IT topic

**Topic 1-2:**

**Security threats, solutions and procedures, as well as workstation health and safety.**

**Task 1: Read the text, find out all the threats for computer, write out them.**

**Security solutions**

Here the focus is on **security threats to IT systems** and what can be done to deal with these threats.

 **Adware** refers to programs that automatically download and/or display advertisements on the computer.

**Spyware** is software that can send information about the use of a computer system. **Malware**, from the words *malicious* and *software*, is a general term that refers to programs designed to gain access to a computer without the user’s authorisation or knowledge. One example is **worms**, programs that spread to other computers without the user taking action.

 Another example is **Trojans**, which are programs that pretend to be useful, encouraging a user to download and/or use them but that in fact damage the system. **Viruses** copy themselves into other programs and cause system problems.

A **browser hijacker** is software that replaces the user’s search engine with its own. Another security threat mentioned is **piggybacking**, which is using someone else’s wireless internet connection without their permission in order to access the internet.

Solutions mentioned include **biometric scanning** (for example, using thumb prints to identify people)and **antivirus software**, which is designed to protect computers from cyber attack.

In addition, there is a communicative focus on expressing probability (for example, *You* ***might*** *have* *a virus on your computer.*).

**Workstation health and safety**

This section deals with how you should sit at your computer as well as giving instructions on health and safety.

You need to know these words: *eye*, *forearm*, *hand*, *foot*, *back*, *shoulder*, *thigh*.

 **Tasks 2:**

1. *Explains the risk factors involved when using a workstation on a daily basis such as those posed to posture and eyesight.*
2. *Offers advice on the best practice for setting up screen and seating to minimise potential health problems.*
3. *Cover when to take breaks and recommends exercises to carry out to relieve stiffness.*

***Workstations and assessment***

If workers use display screen equipment (DSE) daily, as part of their normal work, continuously for an hour or more, employers must do a workstation assessment.

***Employers should look at:***

* the whole workstation, including equipment, furniture, and work conditions

the job being done any special requirements of a member of staff, for example a user with a disability

Where there are risks, they should take steps to reduce them.

Employers must also do an assessment when:

* a new workstation is set up
* a new user starts work
* a change is made to an existing workstation or the way it’s used
* users complain of pain or discomfort

Use this DSE workstation checklist to help make an assessment.

DSE assessment software

Software packages can help train users and help them take part in assessments. But the software is not an assessment on its own.

You should always make sure a trained assessor looks at user assessment results (whether these are software or paper based). The assessor should clear up any doubtful points, provide feedback to users and make sure problems are put right, for example by changes to the DSE or workstation.

Display screen equipment (DSE)

DSE work does not cause permanent damage to eyes. But long spells of DSE work can lead to:

* tired eyes
* discomfort
* temporary short-sightedness
* headaches

DSE work is visually demanding, so it can make someone aware of eyesight problems they have not noticed before (including changes in eyesight that happen with age)

**Reflected** **glare** is the light emitted from the computer screen.

There is also a focus on computer dos and don’ts (for example, connecting peripherals before turning your computer on or off).

**Scandisk** is a utility that checks and repairs file systems.

**Power surges** are when there is an unexpected increase in power (for example, as a result of electric storms).

 **Unauthorised software** is software the organisation has not given permission to use.

**Security procedures**

This section focuses on the kind of rules and recommendations that employees are likely to be asked to follow in a large organisation to meet security requirements.

**Data transfer** means the moving of information (for example, from an officecomputer to a home one).

**Security incidents** are events that threaten security.

A **security breach** is when someone accesses a computer system illegally or without permission.

**Task 3. Further reading**

Use the following keywords to search the internet for websites which give more in-depth information about the topics covered in this unit: ***hacker, viruses, worms, computer health and safety.***