim to experience symptoms such as headaches, fatigue, and dizziness when exposed to electromagnetic fields, including those emitted by mobile phones. However, scientific studies have generally failed to demonstrate a consistent causal relationship between mobile phone use and EHS.

8. Impact on Mental Health

The use of mobile phones, particularly excessive screen time and social media engagement, has been associated with mental health issues such as increased stress, anxiety, depression, and sleep disturbances. However, it is challenging to determine whether these effects are directly caused by mobile phone use or related to other factors.

Health effects of improper use of ICT tools

Improper use of ICT (Information and Communication Technology) tools can have negative health effects. While ICT tools are designed to enhance productivity and communication, misuse or excessive use can lead to various health concerns. Here are some negative health effects associated with improper use of ICT tools:

Physical Health Issues:

Musculoskeletal Problems: Prolonged or improper use of computer keyboards, mice, or mobile devices can lead to repetitive strain injuries (RSI) such as carpal tunnel syndrome, tendonitis, or neck and back pain.

Vision Problems: Staring at computer screens, smartphones, or tablets for extended periods can cause eyestrain, dry eyes, blurred vision, and headaches. This is commonly known as computer vision syndrome or digital eye strain.

Sedentary Lifestyle: Spending excessive time using ICT tools may contribute to a sedentary lifestyle, leading to weight gain, obesity, cardiovascular issues, and metabolic disorders.

Mental and Emotional Health Concerns:

Technology Addiction: Excessive use of ICT tools, including social media, online gaming, or streaming platforms, can contribute to addictive behaviors, leading to decreased social interaction, neglect of responsibilities, and withdrawal symptoms.

Anxiety and Stress: Continuous connectivity and information overload can contribute to feelings of overwhelm, anxiety, and stress, especially when individuals are unable to disconnect or find a healthy work-life balance.

Sleep Disruptions: The use of ICT tools before bedtime, exposure to blue light emitted by screens, and constant digital stimulation can interfere with sleep patterns, leading to insomnia or poor sleep quality.

Social and Relationship Challenges:

Social Isolation: Overreliance on ICT tools for communication and social interactions can lead to reduced face-to-face interactions, social withdrawal, and a sense of isolation.

Communication Issues: Misinterpretation of tone or intent in digital communications, such as emails or text messages, can lead to misunderstandings, conflict, and deteriorating relationships.

Online Harassment and Cyberbullying: Improper use of ICT tools can expose individuals to online harassment, cyberbullying, or privacy infringements, causing emotional distress and negative psychological impacts.

Cognitive and Productivity Impacts:

Reduced Attention and Productivity: Multitasking, constant interruptions, and excessive use of ICT tools can hinder concentration, cognitive performance, and productivity levels.

Information Overload: The overwhelming amount of information available through ICT tools can lead to cognitive overload, difficulty in information processing, and decision-making challenges.

To mitigate these negative health effects, it is important to adopt healthy ICT habits and practices:

- Take regular breaks, practice good ergonomics, and maintain proper posture when using ICT tools.
- Set boundaries and allocate dedicated time for digital detox, relaxation, and physical activity.
- Establish healthy work-life balance and prioritize face-to-face interactions.
- Implement strategies to manage technology use, such as setting time limits, using productivity tools, and promoting digital well-being.
- Stay informed about online safety, privacy settings, and cybersecurity best practices.

Possible causes of ICT infrastructure failure

Failure in ICT infrastructure can occur due to various factors, including environmental factors, user factors, hardware, and software.

Here are some possible causes of failure in ICT infrastructure:

Hardware Failure: Malfunctioning or damaged hardware components such as servers, switches, routers, storage devices, or power supply units can lead to system failures and downtime.

Software Issues: Incompatibility, bugs, glitches, or errors in software applications, operating systems, or firmware can cause system instability, crashes, or data corruption.

Network Connectivity Problems: Issues with network components, including routers, switches, cables, or wireless access points, can result in network outages, slow connectivity, or intermittent connectivity.

Power Outages or Fluctuations: Power failures, voltage fluctuations, or inadequate power backup solutions can disrupt ICT infrastructure, causing system shutdowns, data loss, or hardware damage.

Security Breaches: Cybersecurity threats such as hacking attempts, malware infections, ransomware attacks, or data breaches can compromise ICT infrastructure, leading to data loss, system disruptions, or unauthorized access.

Human Error: Mistakes made by system administrators, IT personnel, or end-users, such as misconfigurations, accidental deletions, or improper handling of equipment, can cause failures or service disruptions.

Natural Disasters: Events like earthquakes, floods, fires, or severe weather conditions can damage physical infrastructure, disrupt power supply, or lead to data loss, impacting ICT systems and services.

Lack of Redundancy: Insufficient redundancy in critical components, such as power supplies, network links, or data storage, can result in single points of failure, making the infrastructure vulnerable to disruptions.

Insufficient Capacity or Scalability: Inadequate infrastructure capacity, including storage, processing power, or network bandwidth, can lead to performance issues, slow response times, or system overloads during peak usage periods.

Lack of Maintenance and Updates: Neglecting regular maintenance, updates, patches, or firmware upgrades can leave systems vulnerable to security threats, software bugs, or compatibility issues, increasing the risk of failure.

Poor Disaster Recovery and Backup Plans: Inadequate disaster recovery strategies, including insufficient backups, outdated recovery procedures, or lack of testing, can result in prolonged downtime and data loss in case of failures or disasters.

To mitigate the risks associated with these potential causes of failure, organizations should implement robust monitoring systems, perform regular maintenance, establish backup and disaster recovery plans, ensure system redundancies, and prioritize cybersecurity measures. Regular training and awareness programs can also help reduce the impact of human errors on ICT infrastructure.

DIAGNOSE AND FIX PROBLEMS

What is the diagnosis?

The term "diagnosis" refers to the process of identifying and determining the root cause of problems or issues within the IT environment. It involves a systematic examination of symptoms, observations, and data to reach an accurate understanding of the underlying problem.

Definition of terms;

Troubleshooting

The process of identifying, analyzing, and resolving problems or issues within an ICT infrastructure. Troubleshooting involves diagnosing the root cause of the problem and implementing appropriate solutions.

Log files

Text files generated by various software applications, operating systems, and network devices that record events, errors, and activities. Log files are often used for diagnostic purposes to analyze system behavior, identify errors, and track issues.

Ping

A network diagnostic utility used to test the reachability of a device or host on an IP network. The ping command sends a small packet to the target device and measures the response time and success rate. It helps assess network connectivity and identify potential issues.

Network monitoring

The process of continuously observing and analyzing network traffic, devices, and systems to identify performance issues, anomalies, or failures. Network monitoring tools collect data, generate alerts, and provide insights into the health and performance of the ICT infrastructure.

Performance metrics

Quantitative measurements used to assess the performance and efficiency of ICT infrastructure components. Performance metrics may include factors such as response time, throughput, CPU and memory utilization, network latency, and disk I/O.

Bandwidth

The maximum data transfer rate or capacity of a network connection. It measures the amount of data that can be transmitted over the network within a specific time frame. Monitoring and analyzing bandwidth utilization help identify bottlenecks and optimize network performance.

Packet loss

The percentage of data packets that are lost or do not reach their destination during network transmission. High packet loss can indicate network congestion, hardware issues, or configuration problems.

Latency

The time delay experienced in data transmission over a network. It represents the time taken for a data packet to travel from the source to the destination. High latency can affect application performance and user experience.

Trace route

A diagnostic tool that traces the path taken by network packets from a source to a destination. It provides information about the intermediate network devices (routers) and the time taken for each hop. Trace route helps identify network connectivity issues and latency problems.

System logs

Logs generated by servers, operating systems, and applications that record events, errors, and system activities. System logs are useful for diagnosing issues, identifying software or hardware failures, and troubleshooting problems within the ICT infrastructure.

Common Diagnostic and Repair Tools used In ICT Infrastructure and Their Functions

Diagnostic and repair tools are software applications or physical devices used to identify, diagnose, and resolve issues or problems in various systems, including computer hardware, software, networks, and other ICT infrastructure components.

These tools provide valuable insights, analysis, and solutions to help troubleshoot and rectify technical problems efficiently.

Categories of diagnostic and repair tools:

1. **System diagnostic tools**

These tools assess the health, performance, and stability of computer systems. They can analyze hardware components, system resources, and software configurations to identify issues such as hardware failures, driver conflicts, system crashes, or performance bottlenecks.

Examples include *CPU-Z, HWiNFO,* and *PC-Doctor.*

2. **Hard drive diagnostic tools**

These tools focus on testing and diagnosing the health and functionality of hard disk drives (HDDs) and solid-state drives (SSDs). They can detect bad sectors, assess disk performance, monitor SMART attributes, and provide insights into potential disk failures.

Popular tools include *CrystalDiskInfo, HD Tune,* and *Western Digital Data Lifeguard Diagnostics*.

3. **Memory diagnostic tools**

Memory-related issues can cause system crashes, freezes, or application errors. Memory diagnostic tools perform comprehensive tests on computer memory (RAM) to detect and diagnose memory errors or failures.

Windows includes its own built-in tool called *Windows Memory Diagnostic*, and *Memtest86+* is a popular standalone memory testing tool.

4. **Network diagnostic tools**

These tools help diagnose network connectivity, performance, and configuration issues. They can test network connectivity between devices, analyze network traffic, measure latency and packet loss, and identify network misconfigurations.

Examples include *ping, tracert, Wireshark*, and *iperf*.

5. Antivirus and anti-malware tools

These tools scan systems for viruses, malware, and other malicious software. They can detect and remove threats, quarantine infected files, and provide real-time protection against security threats.

Popular antivirus tools include *Avast, Norton*, and *Malwarebytes*.

6. Data recovery tools

When data loss occurs due to accidental deletion, formatting, or hardware failure, data recovery tools can help retrieve lost or deleted files. These tools scan storage devices, identify recoverable files, and assist in their restoration.

Notable data recovery tools include *Recuva, TestDisk*, and *EaseUS Data Recovery Wizard*.

7. Operating system repair tools

These tools are designed to fix common issues within operating systems. They can repair system files, restore corrupted configurations, recover boot-related problems, and address software conflicts.

For example, Windows provides built-in tools like *System File Checker (SFC)* and *Deployment Image Servicing and Management (DISM)* for repair and recovery tasks.

8. Remote access and remote administration tools

These tools enable remote control and management of systems, allowing IT professionals to troubleshoot and fix problems from a remote location.

Examples include *Remote Desktop Protocol (RDP), TeamViewer,* and *VNC* (Virtual Network Computing).