

01. The two main parts are: ප්‍රධාන කොටස් දෙක වන්නේ:

- Hardware security / දෘඩාංග ආරක්ෂාව
- Software security / මෘදුකාංග ආරක්ෂාව

02. Computer hardware refers to the physical components of a computer that can be touched and seen. Examples: Monitor, keyboard, mouse, CPU, RAM, hard disk, cooling fan, DVD drive, motherboard, and power supply./ පරිගණක දෘඩාංග යනු ස්පර්ශ කළ හැකි සහ දැකිය හැකි පරිගණකයේ භෞතික කොටස් වේ. උදාහරණ: මොනිටරය, යතුරුපුවරුව, මවුසය, CPU, RAM, දෘඩ තැටිය, සිසිලන විදුලි පංකාව, DVD ධාවකය, මවු පුවරුව සහ බල සැපයුම් ඒකකය.

03. Major causes include: ප්‍රධාන හේතු අතරට පහත දෑ ඇතුළත් වේ:

- Sudden power failure / හදිසි විදුලි බිඳ වැටීමක් සිදුවීම
- Sudden flow of high voltage current / හදිසියේ අධි වෝල්ටීයතා ධාරාවක් ගලා ඒම
- Overheating inside the system unit / පද්ධති ඒකකය තුළ අධික ලෙස උෂ්ණත්වය ඉහළ යාම
- Dust gathering on computer hardware / පරිගණක දෘඩාංග මත දූවිලි තැන්පත් වීම
- Issues related to theft / සොරකම් කිරීම් හා සම්බන්ධ ගැටළු

04. A UPS (Uninterruptible Power Supply) provides continuous power to the computer during a sudden power failure. It gives sufficient time to save current work and shut down the computer safely./ UPS මගින් හදිසි විදුලි බිඳ වැටීමකදී පරිගණකය වෙත අඛණ්ඩව විදුලිය සපයයි. එමගින් දැනට සිදුකරමින් පවතින කාර්යයන් සුරැකීමට සහ පරිගණකය ආරක්ෂිතව ක්‍රියා විරහිත කිරීමට ප්‍රමාණවත් කාලයක් ලබා දේ.

05. Answer:

- Fuse: Prevents damage caused by a sudden flow of high voltage current./ රිසුස් : හදිසි අධි වෝල්ටීයතා ධාරා ගැලීම් නිසා සිදුවන හානි වළක්වයි.
- Surge protector: Protects the computer from high voltage current and lightning by controlling the flow of excess voltage./ සර්ජ් ප්‍රොටෙක්ටර් : අතිරික්ත වෝල්ටීයතා ප්‍රවාහය පාලනය කිරීම මගින් අධි වෝල්ටීයතා ධාරා සහ අකුණු මගින් සිදුවන හානිවලින් පරිගණකය ආරක්ෂා කරයි.

06. Overheating can be reduced by: අධික උෂ්ණත්වය ඉහළ යාම පහත ක්‍රම මගින් අවම කර ගත හැක:

- Installing air conditioners in the computer laboratory./ පරිගණක විද්‍යාගාරය තුළ වායු සමීකරණ සවිකිරීම.
- Installing cooling fans in the computer to remove excess heat./ අතිරික්ත තාපය ඉවත් කිරීම සඳහා පරිගණකය තුළ සිසිලන විදුලි පංකා සවිකිරීම.

07. The laboratory should be kept clean and tidy. Other precautions include: විද්‍යාගාරය පිරිසිදුව සහ පිළිවෙලට තබා ගත යුතුය. වෙනත් ආරක්ෂක පියවරයන් අතරට පහත දෑ ඇතුළත් වේ:

- Not entering with footwear that brings sand and dust./ වැලි සහ දූවිලි රැගෙන එන පාවහන් පැළඳ ඇතුළු නොවීම.
- Cleaning computer circuits regularly./ පරිගණක පරිපථ නිතිපතා පිරිසිදු කිරීම.
- Not taking food into the laboratory./ විද්‍යාගාරය තුළට ආහාර රැගෙන නොයෑම.
- Preventing insects and rats from entering./ කෘමීන් සහ මීයන් ඇතුළු වීම වැළැක්වීම.
- Controlling moisture because it can cause short circuits./ තෙතමනය පාලනය කිරීම (මන්ද එය කෙටි පරිපථ/short circuits ඇති කිරීමට හේතු විය හැක).
- Using air conditioners when necessary./ අවශ්‍ය විටෙක වායු සමීකරණ භාවිත කිරීම.

#ICT කණ්ඩායම

08. Computers can be protected from theft by: සොරකම් කිරීම්වලින් පරිගණක ආරක්ෂා කර ගත හැකි ක්‍රම:

- Locking doors and windows of the computer laboratory./ පරිගණක විද්‍යාගාරයේ දොරවල් සහ ජනෙල් අගුළු දැමීම.
- Locking the system unit securely./ පද්ධති ඒකකය ආරක්ෂිතව අගුළු දැමීම.
- Using CCTV cameras to monitor the laboratory./ විද්‍යාගාරය නිරීක්ෂණය කිරීම සඳහා CCTV කැමරා භාවිත කිරීම.

09. Computer software includes data, information, and programs used to perform various tasks./ පරිගණක මෘදුකාංගවලට විවිධ කාර්යයන් ඉටු කිරීම සඳහා භාවිත කරන දත්ත, තොරතුරු සහ වැඩසටහන් ඇතුළත් වේ.

Examples:

- Operating system / මෙහෙයුම් පද්ධතිය
- Word processing software / වචන සැකසුම් මෘදුකාංග
- Files containing documents / ලේඛන අඩංගු ගොනු
- Files containing pictures/images / පින්තූර

10. Threats to software include: මෘදුකාංග සඳහා වන තර්ජනවලට පහත දෑ ඇතුළත් වේ:

- Unauthorized access / අනවසර ප්‍රවේශය
- Malware / හානිකර මෘදුකාංග
- Unexpected deletion or overwriting of files / අනපේක්ෂිත ලෙස ගොනු මකා දැමීම හෝ ඒවා වෙනුවට වෙනත් දත්ත ලිවීම
- Natural disasters and terrorist attacks / ස්වාභාවික විපත් සහ ත්‍රස්තවාදී ප්‍රහාර
- Sudden power failure / හදිසි විදුලි බිඳ වැටීම්
- Complications in the operating system / මෙහෙයුම් පද්ධතියේ ඇතිවන ගැටළු

They can be prevented by: මේවා පහත ක්‍රම මගින් වළක්වා ගත හැකිය:

- Using passwords and other logical security methods./ මුරපද සහ වෙනත් තාර්කික ආරක්ෂක ක්‍රම භාවිත කිරීම.
- Using locks and door bolts for physical security./ භෞතික ආරක්ෂාව සඳහා අගුළු සහ දොර අගුළු භාවිත කිරීම.
- Installing antivirus software./ Antivirus මෘදුකාංග ස්ථාපනය කිරීම.
- Keeping backups of important data and files. / වැදගත් දත්ත සහ ගොනු වල පිටපත් තබා ගැනීම.

11. Malware (malicious software) is any malicious program or part of a program that does not fulfill the intended requirements of a computer user and is designed to cause damage to computer software, data, networks, or hardware./ හානිකර මෘදුකාංග යනු පරිගණක පරිශීලකයෙකුගේ අපේක්ෂිත අවශ්‍යතා ඉටු නොකරන, සහ පරිගණක මෘදුකාංග, දත්ත, ජාල හෝ දෘඩාංගවලට හානි කිරීමට සැලසුම් කර ඇති ඕනෑම හානිකර වැඩසටහනක් හෝ වැඩසටහන් කොටසකි.

12. The four types are:

- Computer virus / පරිගණක වෛරසය
- Computer worms / පරිගණක පණුවන්
- Trojan horse / ට්‍රොජන් අශ්වයා
- Spyware / ඔත්තු බලන මෘදුකාංග

#ICT නිශ්ශබ්ද

13. A computer virus is malicious software that gains access to a computer's software or files and can replicate itself and spread from one computer to another. It can delete or modify data and can cause harm to computer software./ පරිගණක වෛරසයක් යනු පරිගණකයක මෘදුකාංග හෝ ගොනු වෙත ප්‍රවේශය ලබා ගන්නා, තමන්වම පිටපත් කර ගැනීමට සහ එක් පරිගණකයකින් තවත් පරිගණකයකට පැතිරීමට හැකියාව ඇති හානිකර මෘදුකාංගයකි. එයට දත්ත මකා දැමීමට හෝ වෙනස් කිරීමට මෙන්ම පරිගණක මෘදුකාංගවලට හානි කිරීමටද හැකියාව ඇත.

14. A computer worm is malware that behaves similarly to a virus but can spread across computer networks or the Internet without the support of a host program./ පරිගණක පණුවෙකු යනු වෛරසයකට සමාන ලෙස ක්‍රියා කරන නමුත්, ධාරක වැඩසටහනක සහාය නොමැතිව පරිගණක ජාල හෝ අන්තර්ජාලය හරහා පැතිර යා හැකි ඒකඅරු වර්ගයකි.

15. A Trojan horse appears to be useful software at first, but secretly causes damage to the user once it begins to operate./ Trojan horse එකක් මුලින් ප්‍රයෝජනවත් මෘදුකාංගයක් ලෙස පෙනුනද, එය ක්‍රියාත්මක වීමට පටන් ගත් පසු රහසිගතව පරිශීලකයාට හානි සිදු කරයි.

16. Spyware is malicious software that secretly collects information about a person's computer usage, Internet use, etc., and sends the information to another party without the user's knowledge./ Spyware යනු පුද්ගලයෙකුගේ පරිගණක භාවිතය, අන්තර්ජාල භාවිතය ආදිය පිළිබඳ තොරතුරු රහසිගතව රැස් කර, පරිශීලකයා නොදැනුවත්වම එම තොරතුරු වෙනත් පාර්ශ්වයකට යවන හානිකර මෘදුකාංගයකි.

17. Malware can cause: Malware මගින් පහත දෑ සිදුවිය හැකිය:

- Deletion, hiding, or modification of data and information./ දත්ත සහ තොරතුරු මකා දැමීම, සැඟවීම හෝ වෙනස් කිරීම.
- Creation of unwanted files and folders./ අනවශ්‍ය ගොනු සහ ෆෝල්ඩර නිර්මාණය වීම.
- Malfunction or alteration of software./ මෘදුකාංග අක්‍රිය වීම හෝ වෙනස් වීම.
- Decreased computer efficiency./ පරිගණකයේ කාර්යක්ෂමතාව අඩු වීම.
- Repeated shutdown or restarting of the computer./ පරිගණකය නැවත නැවතත් ක්‍රියා විරහිත වීම හෝ නැවත ආරම්භ වීම.
- Unusual network behaviour or disconnection./ අසාමාන්‍ය ජාල ක්‍රියාකාරීත්වය හෝ ජාල සම්බන්ධතාව බිඳ වැටීම.
- Reduced storage capacity./ ගබඩා ධාරිතාව අඩු වීම.

18. Answer:

- Install antivirus software and update it regularly./ ප්‍රති-වයිරස මෘදුකාංග ස්ථාපනය කර එය නිතිපතා යාවත්කාලීන කරන්න.
- Scan external storage devices before opening them./ බාහිර ගබඩා උපාංග විවෘත කිරීමට පෙර ඒවා පරිලෝකනය කරන්න.
- Activate and correctly configure the firewall./ ගයර්වෝලය සක්‍රිය කර නිවැරදිව වින්‍යාස කරන්න.
- Access only secure websites./ ආරක්ෂිත වෙබ් අඩවි වලට පමණක් ප්‍රවේශ වන්න.
- Do not click suspicious pop-ups./ සැක සහිත උත්පතන ක්ලික් නොකරන්න.
- Do not open suspicious emails or attachments./ සැක සහිත ඊමේල් හෝ ඇමුණුම් විවෘත නොකරන්න.

#ICT කණ්ඩායම

- Use a Limited User Account for daily activities./ දෛනික ක්‍රියාකාරකම් සඳහා සීමිත පරිශීලක ගිණුමක් භාවිතා කරන්න.
- Keep installed software and the operating system updated./ ස්ථාපිත මෘදුකාංග සහ මෙහෙයුම් පද්ධතිය යාවත්කාලීනව තබා ගන්න.
- Use only original, licensed software./ මුල්, බලපත්‍රලාභී මෘදුකාංග පමණක් භාවිතා කරන්න.

19. Keeping backups means maintaining copies of software components or data. Backups can be used when the original copy is lost, damaged, or misplaced.

Examples of storage media include CDs, DVDs, external hard disks, and another location/drive on the same computer./ උපස්ථ තබා ගැනීම යනු මෘදුකාංග සංරචක හෝ දත්තවල පිටපත් පවත්වා ගැනීමයි. මුල් පිටපත නැති වූ විට, හානි වූ විට හෝ අස්ථානගත වූ විට උපස්ථ භාවිතා කළ හැකිය. ගබඩා මාධ්‍ය සඳහා උදාහරණ ලෙස CD, DVD, බාහිර දෘඪ තැටි සහ එකම පරිගණකයේ වෙනත් ස්ථානයක්/ධාවකයක් ඇතුළත් වේ.

20. Access control refers to methods used to control access to computers and protect their resources, data, and information./ ප්‍රවේශ පාලනය යනු පරිගණක වෙත ප්‍රවේශය පාලනය කිරීමට සහ ඒවායේ සම්පත්, දත්ත සහ තොරතුරු ආරක්ෂා කිරීමට භාවිතා කරන ක්‍රම වේ.

Methods include: ක්‍රමවලට ඇතුළත් වන්නේ:

- Using strong passwords./ ශක්තිමත් මුරපද භාවිතා කිරීම.
- Creating suitable user accounts./ සුදුසු පරිශීලක ගිණුම් නිර්මාණය කිරීම.
- Using encryption./ සංකේතනය භාවිතා කිරීම.
- Keeping computers in secure places./ පරිගණක ආරක්ෂිත ස්ථානවල තබා ගැනීම.
- Using CCTV cameras and alarms./ CCTV කැමරා සහ අනතුරු ඇඟවීම් භාවිතා කිරීම.
- Using biometric authentication such as fingerprints, voice recognition, face recognition, or iris recognition./ ඇඟිලි සලකුණු, හඬ හඳුනාගැනීම, මුහුණු හඳුනාගැනීම හෝ අයිරිස් හඳුනාගැනීම වැනි ජෛවමිතික සත්‍යාපනය භාවිතා කිරීම.