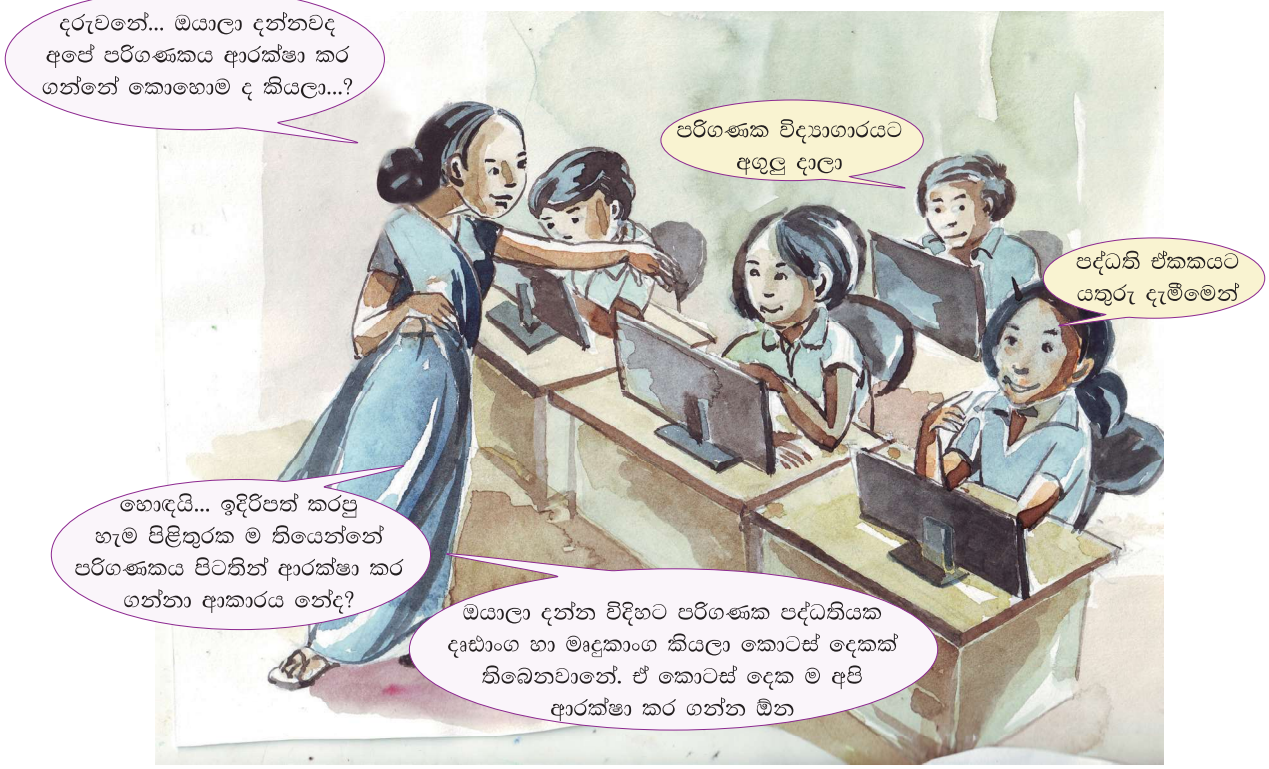
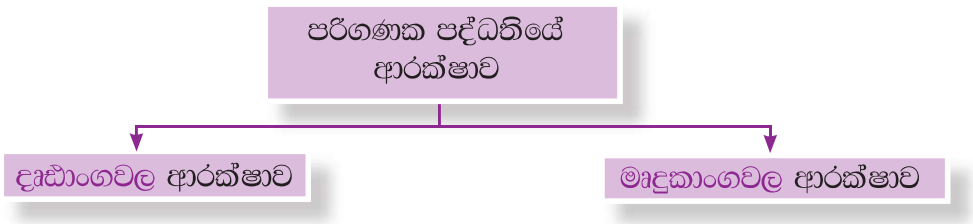
03 පරිගණක පද්ධතියේ ආරක්ෂාව



3.1 පරිගණක පද්ධතිය ආරක්ෂා කර ගනිමු

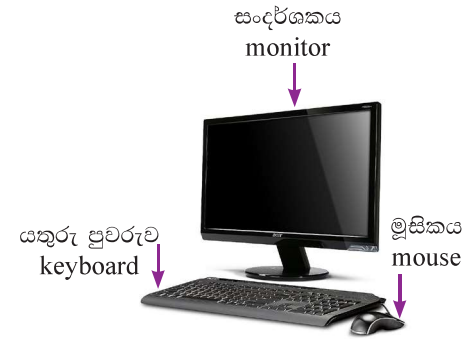
පරිගණකයේ පැවැත්ම හා ආරක්ෂාව සඳහා විවිධ පූර්ව ආරක්ෂක උපක්‍රම යොදා ගෙන තිබීම ඉතා වැදගත් ය. පරිගණක පද්ධතියේ ආරක්ෂාව කොටස් දෙකකට වෙන් කළ හැකි ය.



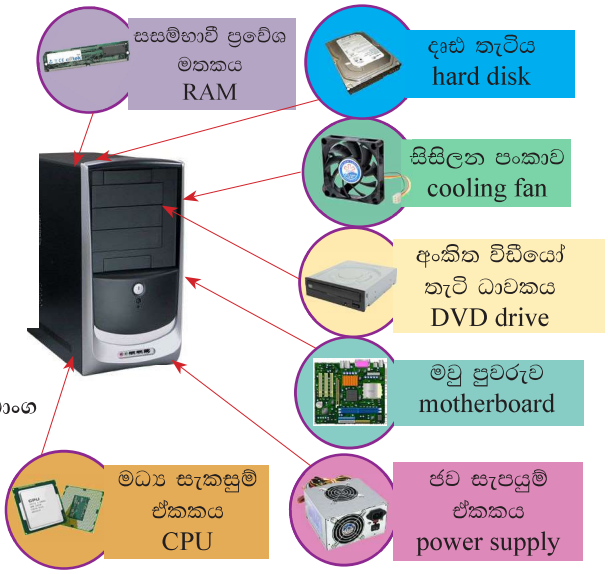
3.2 පරිගණකයක දෘඪාංග ආරක්ෂා කර ගනිමු

පරිගණක දෘඪාංග

පරිගණකයක අතින් ඇල්ලිය හැකි මෙන් ම, දැකිය හැකි කොටස් පරිගණක දෘඪාංග (hardware) සංරචක ලෙස දැක්විය හැකි ය. මේවාට නිශ්චිත හැඩයක් ඇත. පරිගණකයක බාහිරින් පමණක් නොව පරිගණකයක පද්ධති ඒකකය (system unit) තුළ ද පරිගණක දෘඪාංග ඇත.



3.1 රූපය - බාහිරින් දැකිය හැකි පරිගණක දෘඪාංග කිහිපයක්

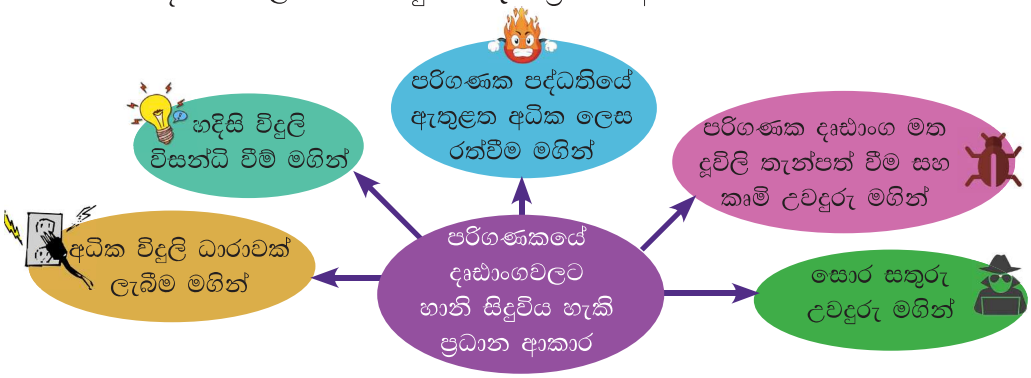


3.2 රූපය - පද්ධති ඒකකය තුළ ඇති දෘඪාංග කිහිපයක්

ක්‍රියාකාරකම 1 : වැඩ පොතේ 3.1 බලන්න

3.2.1 පරිගණක දෘඪාංගවල ආරක්ෂාවට තර්ජන මතුවිය හැකි අවස්ථා

පරිගණකයේ දෘඪාංගවලට හානි සිදුවිය හැකි ප්‍රධාන ආකාර කිහිපයකි.



3.3 රූපය - දඪාංගවලට හානි සිදුවිය හැකි ආකාර කිහිපයක්

3.2.2 පරිගණකයක දෘඩාංග සංරචක ආරක්ෂා කර ගැනීමට සිදු කළ හැකි දෑ

අනවරත ජව සැපයුම් භාවිතය

(uninterruptable power supply - UPS)

- අනවරත ජව සැපයුමක් හරහා විදුලිය ලබා දීම මගින් හදිසි විදුලි බිඳ වැටීමකදී ක්ෂණිකව විදුලිය විසන්ධි නොවී යම් කාලයක් විදුලිය ලබා දෙයි.
- එබැවින් පරිගණකයෙහි සිදු කරන කාර්යයන් සුරැකීම (save) හා පරිගණකය වසා දැමීම (shutdown) සඳහා අවශ්‍ය කාලය ලැබේ.

විලායක භාවිතය

fuse

- අධික ධාරාවක් ලැබීමෙන් පරිගණකයට සිදු වන හානි වළකාලයි.
- ජව සැපයුම් ඒකකය (power supply unit) ආදියෙහි බහුලව භාවිත වේ.
- වර්තමානයේ භාවිතයේ පහසුව නිසා විලායක වෙනුවට සිඟිති පරිපථ බිඳින (mini circuit breakers - MCB) නැමැති උපාංගයක් භාවිත වේ.

ඝර්ජන ආරක්ෂක භාවිතය

surge protection

- අධික ධාරාවක් ගලා යාම හෝ අකුණු ගැසීම ආදියෙන් පරිගණකය ආරක්ෂා කරයි.
- අධික විදුලි ධාරාවක් උපකරණ තුළට ගලා ඒම පාලනය කර එම විදුලිය භූගත කරනු ලැබේ.

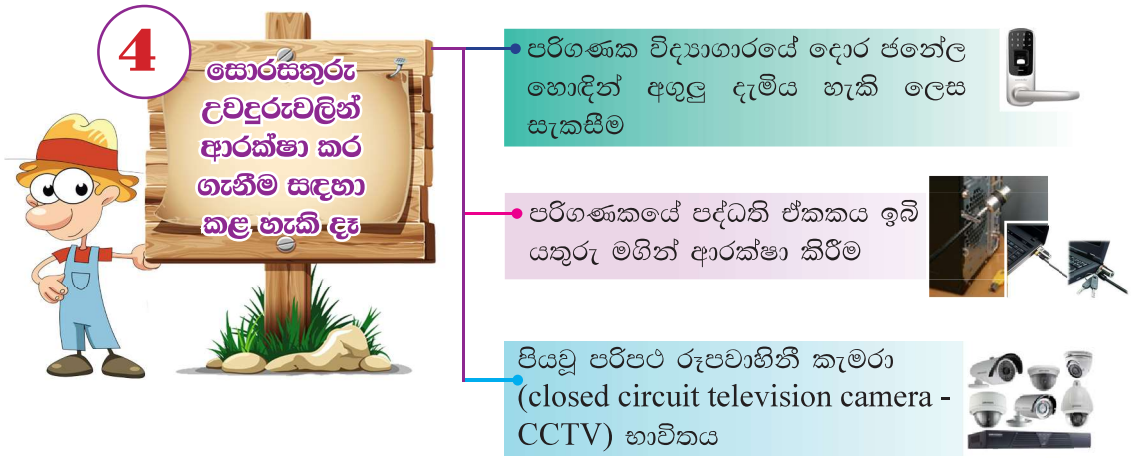
- පරිගණක විද්‍යාගාරය ඇතුළත වායුසමනය කිරීම සඳහා වායුසමීකරණ යොදා ගැනීම

- පරිගණකය තුළ අධික ලෙස රත්වන උපාංග මත සිසිලන පංකා සවි කිරීම

දුවිලි තැන්පත් වීම, අධික තෙතමනය, කෘමි උවදුරු වැනි භෞතික හානිවලින් ආරක්ෂා වීම සඳහා පරිගණක විද්‍යාගාරය ඇතුළත පිරිසිදු ව තබා ගැනීම අවශ්‍ය වේ. ඒ සඳහා අපට අනුගමනය කළ හැකි දෑ පහත ආකාරයට දැක්විය හැකි ය.

3.4 රූපය - භෞතික හානිවලින් පරිගණකය ආරක්ෂා කර ගැනීම සඳහා අනුගමනය කළ හැකි පියවර කිහිපයක්

- පාවහන් ගලවා විද්‍යාගාරයට ඇතුළු වීම මගින් විද්‍යාගාරය තුළ වැලි, දූවිලි ආදියෙන් තොර පරිසරයක් පවත්වාගත හැකි ය.
- විද්‍යාගාරයේ ඇති සියලු පරිගණක තෙමසකට වරක්වත් පිරිසිදු කිරීමෙන් පරිගණකයේ පරිපථ මත දූවිලි ආදිය රැඳීම වැළකේ.
- විද්‍යාගාරය තුළ ආහාර ගැනීමෙන් බිම වැටුණු ආහාර කැබලිවලට කුහුඹුවන් වැනි කෘමීන් ඇදී ආ හැකි ය.
- විද්‍යාගාරය තුළ තෙතමනය රැඳීම නිසා පරිපථ ලුහුවත් (short circuit) විය හැකි ය.



ක්‍රියාකාරකම 2 : වැඩ පොතේ 3.2 බලන්න

3.3 පරිගණකයක මෘදුකාංග සංරචක ආරක්ෂා කර ගනිමු

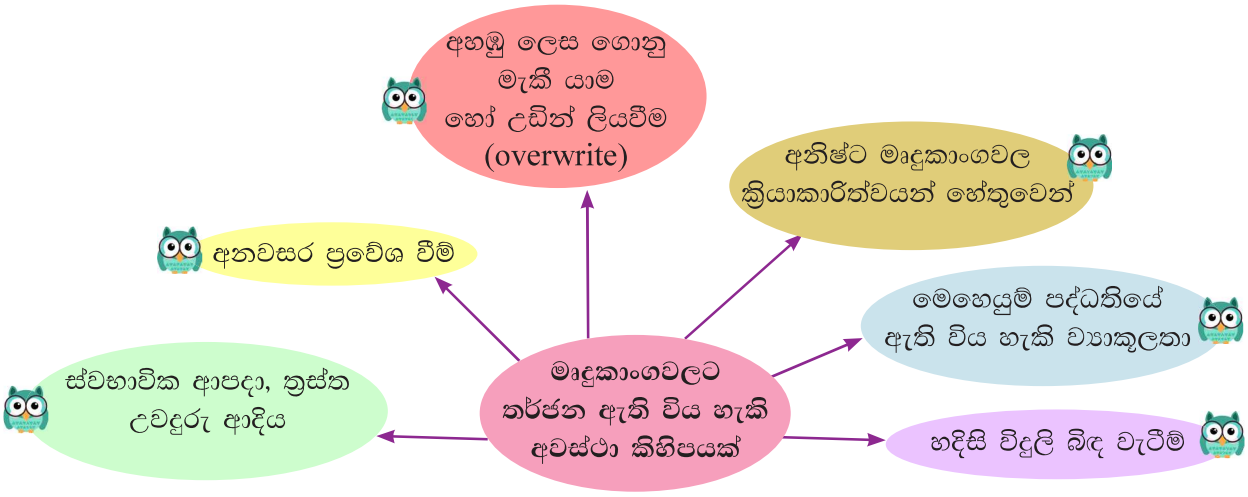
පරිගණකයක මෘදුකාංග

පරිගණකය තුළ ඇති දත්ත, තොරතුරු හා විවිධ කාර්ය සඳහා යොදා ගන්නා වැඩසටහන් පරිගණකයක මෘදුකාංග (software) යටතට ගැනේ.

උදාහරණ:
- මෙහෙයුම් පද්ධතිය
- වදන් සැකසුම් මෘදුකාංග
- ලිපි ලේඛන ඇතුළත් ගොනු
- පින්තූර ඇතුළත් ගොනු

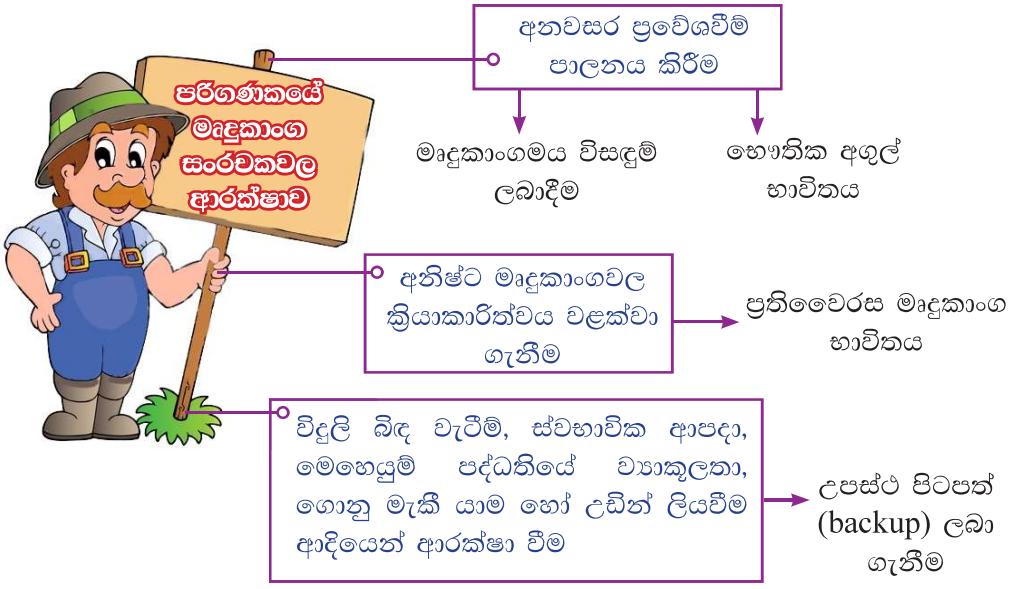
3.3.1 මෘදුකාංගවලට තර්ජන ඇතිවිය හැකි අවස්ථා

මෘදුකාංගවලට තර්ජන ඇති විය හැකි ප්‍රධාන අවස්ථා කිහිපයක් පහත දැක්වේ.



3.5 රූපය - මෘදුකාංග සංරචකවලට තර්ජන ඇතිවිය හැකි අවස්ථා කිහිපයක්

3.3.2 පරිගණකයක මෘදුකාංග සංරචක ආරක්ෂා කර ගැනීම සඳහා සිදු කළ හැකි දෑ



3.5 රූපය - මෘදුකාංග සංරචවල ආරක්ෂාව සඳහා ගත හැකි ක්‍රියාමාර්ග කිහිපයක්

ක්‍රියාකාරකම 3 : වැඩ පොතේ 3.3 බලන්න

1 අනිෂ්ට මෘදුකාංගවලට එරෙහි ආරක්ෂාව සැපයීම

පරිගණකයක මෘදුකාංගවල ආරක්ෂාවට තර්ජනය එල්ල විය හැකි ප්‍රධාන ආකාරයක් ලෙස අනිෂ්ට මෘදුකාංග දැක්විය හැකි ය.

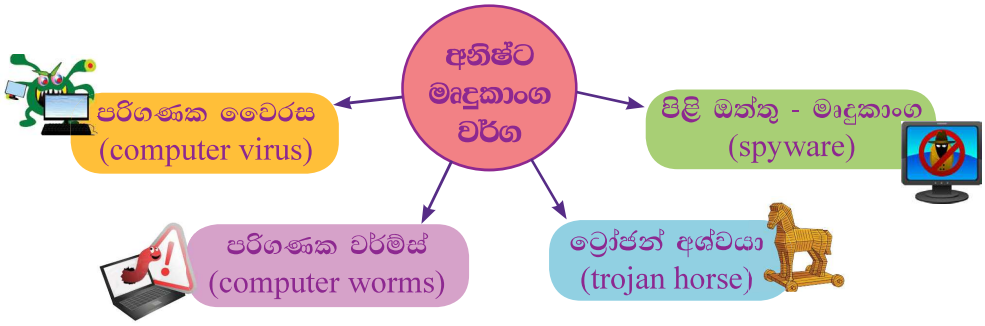
අනිෂ්ට මෘදුකාංග යනු මොනවා ද?

පරිගණක පරිශීලකයකුගේ අවශ්‍යතාවන්ට එරෙහි ව ක්‍රියාත්මක වෙමින්,

- පරිගණකයේ ස්ථාපනය කර ඇති මෘදුකාංගවලට
- පරිගණකයේ තැන්පත් කර ඇති දත්ත ආදියට
- පරිගණක ජාලවලට
- ඇතැම් විට පරිගණක දෘඩාංගවලට පවා හානි කරන මිනිසා විසින් ම නිර්මාණය කර ඇති මෘදුකාංගයක් හෝ මෘදුකාංග කොටසක් අනිෂ්ට මෘදුකාංග (malware software) ලෙස හඳුන්වයි.

අනිෂ්ට මෘදුකාංග වර්ග රැසක් පවතී. මේ අතරින් සමහර අනිෂ්ට මෘදුකාංග දෙමුහුන් ස්වරූපයක් ගනී. එනම් එය වරින් වර විවිධ ස්වරූපයෙන් ක්‍රියාත්මක වේ.

උදා: එක් අවස්ථාවක පරිගණක වෛරසයක් ලෙස හැසිරෙන අනිෂ්ට මෘදුකාංගය ම තවත් අවස්ථාවක ට්‍රෝජන් අශ්වයා ලෙස ද හැසිරේ.



3.6 රූපය - අනිෂ්ට මෘදුකාංග වර්ග කිහිපයක්

1. පරිගණක වෛරස (computer virus)

පරිගණක මෘදුකාංගවලට හා ගොනුවලට සම්බන්ධ වෙමින්, තම වෛරසයේ ම අනුපිටපත් සාදමින් එහා මෙහා රැගෙන යන ආචයන උපාංග හරහා අනෙක් පරිගණක වෙත ආසාදනය වීමේ හැකියාව ඇති ප්‍රධානත ම අනිෂ්ට මෘදුකාංගය යි. දත්ත හා තොරතුරු මකා දැමීම, වෙනස් කිරීම සහ මෘදුකාංග අඩපණ කිරීම වැනි දෑ සිදු කළ හැකි ය.

2. පරිගණක වර්ම්ස් (computer worms)

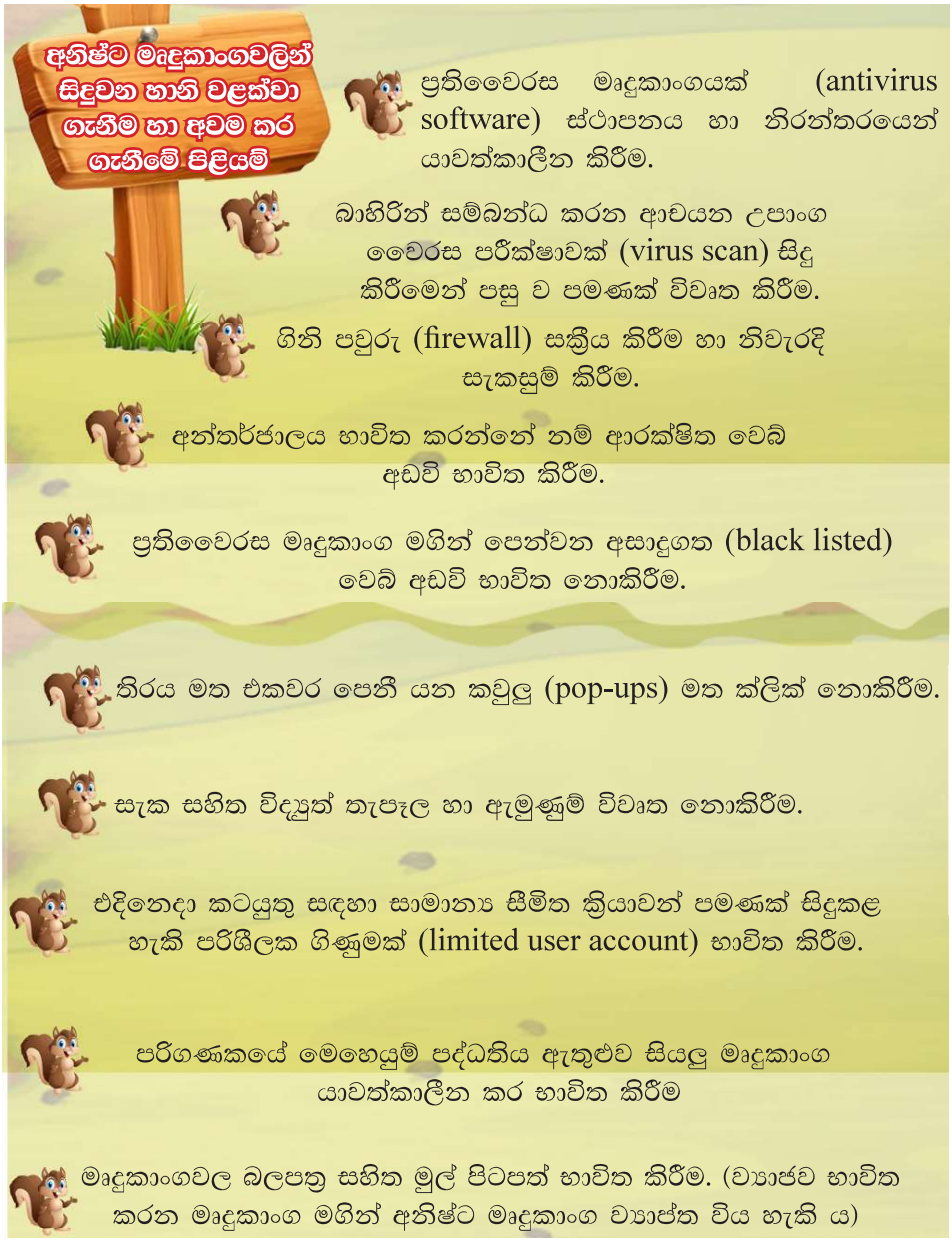
ඉහත ආකාරයේ ම තර්ජන ඇති කරයි. මෙහි ප්‍රධානත ම වෙනස වන්නේ පරිගණක ජාල හා අන්තර්ජාලය භාවිතයෙන් ස්වයංක්‍රියව ව්‍යාප්ත වීමයි.

3. ට්‍රෝජන් අශ්වයා (trojan horse)

බැලූ බැල්මට ප්‍රයෝජනවත් මෘදුකාංගයක් ලෙස පෙනී සිටින අතර භාවිත කිරීම ආරම්භ කළ පසු පරිශීලකයාට රහසින් අනර්ථකාරී කාර්යයන් සිදුකරයි.

4. පිළි ඔත්තු- මෘදුකාංග (spyware)

පුද්ගලයකුගේ පරිගණක භාවිතය, අන්තර්ජාල පරිහරණය ආදී තොරතුරු රහසිගත ව රැස්කර වෙනත් පාර්ශව වෙත රහසින් ලබා දෙන අනිෂ්ට මෘදුකාංගයකි. මෙමගින් දත්ත හා තොරතුරු වුව ද වෙනත් පාර්ශව වෙත රහසින් ලබා දිය හැකි ය.



ක්‍රියාකාරකම 5 : වැඩ පොතේ 3.5 බලන්න

2 උපස්ථ පිටපත් ලබා ගැනීම

මෘදුකාංග සංරචකවල පිටපත් තබා ගැනීමේ ක්‍රියාවලිය උපස්ථ (backups) තබා ගැනීම ලෙස හැඳින්වේ.

උපස්ථ ලෙස තබා ගන්නා පිටපත්, මුල් පිටපත් අවස්ථානගත වූ විට හෝ පළුදු වූ විට භාවිත කළ හැකි ය. උපස්ථ පිටපත් තබා ගැනීම සඳහා විවිධ ආචයන උපක්‍රම භාවිත කළ හැකි ය.

උදාහරණ: සංගත තැටි (CD)
අංකිත වීඩියෝ තැටිය (DVD)
බාහිර දෘඪ තැටි
පරිගණකයේ ම වෙනත් ස්ථානයක් (වෙනත් ගොනු බහලුම, වෙනත් ධාවකයක් වැනි ස්ථානයක)

3 ප්‍රවේශ පාලනය (Access Control)

ප්‍රවේශය පාලනය සඳහා මෘදුකාංගමය විසඳුම් ලබා දීම

මෙහි දී ප්‍රවේශය පාලනය (access control) හා පරිගණකයේ ඇති සම්පත් ආරක්ෂා කිරීම සඳහා විවිධ මෘදුකාංග මගින් සපයන ක්‍රම හා සේවා දැක්විය හැකි ය.

1. ශක්තිමත් හා අනුමාන කළ නොහැකි මුරපද (passwords) භාවිතය
2. සුදුසු පරිශීලක ගිණුම් (user accounts) සැකසීම
3. ගුප්ත කේතනය (encryption)

ඉහත දක්වා ඇති ක්‍රියාමාර්ග මගින් ප්‍රවේශය පාලනය මෙන් ම හදිසි දත්ත නැතිවීම්වලින් ද දත්ත හා තොරතුරු ආරක්ෂා කර ගත හැකි ය.

ගුප්ත කේතනය කර ඇති දත්ත වෙනත් පාර්ශවයක් අතට පත් වුවහොත් එම දත්ත කියවීමට හා කියවා තේරුම් ගැනීම නොහැකි ලෙස සකසා ඇත. මෙම ක්‍රමය විශේෂයෙන් ඉතා වැදගත් දත්ත සන්නිවේදනයේ දී යොදා ගනියි.

ප්‍රවේශය පාලනය සඳහා භෞතික අගුල් භාවිතය

මෙම ක්‍රමයේ දී දෘඪාංග ලෙස පවතින උපාංග හා ක්‍රම භාවිතයෙන් පරිගණක පද්ධතිය හා එහි ගබඩා කර ඇති දත්ත, තොරතුරු හා මෘදුකාංග ආරක්ෂා කරනු ලැබේ. මේ සඳහා භාවිත කරන ක්‍රම වන්නේ;

1. පරිගණකය ආරක්ෂිත ස්ථානයක ස්ථානගත කිරීම

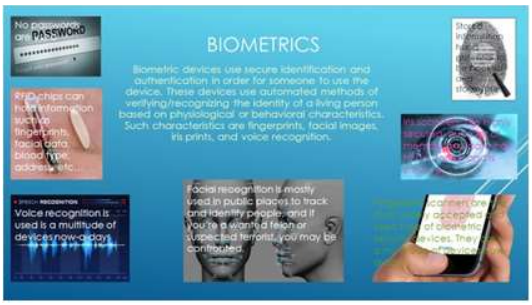
ඉතා සංවේදී හා වැදගත් දත්ත, තොරතුරු ආදිය ගබඩා කර ඇති පරිගණක සොර සතුරන්ගෙන් හා අනවශ්‍ය පුද්ගල ප්‍රවේශයෙන් ආරක්ෂා කිරීම සඳහා පරිගණකය ආරක්ෂිත ස්ථානයක ස්ථානගත කිරීම සුදුසුය.

2. ආරක්ෂිත කැමරා පද්ධති (CCTV camera) හා අනතුරු ඇඟවීමේ සංඥා (alarm) භාවිතය

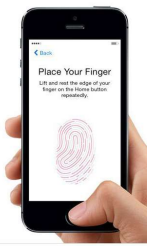
තවදුරටත් අවශ්‍ය අවස්ථාවන්වලදී නිරීක්ෂණයන් සිදු කිරීම, ස්වයංක්‍රීයව හඳිසි පණිවිඩ ලබාදීම වැනි ක්‍රියාවන් මෙවැනි පද්ධති මගින් සිදු කරයි.

3. ජීවමිතික මුරපද භාවිතය (biometric passwords)

වර්තමානයේ දී පරිගණක පද්ධතිවලට ප්‍රවේශවීමට ද පරිගණක විද්‍යාගාර ආදියෙහි දොරගුළු සඳහා ද ඇඟිලි සළකුණු වැනි ජීවමිතික මුරපද බහුලව භාවිත කරයි.



ජීවමිතික (biometric) මුරපද සාම්ප්‍රදායික මුරපද මෙන් නොව අවසරලත් පුද්ගලයාගේ ඇඟිලි සලකුණු කටහඬ, මුහුණ හෝ අක්ෂි කාචය වැනි දෙයක අනන්‍යතාව හඳුනා ගැනීමෙන් පද්ධතියට ප්‍රවේශ වීමේ අවස්ථාව දෙනු ලැබේ.



3.7 රූපය - ජංගම දුරකථන හා ලැප්ටොප් පරිගණක සඳහා ජීවමිතික මුරපද භාවිතය

ක්‍රියාකාරකම 5 : වැඩ පොතේ 3.5 බලන්න

සාරාංශය

★ පරිගණක පද්ධතියට ආරක්ෂාව සැලසීමේ දී දෘඪාංග සංරචකවල මෙන් ම මෘදුකාංග සංරචකවල ද ආරක්ෂාව පිළිබඳ සැලකිලිමත් විය යුතු ය.

★ දෘඪාංග ආරක්ෂාවට තර්ජන මතුවිය හැකි අවස්ථා කිහිපයක්
- හදිසි විදුලි විසන්ධි වීම්
- අධික විදුලි ධාරාවක් ලැබීම
- පරිගණක පද්ධතියේ ඇතුළත අධික ලෙස රත්වීම
- පරිගණක දෘඪාංග මත දූවිලි තැන්පත් වීම සහ කෘමි උවදුරු
- සොරසතුරු උවදුරු

★ දෘඪාංගවල ආරක්ෂාව සඳහා
- විදුලිය නිසා පරිගණකයට සිදුවන හානි අවම කිරීම
- පරිගණකය ඇතුළත අධික ලෙස රත් වීම අවම කිරීම
- භෞතික හානිවලින් පරිගණකය ආරක්ෂා කර ගැනීම
- සොරසතුරු උවදුරුවලින් ආරක්ෂා කර ගැනීම

ආදි පියවර රැසක් අනුගමනය කළ හැකි ය.

★ මෘදුකාංගවල ආරක්ෂාවට තර්ජන මතුවිය හැකි අවස්ථා කිහිපයක්
- අනිෂ්ට මෘදුකාංගවල ක්‍රියාකාරිත්වය
- අනවසර ප්‍රවේශ වීම්
- හදිසි විදුලි බිඳවැටීම්
- ස්වභාවික ආපදා, ත්‍රස්ත උවදුරු ආදිය
- මෙහෙයුම් පද්ධතිය් ඇති විය හැකි ව්‍යාකූලතා
- අහඹු ලෙස ගොනු මැකී යාම හෝ උඩින් ලියවීම

★ මෘදුකාංගවල ආරක්ෂාව සඳහා
- අනිෂ්ට මෘදුකාංගවලට එරෙහි ආරක්ෂාව සැපයීම
- උපස්ථ පිටපත් ලබා ගැනීම
- ප්‍රවේශ පාලනය

ආදී පියවර රැසක් අනුගමනය කළ හැකි ය.