පරිගණක සහ ආරක්ෂාව (Computers and Security)

පරිගණක, පරිගණක ජාල සහ අන්තර්ජාලය අපට බෙහෙවින් ප්‍රයෝජනවත් වුවද ඒවා භාවිතයේදී අපගේ ආරක්ෂාව (දත්ත, මෘදුකාංග සහ පෞද්ගලික ආරක්ෂාව) පිළිබඳව සැලකිලිමත් වීම ද ඉතාමත් වැදගත්ය. පරිගණක සහ පරිගණක ජාල භාවිතයේ දී අපගේ දත්ත සොරා ගැනීමටත්, මැකීමට හෝ වෙනස් කිරීමටත්, මෘදුකාංග වෙනස් කිරීමට හෝ ක්‍රියාවිරහිත කිරීමටත්, පෞද්ගලික දත්ත සොරාගෙන ඒවා අයුතු ලෙස භාවිතාකිරීමටත් යම් අයෙකු ක්‍රියා කළ හැක. පරිගණක භාවිතයේදී ආරක්ෂාව පිළිබඳව ඇතිවිය හැකි ගැටලු සහ ඒවාට විසඳුම් මෙහිදී සාකච්ඡා කෙරේ.

9.1 පරිගණක ජාල සහ අන්තර්ජාලය භාවිතයේදී ආරක්ෂාව පිළිබඳව සැලකිලිමත් විය යුත්තේ ඇයි?

වර්තමානයේ පරිගණක ජාල හා අන්තර්ජාලය හරහා විවිධ ආකාරයේ පරිගණක අපරාධ සිදු වේ. ඇතැම් ත්‍රස්තවාදී සංවිධාන කඩාකප්පල්කාරී ක්‍රියා සඳහාත්, ඇතැම් පුද්ගලයින් විශාල වශයෙන් මුදල් ඉපයීම සඳහාත්, ඇතැම් විට වෙනත් පුද්ගලයින්ගෙන් පලිගැනීම හෝ ඔවුන් අපහසුතාවයට පත් කිරීම සඳහාත් වැනි විවිධ හේතු අරමුණු කර ගෙන පරිගණක අපරාධ සිදු කරයි. එවැනි අපරාධ සමහරක් පහත විස්තර වේ.

9.1.1 අනවසර සම්බන්ධය (Unauthorized Access)

අවසරයකින් තොරව පරිගණකයකට, පරිගණක ජාලයකට, හෝ පරිගණක ගොනුවකට සම්බන්ධවීම මෙයින් අදහස් කරයි. මෙසේ අනවසරයෙන් පරිගණකයකට සම්බන්ධවීම හැකින් (hacking) ලෙස ද එසේ කරන්නා හැකර් (hacker) ලෙසද හැඳින් වේ. එසේ අනවසරයෙන් පරිගණකයකට සම්බන්ධ වී යම් හානියක් සිදු කිරීම ක්‍රැකින් (Cracking) ලෙස හඳුන්වයි. (විවිධ පුද්ගලයින් විවිධ අවශ්‍යතා සඳහා අනවසරයෙන් පරිගණකවලට සම්බන්ධ විය හැක.

- පරිගණකයක ඇති දත්ත සහ තොරතුරු ලබා ගැනීම.
- වෙනත් අයෙකුගේ විද්‍යුත් තැපැල් ලිපියක් කියවීම සහ ඔහු හෝ ඇයගේ නමින් වෙනත් අයෙකුට විද්‍යුත් තැපැල් ලිපියක් යැවීම.
- කෙනෙකුගේ බැංකු ගිණුම් අංකය, ණය පත් අංකය (Credit card) වැනි රහසිගත තොරතුරු සහ පෞද්ගලික තොරතුරු ලබා ගැනීම.
- පරිගණක හරහා සිදුවන දුරකතන ඇමතුම් හෝ වෙනත් පණිවිඩ හුවමාරුවකට සවන්දීම.
- බැංකු ගිණුම්වල තොරතුරු වෙනස් කිරීමෙන් මුදල් ලබා ගැනීම.
- වෙනත් අයෙකුට අයත් රැහැන් රහිත (wi-fi) අන්තර්ජාල සම්බන්ධතාවයක් හරහා නොමිලේ අන්තර්ජාලයට සම්බන්ධ වීම.
- රහසිගත ව්‍යාපාරික තොරතුරු සොරා ගැනීම.
- රටක රාජ්‍ය ආරක්ෂාවට වැදගත් තොරතුරු සොරා ගැනීම.
- කෙනෙකුගේ පරිගණකයකට අසභ්‍ය ඡායාරූප හෝ වෙනත් එවැනි දේ ඇතුලත් කිරීම.
- කෙනෙකුගේ සමාජ වෙබ් අඩවි ගිණුමකට සම්බන්ධ වී එම කෙනාගේ නමින් ඔහුගේ හෝ ඇයගේ මිතුරන් සමඟ පණිවිඩ හුවමාරු කර ගැනීම.

එසේ සම්බන්ධවීම අනුන්ගේ පරිගණකයක් වෙත පැමිණ එය භාවිතා කිරීම හෝ වෙනත් ස්ථානයක සිට පරිගණක ජාලයක් හෝ අන්තර්ජාලය හරහා පරිගණකයකට සම්බන්ධවීම යන ආකාර දෙකෙන්ම සිදුවිය හැක. බොහෝ රටවල නීතියට අනුව මොනම හේතුවක් සඳහා හෝ වෙනත් අයෙකුගේ පරිගණකයකට අනවසරයෙන් සම්බන්ධ වීම දඩුවම් ලැබීමට හේතුවන නීති විරෝධී කාර්යයකි.

9.1.2 පරිගණක හෝ එයට අදාල නොයෙකුත් සම්පත් සඳහා හානි පැමිණවීම (Computer Sabotage)

පරිගණක සහ එයට සම්බන්ධ මෘදුකාංග සහ දත්ත වැනි සම්පත්වලට හානි පැමිණවීම වර්තමානයේ සිදුවන තවත් ප්‍රධාන පරිගණක අපරාධයකි. පරිගණකයකට වෛරසයක් ඇතුලත් කිරීම, පරිගණකයක්

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

ක්‍රියාවිරහිත වන ආකාරයේ ක්‍රියාවක් කිරීම, වෙබ් අඩවියක අඩංගු කරුණු වෙනස් කිරීම, පරිගණකයක ඇති දත්ත හෝ මෘදුකාංග වෙනස් කිරීම යනාදී ක්‍රියා මෙහිදී සිදුවේ. මෙසේ පරිගණක සම්පත් සඳහා හානි පැමිණීමේදී වර්තමානයේ යොදා ගන්නා ප්‍රධාන ක්‍රමයක් බොට්නෙට් (Botnet) ලෙස හැඳින් වේ. බොට්නෙට් ලෙස හැඳින්වෙන මෘදුකාංගයක් යම් පරිගණකයකට රහසිගතව ස්ථාපිත කිරීමෙන් (අන්තර්ජාලය භාවිතයෙන් මෙම මෘදුකාංගය ඈත පිහිටි පරිගණකයකට වුවද ස්ථාපිත කළ හැක) එම පරිගණකය ඈත සිට අන්තර්ජාලය හරහා පාලනය කිරීමට එම මෘදුකාංගය ස්ථාපිත කල තැනැත්තාට පුළුවන. එවිට එම පරිගණකයේ ඇති සියලුම මෘදුකාංග සහ දත්ත ලබාගැනීමට හෝ වෙනස් කිරීමටත් පරිගණකය භාවිතාකරන්නා පරිගණකය සමග කරනු ලබන සියලු කටයුතු නිරීක්ෂණය කිරීමටත් එම බොට්නෙට් මෘදුකාංගය ස්ථාපිත කළ තැනැත්තාට හැකියාව ලැබේ. මෙම බොට්නෙට් මෘදුකාංග නිෂ්පාදනය කරන්නේ ඒවා වෙනත් අයට විකිණීමත් සහ බොට්නෙට් මගින් ලබා ගන්නා රහසිගත තොරතුරු විවිධ නීති විරෝධී කාර්යයන් සඳහා යොදා ගැනීමත් වර්තමානයේ අන්තර්ජාලය සහ පරිගණක ජාල භාවිතා කරන්නන් මුහුන දෙන විශාල ගැටලුවකි.

9.1.3 පරිගණක වෛරස සහ වෙනත් එවැනි අනිශ්ඨ මෘදුකාංග (Computer viruses and other types of Malware)

අනිශ්ඨ මෘදුකාංග යනු පරිගණක භාවිතයේදී ගැටලු ඇති කරවන ආකාරයට සිතාමතාම නිර්මාණය කර ඇති විවිධාකාරයේ මෘදුකාංග වේ. අනිශ්ඨ මෘදුකාංග වර්ග කීපයකි. පරිගණක වෛරස (computer virus), පරිගණක වර්ම් (computer worm), සහ ට්‍රෝජන් හෝස් (Trojan horse)

පරිගණක වෛරස

පරිගණක වෛරසයක් යනු යම් පුද්ගලයකු විසින් සිතාමතාම සකස් කර ඇති පරිගණකයක සාමාන්‍ය ක්‍රියාකාරිත්වය යම් ආකාරයක වෙනසකට ලක් කරවන මෘදුකාංගයකි. මෙහි ඇති විශේෂ ලක්ෂණයක් වන්නේ පරිගණකයක් භාවිතා කරන්නාට නොදැනීම පරිගණකයට ඇතුළු වී ඉබේම පරිගණකයට ස්ථාපිත වීම සහ එම පරිගණකයට සම්බන්ධ වන වෙනත් පරිගණක සහ දත්ත ගබඩා මාධ්‍යයනට ද එම වෛරසය ඉබේම පැතිරීමයි. පරිගණක වෛරස බොහෝවිට වෙනත් මෘදුකාංග හෝ දත්ත ගොනු සමඟ සම්බන්ධ වී ඒවා බාගත (download) කරන විට හෝ පිටපත් (Copy) කරන විට පැතිරෙයි. උදාහරණ වශයෙන් පරිණාක ක්‍රීඩා, වීඩියෝ සහ ගීත අන්තර්ජාලයේ වෙබ් අඩවි වලින් බාගත කිරීමේදි අප පරිගණකවලට වෛරස ඇතුළු විය හැක. විද්‍යුත් තැපැල් ලිපි සමඟ ද වෛරස පැතිරෙයි. විද්‍යුත් තැපැල් ලිපියක ඇති සබැඳියක් (link) ක්ලික් කිරීමේදී එයට සම්බන්ධකර ඇති වෛරසයක් අප පරිගණකයට ස්ථාපිත විය හැක. පරිගණක අතර දත්ත හුවමාරු කරන ගබඩා මාධ්‍ය (Pen drive වැනි) මගින් ද වෛරස පැතිරේ.

පරිගණක වර්ම් (Computer Worm)

පරිගණක වෛරස මෙන්ම පරිගණක වර්ම් අපගේ පරිගණක භාවිතයේදී ගැටලු ඇති කරයි. මෙහි ඇති ප්‍රධාන වෙනස වන්නේ ඒවා අනිකුත් පරිගණකවලට පැතිරීම සඳහා පරිගණක ගොනු (files) වලට සම්බන්ධ නොවීමයි. වර්ම් පැතිරෙන්නේ පරිගණක ජාල සහ අන්තර්ජාලය හරහායි. බොහෝවිට වර්ම් පැතිරෙන්නේ විද්‍යුත් තැපැල් ලිපිවල ඇමුණුම් (Attachment) වශයෙනි. යම් විද්‍යුත් තැපැල් ගිණුමකට පැමිණෙන වර්ම් එකක් එම ගිණුමේ ඇති අනිකුත් සියලුම විද්‍යුත්තැපැල් ලිපිනයන්ට (contact list/Address book) එම වර්ම් එකේ පිටපත් ස්වයංක්‍රීයව යවයි. එබැවින් පරිගණක වර්ම් විද්‍යුත් තැපැල් හරහා ලෝකය පුරා ඉතා වේගයෙන් පැතිරී යයි.

ට්‍රෝජන් හෝස් (Trojan horse)

ට්‍රෝජන් හෝස් යනු පරිගණකයේ සාමාන්‍ය ක්‍රියාකාරිත්වයට යම් වෙනසක් ඇති කරවන යම් පුද්ගලයකු සිතාමතා ලියා ඇති පරිගණක වැඩසටහනකි. මෙහි ඇති විශේෂත්වය වනුයේ එය සාමාන්‍ය පරිගණක වැඩසටහනක් ලෙස පරිගණකය භාවිතා කරන්නාට පෙනන නමුත් එම වැඩසටහන ක්‍රියාත්මක කිරීමේදී එයින් බලාපොරොත්තු වන කාර්යයට අමතරව භාවිතා කරන්නට නොදැනිම වෙනත් හානිකර කාර්යයක්

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

සිදුවීමයි. උදාහරණයක් වශයෙන් පරිගණක ක්‍රීඩාවක් ලෙස පෙනෙන ට්‍රෝජන් හෝස් වෛරසයක් එම ක්‍රීඩාව කිරීමේදී ක්‍රීඩාව කරන්නා බලාපොරොත්තු නොවන හානිකර කාර්යයක් යටින් සිදුවීම. ට්‍රෝජන් හෝස් වෛරස් අනෙකුත් වෛරස් මෙන් ඉබේ පැතිරීමේ හැකියාවෙන් යුක්ත නොවන නමුත් අන්තර්ජාලය හරහා බාගත (download) වීම මගින් පැතිරී යයි. එසේම විද්‍යුත් තැපැල් ලිපියක ඇමුණුමක් වශයෙන් ට්‍රෝජන් හෝස් වෛරසයක් පැමිණිය හැක. බොහෝ විට ට්‍රෝජන් හෝස් මගින් අපගේ පරිගණකවල ඇති දත්ත, බැංකු ගිණුම් අංක, මුරපද (password), ණයපත් අංක හෝ වෙනත් එවැනි පෞද්ගලික තොරතුරු වෙනත් කෙනෙකු වෙත යැවීම සිදුවේ.

පරිගණක වයිරස සහ වෙනත් එවැනි අනිශ්ඨ මෘදුකාංග මගින් සිදුවිය හැකි අහිතකර ප්‍රතිඵල

- පරිගණකයක ඇති ප්‍රයෝජනවත් දත්ත මැකීම.
- පරිගණකයේ සාමාන්‍ය ක්‍රියාකාරී වේගය අඩුවීම.
- පරිගණක වැඩසටහන්වල ක්‍රියාකාරීත්වය වෙනස් වීම.
- පරිගණක වැඩසටහන් ක්‍රියාවිරහිත වීම.
- පරිගණකය ආරම්භ කල නොහැකිවීම (boot)
- පරිගණකය ඉබේම වැසීම (shutdown)
- පරිගණකයේ දත්ත ගොනු විවෘත කළ නොහැකි වීම.
- පරිගණකයේ මතකයට අනවශ්‍ය දත්ත පුරවා අවහිර කිරීම.
- අනවශ්‍ය ගොනු හෝ තිබෙන ගොනුවල පිටපත් රාශියක් තැන්පත් වීමෙන් පරිගණකයේ දෘඪ තැටියේ ධාරිතාවය අඩුවීම.
- දෘඪ තැටියේ ඇති සියලුම ගොනු මැකීම.
- වෙබ් පිටුවක අඩංගු කරුණු වෙනස් කිරීම.
- පෞද්ගලික දත්ත සොරා ගැනීම.
- පරිගණකය භාවිතා කරන්නා කරන කටයුතු නිරීක්ෂණය කිරීම.
- විද්‍යුත් තැපැල් ලිපි කියවීම.

ඇතැම් පරිගණක වෛරස හානිකර නොවන අතර ඒවා පවතින බව පෙන්වීමට පරිගණක තිරයේ යමක් දර්ශනය වීම වැනි ක්‍රියාවක් පමණක් සිදුවේ. ඇතැම් පරිගණක වෛරස ඒවා අපගේ පරිගණකයට පැමිණි වහාම ක්‍රියාත්මක වන නමුත් තවත් ඇතැම් වෛරස යම් දිනයක්, වෙලාවක් හෝ පරිගණකය භාවිතා කරන්නා කරනු ලබන යම් ක්‍රියාවක් (යම් වැඩසටහනක් ක්‍රියාත්මක කිරීම, යතුරු පුවරුවේ යම් යතුරක් ඔබීම) බලාපොරොත්තුවෙන් සිටින අතර එම අවස්ථාව පැමිණි වහාම ක්‍රියාත්මක වේ (time-bomb, Logic-bomb). පරිගණකවලට බොහෝ දුරට සමාන ක්‍රියාකාරීත්වයක් සහිත ජංගම දුරකතන හෝ වෙනත් එවැනි උපකරණ සඳහා ද පරිගණක වෛරස මගින් හානිකර ප්‍රතිඵල ඇතිවිය හැක.

පරිගණක වෛසරය සහ වෙනත් එවැනි අනිෂ්ඨ මෘදුකාංග පැතිරීම සහ ඒවායින් සිදුවන අහිතකර ප්‍රතිඵල අවමකර ගැනීම සඳහා පරිගණක පරිශීලකයකුට භාවිත කළ හැකි සාමාන්‍ය ආරක්ෂණ ක්‍රම-

- තම පරිගණකය සඳහා ප්‍රති වෛරස (Anti-virus) මෘදුකාංගයක් ස්ථාපිත කර ගැනීම. ප්‍රතිවයිරස මෘදුකාංග පරිගණකය වෙත පැමිණෙන වෛරස හඳුනාගෙන ඒවා ඉවත් කිරීමට කටයුතු කරයි.
- ප්‍රතිවෛරස මෘදුකාංගය නිතර යාවත්කාලීන කිරීම: යම් ප්‍රති වෛරස මෘදුකාංගයකට හසුකරගත හැක්කේ එයට හඳුනාගත හැකි වෛරස පමණි. වෛරස හඳුනාගැනීම සඳහා ඒවායේ ලක්ෂණ සහ හැසිරීම් රටාව පිළිබඳව දත්ත ඇතුලත් දත්ත සමූදායක් (Virus definition file) ප්‍රතිවෛරස මෘදුකාංගයට සම්බන්ධව ඇත. යම් ප්‍රතිවෛරස මෘදුකාංගයක් නිර්මාණය කිරීමෙන් පසුව නිශ්පාදනය කරන අලුත් වෛරස් පිළිබඳ දත්ත මෙම දත්ත සමුදාය තුල නොමැති බැවින් ඒවා හඳුනාගැනීමට ප්‍රති වෛරස මෘදුකාංගය අසමත් වේ. එබැවින් අළුත්

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

වෛරස හඳුනා ගැනීම සඳහා එම වෛරසය පිළිබඳ දත්ත මෙම දත්ත සමුදායට ඇතුලත් කිරීම අවශ්‍ය වේ. එසේ කළ හැක්කේ ප්‍රති වෛරස මෘදුකාංගය නිතර යාවත්කාලීන කිරීම මගිනි.

- පරිගණක ක්‍රීඩා, වෙනත් මෘදුකාංග හෝ වීඩියෝ දර්ශන, ගීත යනාදිය ඒවා නොමිලේ ලබාදෙන වෙබ් අඩවි වලින් බාගත කිරීමෙන් හැකි පමණ වැලකී සිටිය යුතු අතර යම් මෘදුකාංගයක් එසේ බාගත කරන්නේ නම් ඒවා භාවිතා කිරීමට පෙර හෝ බාගත කරන අවස්ථාවේදීම ප්‍රතිවෛරස මෘදුකාංගයක් මගින් හොඳින් පරීක්ෂා කළ යුතුය.
- පරිගණක අතර දත්ත හුවමාරු කිරීම සඳහා භාවිතා කරන ප්ලැෂ් පෙන් ධාවක (Pen drives/thumb drives) වැනි ගබඩා මාධ්‍ය භාවිතා කිරීමට පෙර ඒවායේ වෛරස් ඇත්දැයි ස්කෑන් කර බැලීම.
- නොහඳුනන පුද්ගලයින්ගෙන් ලැබෙන විද්‍යුත් තැපැල් ලිපි විවෘත නොකිරීම
- විද්‍යුත් තැපැල් ලිපියක ඇති ඇමුණුමක් පිළිබඳව සැක සහිත නම් එය විවෘත නොකිරීම.
- විද්‍යුත් තැපැල් ලිපිවල ඇති සැක සහිත සබැඳියන් (Links) ක්ලික් නොකිරීම.
- යම් සැක සහිත පුද්ගයකු කියනු ලබන විධානයක් පරිගණකයට ඇතුලත් නොකිරීම.
- සමාජ වෙබ් අඩවි භාවිතයේදී තම පෞද්ගලික තොරතුරු අනාවරණය කිරීමෙන් හැකි පමණ වැලකීම.
- වෙබ් අඩවි භාවිතයෙන් කතාබස් (chat) කිරීමේදී නොහඳුනන පුද්ගලයකු විසින් ලබා දෙන ගොනු බාගත නොකිරීම.
- යම් ආයතනයකට අදාල රහසිගත තොරතුරු ඇතුලත් පරිගණකයක් අන්තර්ජාලයට සම්බන්ධ කිරීමෙන් වැලකී සිටීම.

9.1.4 සේවා අත්හිටුවීමේ ප්‍රහාර (Denial of Service Attack/Dos attack)

බොහෝ විට මෙවැනි ප්‍රහාර එල්ලවන්නේ විශාල පරිගණක ජාලයක සේවා සපයන ප්‍රධාන පරිගණක සඳහායි. මෙහිදී වෙනත් පරිගණකයක් හෝ පරිගණක කීපයක් යොදාගෙන සේවාසපයන ප්‍රධාන පරිගණකය වෙත සේවා ඉල්ලීම් රාශියක් එවනු ලැබේ. (service request). ඒවා සාමාන්‍ය සේවා ඉල්ලීම් ලෙස සලකන ප්‍රධාන පරිගණකය එම ඉල්ලීම් ඉටු කිරීමට ක්‍රියා කරයි. නමුත් නොකඩවා ලැබෙන විශාල සේවා ඉල්ලීම් ප්‍රමාණය හසුරුවාගත නොහැකිව ප්‍රධාන පරිගණකය ක්‍රියා විරහිත වේ. උදාහරණයක් වශයෙන් ලොව පුරා විසිරී සිටින පාරිභෝගිකයන්ට භාණ්ඩ අලෙවිකරණ විද්‍යුත් වෙළඳාම වෙබ් අඩවියක් සඳහා විවිධ භාණ්ඩ පිළිබඳ විස්තර ඉල්ලීම් රාශියක් එකවර නොකඩවා ඉදිරිපත් වන්නේ නම් එතරම් වේගයෙන් අදාල සියලු විස්තර සපයාගත නොහැකිව ප්‍රධාන පරිගණකය ක්‍රියා විරහිත වේ. යම් ආයතනයකට මෙවැනි ප්‍රහාරයක් සිදුවුවහොත් එම ආයතනයට එය විශාල අලාභයක් වේ.

9.1.5 අනන්‍යතාවය සොරකම් කිරීම (Identity theft)

මෙවැනි වංචාකරන පුද්ගලයින් ප්‍රථමයෙන්ම යම් අයෙකුගේ සියලුම පෞද්ගලික තොරතුරු රැස්කර ගනී (නම, ලිපිනය, හැඳුනුම්පත් අංකය, දුරකථන අංකය, උපන් දිනය, බැංකු ගිණුම් අංක, පවුලේ අයගේ නම් යනාදී අවශ්‍ය සියලු විස්තර) සමාජ වෙබ් අඩවි, වෙනත් වෙබ් අඩවි සහ පරිගණකගත දත්ත සමුදායන් පිරික්සීම තුලින් මෙම තොරතුරු රැස්කර ගනී. එසේ ලබාගත් තොරතුරු ප්‍රයෝජනයට ගෙන අදාල පුද්ගලයා ලෙස පෙනී සිට විවිධ ගනුදෙනු කර මුදල් නොගෙවා පලා යයි. උදාහරණයක් ලෙස ගෙවීමේ ක්‍රමයට භාණ්ඩ මිලදී ගෙන ගෙවීම් පැහැර හැරීම. එවිට එම වංචාව සඳහා වගකිව යුතු වන්නේ අදාල නම, ලිපිනය යනාදී තොරතුරු හිමි සත්‍ය පුද්ගලයාටයි.

9.1.6 අන්තර්ජාල වෙන්දේසි වංචා

මෙහිදී වංචනික පුද්ගලයා හෝ ආයතනය අන්තර්ජාලය හරහා භාණ්ඩ අලෙවිකරන ආයතනයක් ලෙස පෙනී සිටී. ඔවුන්ගේ වෙබ් අඩවියේ භාණ්ඩ ප්‍රදර්ශනය කෙරෙන අතර ණයපත් (Credit card) මගින් මුදල් ගෙවා භාණ්ඩ ඇනවුම් කළ හැක. ගණුදෙනුකරුවන් මුදල් ගෙවා භාණ්ඩ ඇනවුම් කලත් භාණ්ඩ

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

ගණුදෙනුකරු වෙත නොඑවීම හෝ බාල භාණ්ඩ එවීම සිදු වේ. මෙවැනි වැරදි නීති විරෝධී වුවත් වංචාකරු ඈත රටක පදිංචිකරුවකු හෝ සමහර විට ත්‍රස්තවාදී සංවිධානයක් නිසා ඔවුන් හසුකර ගැනීම ඉතාමත් අපහසුය.

9.1.7 අන්තර්ජාලය හරහා සේවා සපයන්නකු ලෙස පෙනී සිට වංචා කිරීම (Internet offer scams)

අව්‍යාජ ආයතනයක් ලෙස පෙනී සිටිමින් වෙබ් අඩවියක් මගින් හෝ විද්‍යුත් තැපැල් ලිපි මගින් යම් පුද්ගලයිනට ලොතරැයියක ජයග්‍රහනයක් හිමි වී ඇති බව දැනුම් දීමෙන් හෝ ව්‍යාපාරයක කොටස්කරුවකු ලෙස සම්බන්ධ වීමට අවස්ථාවක් ලබාදිය හැකි බව දැනුම්දීමෙන් හෝ ගෙදර සිටිම මුදල් ඉපයිය හැකි ක්‍රමයක් ලබාදෙන බව දැනුම් දීමෙන් හෝ පිරමීඩාකාර ව්‍යාපාරයකට සම්බන්ධකර ගැනීමෙන් හෝ රවටා මුදල් වංචා කිරීම බොහෝ විට සිදු වේ.

9.1.8 ෆිෂින් (Phishing)

මෙහිදී ප්‍රසිද්ධ ආයතනයක් විසින් එවන ලද ආකාරයට එම ආයතනය සමග ගනුදෙනු කරන පුද්ගල කණ්ඩායමකට විද්‍යුත් තැපැල් ලිපියක් එවයි. එම ලිපිය මගින් හදිසි අවශ්‍යතාවයක් සඳහා එම ලිපියෙහි ඇති සබැඳියක් (Link) ක්ලික් කරන ලෙස ඉල්ලා සිටී. ගනුදෙනුකරු එම සබැඳිය ක්ලික් කල හොත් ප්‍රසිද්ධ ආයතනයේ වෙබ් අඩවියට සමාන ව්‍යාජ වෙබ් අඩවියක් වෙත ගනුදෙනුකරු යොමු කෙරෙන අතර එහිදී ඔහුගේ ගිණුමේ යම් ප්‍රශ්නයක් ඇති බවත් එය නිවැරදි කිරීම සඳහා ගිණුම් අංකය සහ රහස් අංකය/මුර පදය ඇතුලත් කරන ලෙසත් ඉල්ලා සිටී. ඒ ආකාරයට ගනුදෙනුකරුගේ ගිණුම් අංකය සහ මුරපදය ලබා ගන්නා පුද්ගලයා ගෙනුදෙනුකරු ලෙස පෙනී සිටිමින් අදාල ආයතනය සමග ගණුදෙනු කරයි. අවසානයේ ව්‍යාජ පුද්ගලයා කරන ගනුදෙනු සඳහා ද මුදල් අඩුවන්නේ ගනුදෙනුකරුගේ ගිණුමෙනි.

9.1.9 ෆාමින් (Pharming)

අප යම් වෙබ් අඩවියකට සම්බන්ධ වීම සඳහා වෙබ් බ්‍රවුසරයට එහි ලිපිනය (domain name) ඇතුලත් කල විට ඊට අදාළ IP ලිපිනය සොයා දෙනු ලබන්නේ ජාලයට සම්බන්ධ DNS සර්වර් නැමති පරිගණකයක් මගිනි. ඩොමේන් ලිපිනයන්වලට අදාල IP ලිපියන් DNA සර්වරයේ දත්ත ගොනුවක ගබඩාකර ඇත. ෆාමින් වලදී සිදුවන්නේ වංචනික පුද්ගලයා DNA සර්වරය හැක් (hack) කර ප්‍රසිද්ධ ආයතනයක IP ලිපිනය වෙනුවට ඔහු හෝ ඇය විසින් නිර්මාණය කරන ලද ව්‍යාජ වෙබ් අඩවියක IP ලිපිනය එයට ඇතුලත් කරයි. එවිට එම ප්‍රසිද්ධ ආයතනයේ ගනුදෙනුකරුවකු එම ආයතනයේ වෙබ් අඩවියට සම්බන්ධවීමට එහි වෙබ් ලිපිනය බ්‍රවුසරයට ඇතුලත් කල විට ගනුදෙනුකරු සම්බන්ධ වන්නේ ව්‍යාජ වෙබ් අඩවියටයි. වංචනික පුද්ගලයා එම වෙබ් අඩවිය නිර්මාණය කරනු ලබනන්නේ ප්‍රසිද්ධ ආයතනයේ වෙබ් අඩවියට සමාන ආකාරයටයි. එහිදී ගනුදෙනුරු එම වෙබ් අඩවියට සම්බන්ධ වීමට පාවිච්චි කරන ගිණුම් අංකය සහ මුරපදය විමසන අතර එය ඇතුලත් කල විට වංචාකරු විසින් එය ලබාගෙන මුරපදය වැරදි යැයි දැක්වෙන පණිවිඩයක් ගනුදෙනුකරුට පෙන්වා ප්‍රසිද්ධ ආයතනයේ නිවැරදි වෙබ් අඩවිය වෙත ගනුදෙනුකරු යොමු කරයි. ගනුදෙනුකරු සිතන්නේ පළමුවර මුරපදය ඇතුලත් කිරීමේදී යම් වරදක් වූ බවයි. මේ ආකාරයට වංචාකරු විසින් ලබා ගන්නා ගිණුම් අංකය සහ මුරපදය භාවිත කර අදාල ආයතනය සමඟ ගනුදෙනු කරයි.

9.1.10 ඔත්තුබැලීමේ මෘදුකාංග (Spyware)

මෙම මෘදුකාංග පරිගණකයක් භාවිතා කරන්නාගේ අනුදැනුමකින් තොරව පරිගණකයකට ස්ථාපිත වී එය භාවිතා කරන්නා පිළිබඳ තොරතුරු රහසිගතව රැස්කර අන්තර්ජාල සම්බන්ධතාවය හරහා එම තොරතුරු වෙනත් පරිගණකයකට යවයි. සමහර විට මෙම තොරතුරු වෙළඳ දැන්වීම් බෙදා හැරීම වැනි එතරම් හානිකර නොවූ කාර්යයන් සඳහා භාවිතා කරන අතර තවත් සමහර විට බැංකු ගිනුම් අංක ඒවායේ රහස් අංක සොරා ගැනීම වැනි වඩාත් හානිකර කාර්යයන් සඳහා භාවිතා කරයි.

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

9.2 පරිගණක සහ දත්තවල ආරක්ෂාව සඳහා භාවිත කල හැකි විශේෂ ක්‍රම

අනවසරයෙන් පරිගණක සහ පරිගණක ජාලවලට සම්බන්ධ වීමට ඇති ඉඩකඩ අවහිර කිරීම එක් ආරක්ෂණ ක්‍රියා මාර්ගයකි. මෙහිදී පරිගණකයකට පිවිසීමට ඇති හැකියාව පාලනය කිරීම, පරිගණකයක් භාවිතාකරන්නකුට කල හැකි කාර්යයන් සීමා කිරීම, පරිශීලකයකුට භාවිතා කළ හැකි දත්ත මොනවාද යන්න සීමා කිරීම, මෙහෙයුම් පද්ධතියේ (Operating system) ඇති ආරක්ෂණ ක්‍රියාමාර්ග ක්‍රියාත්මක කිරීම, (Firewalls, antivirus, anti spyware) වැනි ක්‍රම භාවිත කරයි. මෙම ක්‍රම මගින් බලාපොරොත්තු වන්නේ අවසර ලත් පුද්ගලයිනට පමණක් පරිගණක ජාල සහ දත්ත ගබඩා වෙත යොමු වීමට ඉඩ ලබාදීමයි. මෙවැනි ක්‍රම කිහිපයක් පහත සාකච්ඡා කෙරේ.

9.2.1 රහස් පද භාවිතයෙන් ප්‍රවේශ වීමේ ක්‍රම

මෙහිදී පරිගණක පද්ධතියට සම්බන්ධ වීමට හෝ දත්ත සමුදාය වෙත ප්‍රවේශ වීමට අවශ්‍ය පුද්ගලයා ඒ සඳහා අවශ්‍ය පරිශීලක නම (user name), මුර පදය (Password), හෝ රහස් අංකය (PIN Number) වැනි තොරතුරු ලබාදිය යුතුයි. එම තොරතුරු අවසර ලත් පුද්ගලයින් සතුව පමණක් පවතින බැවින් අවසර නොලත් පුද්ගලයිනට සම්බන්ධ විය නොහැක. පරිගණක පද්ධතිවලට, දත්ත සමුදායන්ට සම්බන්ධවීමේදීත්, විද්‍යුත් තැපැල් ගිණුම්වලට සම්බන්ධවීමේදීත් අවසරලත් පුද්ගලයා හඳුනා ගැනීම සඳහා මුර පද භාවිතා කරයි. ටෙලර් යන්ත්‍රවලට සම්බන්ධ වීමේදී රහස් අංක භාවිතා කරයි.
මුරපද භාවිතා කිරීමේදී ඇති ප්‍රධාන ගැටලුවන්නේ ඒවා අමතක වීමට ඇති ඉඩකඩ වැඩිවීම සහ හැකර් කෙනෙක් එය අනුමානකර පද්ධතියට සම්බන්ධ වීමට ඇති හැකියාවයි.

ශක්තිමත් (ආරක්ෂාකාරී) මුර පදයක් පවත්වා ගැනීම සඳහා උපදෙස්

- කැපිටල්, සිම්පල් අකුරු ඉලක්කම් සහ අනෙකුත් සංකේත මිශ්‍රකර අකුරු අටකට වඩා දිග මුර පදයක් භාවිතා කරන්න.
- මුර පදය සඳහා ඔබේ හෝ ඔබට සමීප පුද්ගලයෙකුගේ නමක් හෝ වෙනත් අයට අනුමාන කළ හැකි වචනයක් හෝ සාමාන්‍ය වචනයක් භාවිතා නොකරන්න. ඔබට මතක තබා ගැනීමට පහසු අනෙක් අයට අනුමාන කිරීමට අපහසු පද, සංඛ්‍යා සහ සංකේත මිශ්‍රනයක් මුර පදය සඳහා භාවිතා කරන්න.
- කිසිම විටක පරිගණකයට ආසන්නයේ හෝ අනෙක් අයට ප්‍රවේශ වීමට හැකි ස්ථානයක මුර පදය ලියා නොතබන්න.
- අන්තර්ජාලය තුල සමාජ වෙබ් අඩවි, විද්‍යුත් තැපැල් ගිණුම් සහ වෙනත් එවැනි කටයුතු සඳහා භාවිතා කරන මුරපද ණය පත් මගින් මුදල් ගෙවීම්, බැංකු කටයුතු හෝ දැඩි ආරක්ෂාවක් අවශ්‍ය වන වෙනත් ස්ථානවලදී භාවිතා නොකරන්න.
- මුර පදය නිතර වෙනස් කරන්න.
- මුර පදය පරිගණකයකට ඇතුලත් කිරීමේදී ඔබ එය ඇතුලත් කරනුයේ ව්‍යාජ ලෙස නිර්මාණය කරන ලද මෘදුකාංගයකටද යන්න සහ ඔබ අවට කිසිවකු සිටී දැයි සැලකිලිමත් වන්න.

9.2.2 පරිගණක පද්ධතියට සම්බන්ධ වීම සඳහා කාඩ්පතක් වැනි යමක් භාවිතා කිරීම

මෙහිදී පරිගණක පද්ධතියට සම්බන්ධ වීම සඳහා කාඩ්පතක් (smart card or magnetic card) ටෝකන් එකක් (token), ප්ලැෂ් ධාවකයක් (USB Flash drive), බැජ් එකක් (RFID-encoded badges) වැනි දෙයක් පරිගණකයට සම්බන්ධ කළ යුතුයි. (කාඩ් කියවයක් මගින් කාඩ්පත කියවීම, USB ධාවකය පරිගණකයට සම්බන්ධ කිරීම යනාදී ලෙස) මුරපද භාවිතා කිරීම හා සැසඳීමේදී මෙහි ඇති වාසිය වන්නේ මුරපදය අමතක වීමේ ගැටලුවට විසඳුමක් ලැබීම සහ බාහිර පුද්ගලයකුට අදාල අංගය නොමැතිව අන්තර්ජාලය මගින් හෝ පරිගණක ජාලයක් හරහා පරිගණක පද්ධතියට සම්බන්ධ වීමට නොහැකිවීමයි. නමුත් මෙහි ඇති ප්‍රධාන අවාසිය වන්නේ මෙම උපකරණය නැතිවීමට ඇති හැකියාව සහ එය සොරාගත් පුද්ගලයකුට පරිගණකයට සම්බන්ධවීමට ඇති හැකියාවයි. මෙම දුර්වලතා

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

මගහැරීම සඳහා මෙවැනි උපකරණාක් සමග මුර පදයක් ද භාවිතා කිරීම බොහෝ විට සිදු වේ. උදාහරණ වශයෙන් බැංකු ටෙලර් යන්ත්‍ර භාවිතයේ දී කාඩ්පත සහ රහස් අංකය යන දෙකම භාවිතා කිරීමට සිදුවීම. මෙහිදී කාඩ්පත සොරා ගැනීමෙන් පමණක් හෝ මුර පදය අනුමාන කිරීමෙන් පමණක් පරිගණක පද්ධතියට සම්බන්ධ විය නොහැක.

9.2.3 විශේෂ ශරීර ලක්ෂණ මගින් පුද්ගලයන් හඳුනාගෙන පරිගණක පද්ධතියට සම්බන්ධවීමට අවසර ලබාදීම (Biometric Access systems)

මෙහිදී ඇඟිලි සලකුණු හඳුනාගැනීම (finger print), අතේ රේඛා හඳුනා ගැනීම (Palm geometry), මුහුණ හඳුනා ගැනීම, (Face recongition) ඇසේ කළු ඉංගිරියාව අනුව හඳුනා ගැනීම (Iris of an eye) වැනි ක්‍රම මගින් පුද්ගලයන් හඳුනාගෙන අවසරලත් පුද්ගලයිනට පමණක් පරිගණක පද්ධතියට ඇතුල්වීමට අවසර ලබාදෙයි. මෙවැනි ක්‍රමයක් ක්‍රියාකරන ආකාරය තේරුම් ගැනීමට උදාහරණයක් වශයෙන් ඇඟිලි සලකුණු අනුව පුද්ගලයන් හඳුනා ගැනීමේ පද්ධතියක් සැලකිල්ලට ගනිමු. මෙහිදී ප්‍රථමයෙන් පරිගණක පද්ධතිය භාවිතා කිරීමට අවසරලත් පුද්ගලයින්ගේ ඇඟිලි සලකුණු පරිගණක පද්ධතියේ ගබඩා කරයි. පසුව ඔවුන් පරිගණක පද්ධතියට සම්බන්ධ වීමට උත්සාහ කරන අවස්ථාවේදී ඔවුන්ගේ ඇඟිලි සලකුණු කියවා ඒවා පරිගණක පද්ධතියේ ගබඩා කර ඇති ඇඟිලි සලකුණු සමඟ සසඳා බලයි. ඒවා ගැලපේ නම් පමණක් ඔවුනට පරිගණක පද්ධතිය භාවිතා කිරීමට ඉඩ ලාබ දෙයි. මෙම ක්‍රමයේ ඇති ප්‍රධානම වාසිය වන්නේ කාඩ් පතක් හෝ මුර පදයක් වැනි දෙයක් වෙනත් කෙනෙකුට සොරකම් කල හැකි වූවත් කෙනෙකුගේ ශරීර ලක්ෂණයක් කිසිවිටකත් වෙනත් අයෙකුට සොරකම් කල නොහැකි වීමයි. එබැවින් පරිගණක පද්ධතිවල දී පුද්ගලයින් හඳුනා ගැනීම සඳහා මෙම ක්‍රම භාවිතය දිනෙන් දින වර්ධනය වෙමින් පවතී. මෙහි ඇති ප්‍රධාන අවාසිය වන්නේ අදාල සලකුනු හඳුනා ගැනීම සඳහා භාවිතා වන උපකරණ සහ මෘදුකාංග සඳහා වැඩි වියදමක් දැරීමට සිදුවීමයි. නමුත් වැඩි ආරක්ෂාවක් අවශ්‍ය වන බැංකු ගනුදෙනු වැනි මූල්‍යමය ගනුදෙනුවලදී පුද්ගලයින් හඳුනා ගැනීම සඳහා මෙවැනි ක්‍රම භාවිතා කිරීම ඉතා වැදගත් වේ.

9.2.4 රැහැන් රහිත පරිගණක ජාලවලට අනවසරයෙන් සම්බන්ධවීම පාලනය කිරීම (Controling access to wireless netwroks)

යම් ආයතනයක හෝ නිවසක රැහැන් රහිත පරිගණක ජාලයක් ඇත්නම් එහිදී ජාලය භාවිතා කරන පුද්ගලයින් ජාලයට සම්බන්ධ වන්නේ රැහැනක් මගින් ප්‍රධාන පරිගණකයට සම්බන්ද කර ඇති රවුටර් (router or access point) නැමති උපකරණයට රැහැන් රහිතව තම පරිගණකය සම්බන්ධකර ගැනීමෙනි. රවුටරයකට සම්බන්ධ වන පරිගණක සහ පුද්ගලයින් හඳුනා ගැනීම සහ පාලනය කිරීම සඳහා පහසුකම් රාශියක් වර්තමානයේ භාවිතා වන රවුටර්වල ඇත. ඒවා අවශ්‍ය ආකාරයට සකසා ගැනීමෙන් අදාල රවුටර්ය හරහා පරිගණක ජාලයට රැහැන් රහිතව සම්බන්ධ වන පරිශීලකයන් පාලනය කළ හැක. එසේ භාවිතා කල හැකි ආරක්ෂක ක්‍රම සමහරක් පහත දැක්වේ.

- ජාලයට සම්බන්ධ වීම සඳහා මුර පදයක් හඳුන්වා දීම.
- රැහැන් රහිත ජාලයෙහි නම (SSID) එයට සම්බන්ධවන අයට නොපෙනෙන ලෙස සැගවීම.
- රවුටරයේ අදාල සැකසීම් කිසිවකුටත් වෙනස් කිරීමට නොහැකිවීම පිණිස එයට පාලක මුරපදයක් (Administrator Password) දැමීම.
- ජාලයට සම්බන්ධ වීමට අවසර ඇති පරිගණකවල ජාල ඇඩැප්ටර ලිපිනයන් (MAC Address) සියල්ලම රවුටරයට ඇතුලත් කිරීම. එවිට වෙනත් පරිගණකයකට අදාල රවුටරයට සම්බන්ධ විය නොහැක.
- ජාලයට සම්බන්ධ විය හැකි වේලාවන් නියම කිරීම. උදාහරණයක් වශයෙන් කාර්යාලයක ඇති රැහැන් රහිත ජාලයක් නම් කාර්යාල වේලාව තුලදී පමණක් ජාලයට සම්බන්ධ විය හැකි බව දැක්වීම.
- රැහැන් රහිත සංඥා රවුටරයේ සිට ගමන් කරන දුර සීමා කිරීම.

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

9.2.5 ෆයර්වෝල් (Fire Walls)

පරිගණකයක් හෝ පරිගණක ජාලයක් සහ අන්තර්ජාලය අතර ආරක්ෂිත පවුරක් ඇතිකරන ආරක්ෂිත ක්‍රමයක් ෆයර්වෝල් නමින් හැඳින් වේ. පරිගණකයේ සිට අන්තර්ජාලය වෙතට ගමන් කරන සහ අන්තර්ජාලයේ සිට පරිගණකය වෙත ගමන් කරන දත්ත, පණිවිඩ, සංඥා යනාදිය පරීක්ෂා කර බැලීම ෆයර්වෝල්වල කාර්යභාරයයි. එසේ පරීක්ෂාකර බැලීමේදී අවසරලත් දත්තවලට පමණක් ගමන් කිරීමට ඉඩ ලබාදෙයි. පෞද්ගලික පරිගණක සමඟ භාවිතාවන ෆයර්වෝල් මෘදුකාංග වන අතර පරිගණක ජාලවල දී දෘඩාංග ෆයර්වෝල් සහ දෘඩාංග, මෘදුකාංග මිශ්‍ර ෆයර්වෝල් භාවිතා වේ. උදාහරණයක් වහයෙන් ඔබගේ පරිගණකයේ ඇති දත්තවලට හැකර් කෙනෙකුගෙන් ඇතිවිය හැකි යම් අනතුරක් පාලනය කර ගැනීම සඳහා මයික්‍රොසොෆ්ට් වින්ඩෝස්වල ඇති ෆයර්වෝල් එක අවශ්‍ය පරිදි සකස් කර ගැනීමට පුළුවන.

9.2.6 ගුප්ත කේතනය (Encription)

පරිගණක අතර දත්ත හුවමාරු කිරීමේදී ඒවා කියවා තේරුම් ගැනීමට නොහැකි විශේෂ සංඛේත ක්‍රමයකට හැරවීම මෙහිදී සිදු වේ. දත්ත හුවමාරුව අතරතුරදී යම් අනවසර පුද්ගලයෙක් ඒවා ලබාගතහොත් ඔහුට හෝ ඇයට ඒවා කියවා තේරුම් ගත නොහැක. මෙසේ දත්ත විශේෂ කේතවලට හරවන අවස්ථා රාශියක් ඇත.

- බැංකු සහ වෙනත් එවැනි මූල්‍ය ගනුදෙනු මාර්ගගතව සිදු කරන වෙඩ් අඩවි ගනුදෙනුකරුවන්ගේ ගිණුම් අංක, රහස් අංක අන්තර්ජාලය හරහා ලබා ගැනීමේදී ඒවා ගුප්ත කේතවල පරිවර්තනය කරයි.
- විද්‍යුත් තැපැල් පණිවිඩ සහ ඒවායේ ඇමුණුම් ගුප්ත කේතකරණය කළ හැක.
- අන්තර්ජාලය හරහා හුවමාරු වන දුරකතන ඇමතුම් සහ වෙනත් පණිවිඩ මෙසේ කේත කල හැක.

  ගුප්ත කේතකරනයේ ප්‍රධාන වර්ග දෙකක් ඇත. එනම් පෞද්ගලික යතුරු ක්‍රමය (Private key encription) සහ පොදු යතුරු ක්‍රමය (Public key encription)

පෞද්ගලික යතුරු ක්‍රමය (Private Key Encription)

මෙහිදී දත්ත ගුප්ත සංකේතකරණය සඳහාත් එම සංඛේතකරණය කළ දත්ත නැවත තේරුම්ගත හැකි ක්‍රමයට හරවා ගැනීම සඳහාත් එක් මුර පදයක් (Private key) පමණක් භාවිතා වේ. පරිගණකයක ගබඩාකරණ දත්ත ගුප්ත සංකේතකණය සඳහා මෙම ක්‍රමය භාවිතා කළ හැක. මෙහිදී දත්ත ගුප්ත සංකේතකරණය කරනුයේත් ඒවා නැවත සාමාන්‍ය ක්‍රමයට හරවනුයේත් එකම පුද්ගලයකු විසින් බැවින් එක් මුරපදයක් භාවිතා කිරීම ගැටලු සහගත නොවේ. එසේම එක් පරිගණකයක සිට වෙනත් පරිගණකයකට හෝ පරිගණක කිපයකට දත්ත යැවීමේදි පෞද්ගලික යතුරු ක්‍රමය භාවිතා කළ හැකි වන්නේ දත්ත භාවිතාකරන අවසරලත් සියලු දෙනා පෞද්ගලික මුරපදය දන්නේ නම් සහ ඔවුන් ඒ සඳහා එකඟවන්නේ නම් පමණි.

පොදු යතුරු ක්‍රමය (Public Key Encription)

මෙහිදී දත්ත ගුප්ත සංකේතකරණය සඳහා එක් මුර පදයක් ද (Public key) ගුප්ත සංකේතවලට හරවන ලද දත්ත නැවත සාමාන්‍ය තත්වයට පත් කිරීම සඳහා තවත් මුරපදයක් ද (Private key) භාවිතා කරයි. මෙම පෞද්ගලික යතුර සහ පොදු යතුර අතර කිසිවකුටත් අනුමාන කල නොහැකි ගණිතමය සම්බන්ධතාවයක් ඇති අතර පොදු යතුර මගින් ගුප්ත ක්‍රමයට හරවන ලද දත්ත පෞද්ගලික යතුර මගින් නැවත සාමාන්‍ය ක්‍රමයට හැරවිය හැක. මෙම මුරපද නිපදවීම සඳහා විශේෂ මෘදුකාංග ඇත. මෙම ක්‍රමය භාවිතා කිරීමේදී යම් පුද්ගලයකු හෝ ආයතනයක පෞද්ගලික යතුර තමන් රහසිගතව තබාගෙන පොදු යතුර ප්‍රසිද්ධ කරයි. එම පුද්ගලයා හෝ ආයතනය වෙත දත්ත හෝ පණිවිඩ එවනු ලබන තැනැත්තන් පොදු යතුර මගින් එය ගුප්ත සංකේතවලට හරවා එවිය යුතුයි. එවිට එම පණිවිඩය ලබන පුද්ගලයා හෝ ආයතනය පෞද්ගලික යතුර යොදාගෙන එම දත්ත හෝ පණිවිඩ තේරුම් ගතහැකි

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

සාමාන්‍ය තත්ත්වයට පත්කර ගනී. පෞද්ගලික යතුර වෙනත් කිසිම පුද්ගලයකු ලඟ නොමැති බැවින් එම දත්ත හෝ පණිවිඩ කිසිවකුටත් කියවා තේරුම් ගත නොහැක.

9.2.7 ප්‍රතිවෛරස මෘදුකාංග (Antivirus Software) සහ ආරක්ෂාව සපයන වෙනත් මෘදුකාංග

පරිගණක වෛරස සහ අනෙකුත් එවැනි හානිකර මෘදුකාංගවලින් ආරක්ෂාවීම සඳහා අන්තර්ජාලයට හෝ වෙනත් පරිගණක ජාලවලට සම්බන්ධ වන සියලුම පරිගණක, ස්මාට් දුරකතන සහ අනෙකුත් එවැනි උපකරණ සඳහා ප්‍රති වෛරස මෘදුකාංගයක් ස්ථාපිත කළ යුතුයි. පරිගණකයක ආරක්ෂාව සඳහා ප්‍රතිවෛරස මෘදුකාංග කරනු ලබන කාර්යයන්:

- පරිගණකය ක්‍රියාත්මක කල අවස්ථාවේ සිට වසා දමන අවස්ථාව දක්වා පරිගණකයේ ප්‍රධාන මතකයේ රැඳී සිටිමින් පරිගණකයේ සිදුවන සියලු කටයුතු පිළිබඳ සුපරීක්ෂාකාරී වේ. සැකකටයුතු මෘදුකාංගයක් හෝ වෙනත් විශේෂ හැසිරීමක් නිරීක්ෂණය වූ වහාම ඒ පිළිබඳව පරිශීලකයාට දැනුම් දෙයි.
- පරිගණකය වෙත පැමිණෙන විද්‍යුත් තැපැල් පණිවිඩ සහ වෙනත් පණිවිඩ පරීක්ෂාකර බලයි.
- පරිශීලකයාට අවශ්‍ය ඕනෑම අවස්ථාවක පරිගණකයේ ඇති ගබඩා මාධ්‍ය ස්කෑන් කර ඒවායේ පරිගණක වෛරස සහ වෙනත් හානිකර මෘදුකාංග තිබේ දැයි සොයා බැලීම. (යම් දෙනලද වේලාවකදී පරිගණකය ඉබේම ස්කැන්වන ලෙසට සකස් කළ හැක.)
- USB කවුලුවකට සම්බන්ධ කරන ඕනෑම උපකරණයක් ඉබේම ස්කෑන් වන ලෙස ද නියම කළ හැක.
- අන්තර්ජාලයට සම්බන්ධවීමේදී සහ අන්තර්ජාලයෙන් ගොනු බාගත කිරීමේදී ඒවායේ වෛරස සහ අනිකුත් අනිශ්ඨ මෘදුකාංග තිබේදැයි පරීක්ෂාකර බැලීම.

වර්තමාන ප්‍රතිවෛරස මෘදුකාංග වෛරස සහ අනිශ්ඨ මෘදුකාංග පරීක්ෂා කිරීමට අමතරව ඔත්තු බැලීමේ මෘදුකාංග, ෆිෂින් ප්‍රහාර යනාදිය ද පරීක්ෂා කර බලයි.

9.3 පෞද්ගලික ආරක්ෂාව

අන්තර්ජාලය භාවිතා කිරීමේදී අපගේ පෞද්ගලික ආරක්ෂාව පිළිබඳව ද සැලකිලිමත් වීම ඉතා වැදගත් වේ. විශේෂයෙන් සමාජ වෙබ් අඩවිවලදී (Social networks) සහ කතාබස් වෙබ් අඩවිවලදී (chat rooms) අපට හමුවන නොහඳුනන පුද්ගලයන් හෝ සමහර විට හඳුනන පුද්ගලයන්ගෙන් පවා විවිධාකාර ප්‍රශ්න ඇති විය හැක. මෙවැනි ඇතැම් පුද්ගලයින් අප අපහසුතාවයට පත්වන ප්‍රකාශ සිදු කිරීමට හෝ ඡායාරූප පෙන්වීමට ඉඩ තිබේ. සමහර විට ව්‍යාජ නම් වලින් ඉතා වැදගත් සමාජ තත්ත්වයක් ඇති පුද්ගලයකු ලෙස පෙනී සිට අප සමඟ කිට්ටු සම්බන්ධතාවයක් ඇති කර ගැනීමට උත්සාහ කරයි. අප තුල ඔහු හෝ ඇය පිළිබඳව විශ්වාසයක් ගොඩනඟාගෙන අපගේ පෞද්ගලික තොරතුරු ලබාගනී. පසුව එසේ ලබාගත් තොරතුරු ප්‍රසිද්ධ කරන බවට තර්ජනය කරමින් මුදල් ඉල්ලා සිටිය හැක. අන්තර්ජාලය හරහා කෙටි කලකින් මිතුරන් බවට පත්වන නොහඳුනන පුද්ගලයන් ළමයින් සහ තරුණ තරුණියන් නොමඟ යැවූ අවස්ථා නිතර අසන්නට ලැබේ. අන්තර්ජාලය හරහා ළමයින් මිතුරන් බවට පත්කර ගන්නා මෙවැනි ඇතැම් පුද්ගලයින් එම ළමයින් පෞද්ගලිකව හමුවී විවිධ අපයෝජන සඳහා යොදා ගනී.

එබැවින් සමාජ වෙබ් අඩවි, කතාබස් වෙබ් අඩවි වැනි වෙබ් ඩවි වලට සම්බන්ධවන පුද්ගලයින් හැකි පමණ තමන්ගේ පෞද්ගලික තොරතුරු අනාවරණය කිරීමෙන් වැලකී සිටිය යුතුයි. මෙවැනි වෙබ් අඩවිවල ගිණුම් සැදීමේදී තමන්ගේ සත්‍ය නම හෝ ඡායාරූපය භාවිතා නොකල යුතුයි. එවැනි වෙබ් අඩවි හරහා හඳුනාගන්නා පුද්ගලයින් පිළිබඳව විශ්වාසය තබා ඔවුන් පෞද්ගලිකව මුණගැසීම හෝ ඔවුන් කියනු ලබන සැක කටයුතු දේ කිරීමෙන් වැලකිය යුතුයි.

තවද අසභ්‍ය ඡායාරූප සහ වීඩියෝ දර්ශන විශාල වශයෙන් අන්තර්ජාලයේ පවතින බැවින් ළමයින් මේවායෙන් ආරක්ෂාකර ගැනීමට දෙමාපියන් විශේෂයෙන් සැලකිලිමත් විය යුතුයි. ඔවුන්ගේ අධ්‍යාපන

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura

කටයුතු සඳහා අන්තර්ජාලය භාවිතා කිරීමට අවශ්‍ය වන අවස්ථාවල දී දෙමාපියන්ගේ අධීක්ෂණය යටතේ පමණක් අන්තර්ජාලය භාවිතා කිරීමට ඉඩලබාදි යුතුයි. අන්තර්ජාලය භාවිතා කිරීමෙන් ලබාගත හැකි ඵල ප්‍රයෝජන මෙන්ම එහි ඇති අවදානම පිළිබඳවත් ඔවුන් දැනුවත් කළ යුතුයි. යම් අවස්ථාවක අන්තර්ජාලය හරහා යමකු තමන් අපහසුතාවයට ලක් කිරීමට හෝ රැවටීමට උත්සාහකරන බව පෙනී ගියහොත් ඒ පිළිබඳව තම දෙමාපියන් හෝ පාසැලේදී නම් ගුරුවරුන් දැනුවත් කර එම පුද්ගලයා පිළිබඳව රටේ ආරක්ෂක අංශ දැනුවත් කිරීමට කටයුතු කළ යුතුයි.

Prepared by ID Jayaruwan,
Senior Lecturer,
University of Sri Jayewardanepura