MODULE 3

ඩිජිටල් ආරක්ෂාව තර කිරීම

ප්‍රකාශනය

පළමු ප්‍රකාශනය 2020 මාර්තු

ප්‍රකාශනය :
ශ්‍රී ලංකාජාතික ක්‍රිස්තියානි එවැන්ජලික සන්ධානය**(NCEASL)**

වෙබ් අඩවියථ **www.minormatters.org**

සංස්කාරකථ නාලක ගුණවර්ධන

ව්‍යාපෘති සම්බන්ධීකරණය:

යමිනිරවින්ද්‍රන්,අධ්‍යක්ෂ -නීති සහ උපදේශන ෂලෝමි ඩැනියෙල්, නීති සහ උපදේශනසම්බන්ධීකාරක, ආගමික නිදහස සහ සමාජ සාධාරණ කොමිෂන් සභාඅක්ෂිණපළිහවඩන, මාධ්‍ය මූලෝපාය නිලධාරී, ආගමික නිදහස සහ සමාජ සාධාරණ කොමිෂන් සභා

පිට කවර නිර්මාණය: සංජයන් අරියදුරෙ

පිටු පිරිසැලසුම සහ නිර්මාණය: ෂෙනල් ජෙසුඩියන්

වියාචනය:

මෙම ප්‍රකාශනයේ අන්තර්ගත විශ්ලේෂණයන් අදහස් දායකයින්ගේ සහ සංස්කාරකවරුන්ගේ අදහස් වේ. ඔවුන් ශ්‍රී ලංකාවේ ජාතික ක්‍රිස්තියානි එවැන්ජලික සන්ධානයේ සාමාජිකයන් නොවන අතර සංවිධානය නියෝජනය නොකරයි.

ඩිජිටල් ආරක්ෂාව තර කිරීම

අන්තර්ජාලය යනු තොරතුරු හුවමාරු කරගත හැකි පරිදි විද්‍යුත් වශයෙන් එකිනෙක හ සම්බන්ධ වී ඇති ගෝලීය පරිගණක ජාලයකි.

අන්තර්ජාලය, භෞතික ලෝකයේදී තැපැල් පද්ධතියක ක්‍රියාත්මක වීම හා සමාන ය. එහෙත්, එය පණිවුඩ බෙදාහරින්නේ ආලෝකයේ වේගයෙනි. එසේ ම එය අති සියුම් ය. තැපැල් සේවයකදී ජනතාවට එකිනෙකා වෙත ලියුම් කවරවල දැමූ පණිවුඩ යැවීම කරනු ලැබේ. අන්තර්ජාලයේදී එය සිදු වන්නේ පරිගණකයෙන් පරිගණකයට කුඩා ඩිජිටල් දත්ත පැකට් යැවීමෙනි.

ගෝලීය අන්තර්ජාලය සමග එකිනෙකට වෙනස් උපාංග බිලියන් ගණනක් සම්බන්ධ වී තිබේ. ඒ අතර සුපිරි පරිගණක, ඩෙස්ක්ටොප්, ලැප්ටොප්, ටැබ්ලට් වැනි පෞද්ගලික පරිගණක සහ දහස් ගණනක් නිෂ්පාදකයන් විසින් නිපදවනු ලබන විශේෂ උපාංග තිබේ.

මෙම එකිනෙකට වෙනස් උපාංග අතර දත්ත හුවමාරු කිරීම පිණිස, ඒ සැම විසින් (TCP/IP - Transmission Control ප්‍රොටොකෝල/Internet ප්‍රොටොකෝල) යන තාක්ෂණික ප්‍රමිතිය භාවිතා කරනු ලැබේ. එයට සම්බන්ධ වන සෑම උපකරණයකට ම අන්තර්ජාලයේ ප්‍රොටොකෝලයක් හෙවත් ලිපිනයක් තිබේ.

ඔබ ලිපියක් තැපැල් කරන විට, තැපැල් පද්ධතිය විසින් සියලු සංවිධාන කටයුතු හසුරුවනු ලැබේ. ඔබට එම ලිපි එකතු කරගන්නා ආකාරය, තෝරන ආකාරය, ප්‍රවාහනය කරන ආකාරය සහ අවසානයේදී බෙදාදෙන ආකාරය ගැන සිතීමේ අවශ්‍යතාවක් නැත. ඒ හා සමානව ම අන්තර්ජාල දත්ත පැකට් ද විවිධ රැහැන්, රවුටර (routers) සහ හොස්ට් පරිගණක (host computers) හරහා සම්ප්‍රේෂණය වී ගමනාන්තයට ළඟා වේ.

2018 අවසානය වන විට, බිලියන 3.9ක් ජනතාව අන්තර්ජාලය පරිහරණය කළ අතර, රජය, සමාගම්, පුණ්‍යායතන සහ වෙනත් සංවිධාන වැනි කෝටි ගණන් ආයතන ද ඒ අතර විය. ඒ අතරින් වැඩි දෙනෙක්ගේ වෙබ් පරිහරණය කිරීමේ අත්දැකීම ආරක්ෂිත සහ තෘප්තිමත් විය. එහෙත් බොහෝ සංඛ්‍යාවක් පරිශීලකයන් සිටින විට සහ බොහෝ උපාංග අන්තර්ජාලයට සම්බන්ධ වී ඇති විට වැරදි සිදු විය හැකි ය. ඩිජිටල් ආරක්ෂාව හෝ සයිබර් ආරක්ෂාව එහිදී වැදගත් ය.

සයිබර් ආරක්ෂාව පද්ධති හා ද්‍රව්‍ය සම්බන්ධ දෙයක් වන අතර සයිබර් සුරක්ෂිතබව මිනිසුන් සම්බන්ධ කාරණාවකි. මෙම මොඩියුලයේදී අප ආවරණය කරන්නේ ඩිජිටල් ආරක්ෂාව පිළිබඳ මූලධර්මයි. (ඔබගේ ඩිජිටල් පද්ධති හා උපකරණ ආරක්ෂා කරගැනීම). ඊළඟ මොඩියුලය සයිබර් සුරක්ෂිතබව පිළිබඳ වන අතර එමගින් ඩිජිටල් සේවා භාවිතා කිරීමේදී පුද්ගලයන් ආරක්ෂා කරගැනීම පිළිබඳ සාකච්ඡා කරනු ඇත.

ප්‍රධාන යෙදුම්

ඩිජිටල් ආරක්ෂාව (මෙයට තොරතුරු තාක්ෂණ ආරක්ෂාව යයි ද කියනු ලැබේ.): යනු, ඩිජිටල් වශයෙන් ගබඩා කර තිබෙන තොරතුරු ආරක්ෂා කිරීමට හා රැකවරණයට ක්‍රම ක්‍රියාත්මක කිරීමයි. මෙම උපාංග අන්තර්ජාලයට සම්බන්ධ වී හෝ සම්බන්ධ නොවී තිබිය හැකි ය. පරිගණක සංදර්භයකදී, ආරක්ෂාව යනු භෞතික මෙන් ම සයිබර් ආරක්ෂාව ද වේ.

සයිබර් ආරක්ෂාව: අන්තර්ජාලයට සම්බන්ධ ඩිජිටල් උපාංග ආරක්ෂා කරගැනීම සඳහා ගනු ලබන පූර්ව ආරක්ෂක පියවර සයිබර් ආරක්ෂාවයි. විශේෂයෙන් ම පරිගණක පද්ධති සහ දත්ත වෙත අනවසර ප්‍රවේශය හෝ ප්‍රහාර වියට අයත් වේ.

ක්ලවුඩ් පරිගණක යන්නෙන් අදහස් වන්නේ දත්ත හා වැඩසටහන් ගබඩා කිරීම සහ ඒවා වෙත පිවිසීම පරිගණක දෘඪ තැටියක් මගින් කරනු වෙනුවට අන්තර්ජාලය හරහා කිරීමයි. මෙහිදී ක්ලවුඩ් යනු අන්තර්ජාලය සඳහා යෙදෙන රූපකයක් පමණි.

ඩිජිටල් සහ සයිබර් ආරක්ෂාව පිළිබඳ මූලධර්ම

අප ඕනෑම ඩිජිටල් පද්ධතියක් භාවිතා කරන විට අප එයට දත්ත ඇතුළත් කරන්නෙමු. ඒවා අතරට පෞද්ගලික දත්ත, අප වැඩ කරන සංවිධානවල රහස්‍ය නිල දත්ත, නිර්මාණාත්මක අන්තර්ගතයන් සහ වෙනත් වර්ගවල දත්ත තිබේ. අප පරිගණක පද්ධතියකට සම්බන්ධ වන විට, සංවිධානයක් තුළ වුවත්, ගෝලීය අන්තර්ජාලයේ වුවත්, අපට වෙනත් පුද්ගලයන්ගේ දත්ත හමුවේ.

අපගේ දත්ත හා උපකරණ ආරක්ෂා කරගත යුතු අතර ඒ අතර ම වෙනත් අයගේ දත්ත හා උපකරණවල ආරක්ෂාව පිළිබඳව ද සැලකිලිමත් විය යුතු ය. අන්තර්ජාලය වැනි එකිනෙක සම්බන්ධ ජාලයකදී, සෑම කෙනෙකුට ම ආරක්ෂාව පිළිබඳ අවධානය යොමු කිරීමට සිදු වේ. මීට හේතුව වන්නේ පරිශීලකයන්ගේ දුර්වලකම් නිසා සෑම කෙනෙකුට ම හානි සිදු විය හැකි බැවිනි.

ඩිජිටල් සහ සයිබර් ආරක්ෂාව යනු හුදෙක් අවසර රහිත ප්‍රවේශයෙන් ආරක්ෂා වීම පමණක් නොවේ. හදිසි අනතුරු මගින් දත්තවලට හානි වීම පිළිබඳ සහ අවසර සහිත අප අතින් හෝ දත්ත හසුරුවන වෙනත් අයකු අතින් දත්තවලට හානි සිදුවීම පිළිබඳව ද අප පරිස්සම් සහගත විය යුතු ය. ගංවතුර, ගිනි සහ විදුලි සැර වැනි හේතු මත ද දත්තවලට හානි සිදු වේ.

ඩිජිටල් සහ සයිබර් ආරක්ෂාව යනු අධි සංකීර්ණ ආරක්ෂණ පද්ධති පිහිටුවාගැනීම නොවේ. ඇතැම් විට, හොඳම විසඳුම ඉතා තාක්ෂණික එකක් නොවන්නට ඉඩ තිබේ. විශේෂයෙන් ම අන්තර්ජාලයේදී, අලුත් තර්ජන මතු වන විට, ආරක්ෂක භාවිතාවන් නැවත තක්සේරු කරගැනීම ද වැදගත් ය.

හොඳ ඩිජිටල් සහ සයිබර් ආරක්ෂාව සඳහා පරිශීලක මැදිහත්වීම, වගකීම සහ අවදියෙන් කටයුතු කිරීම අවශ්‍ය බව මතක තබාගන්න. මෙය, දෘඩාංග හෝ මෘදුකාංග සපයන්නකු, තොරතුරු තාක්ෂණ වෘත්තිකයකු හෝ පද්ධති කළමනාකරුවකු වැනි වෙනත් සේවාදායකයකු ලවා කරවාගත හැකි දෙයක් නොවේ.

ඩිජිටල් සහ සයිබර් ආරක්ෂාව සඳහා අවශ්‍ය සියලු පියවර මෙහි ලැයිස්තුගත කළ නොහැකි ය. අන්තර්ජාලයේ ඇති තරම් උපදෙස් තිබේ. පහත සාකච්ඡා කරනු ලබන්නේ මූලික පියවර කිහිපයකි. එමගින් සියලු දෙනාට අවබෝධ කරගත හැකි සරල ප්‍රවේශයක් ලබා දෙයි

Source: https://wiobyrne.com/digital-hygiene/

ඩිජිටල් සනීපාරක්ෂාව වැදගත්!

ඩිජිටල් සනීපාරක්ෂාව යනු යමෙකුගේ ඩිජිටල් උපාංග, ගිනුම් සහ දත්තවල පිරිසිදුකම, අපිරිසිදුකම විස්තර කිරීමට යොදන යෙදුමකි.

ගෙදරදී මෙන් ම සේවා ස්ථානයේදී ද ඩිජිටල් සනීපාරක්ෂාව වැදගත් ය. අනාරක්ෂිත වූ චික් ගිනුමක් හෝ උපාංගයක් හේතුවෙන් ඔබගේ ගිනුම් හෝ උපාංගවලට වෙනත් අය පිවිසිය හැකි ය. මෙය ද්වේෂසහගත ලෙස කළහොත්, එයින් අදහස් වන්නේ යමෙකු ඔබගේ දත්තවලට පහර දී ගොනු, මුරපද සොරකම් කිරීම හා ගිනුම් හැක් කිරීම හෝ ඊටත් වඩා නරක දේ කිරීමයි.

පරිගණක වයිරසවලින් හා මැල්වෙයා (MALWARE) වලින් ඔබගේ දත්ත ආරක්ෂා කරගැනීම

පරිගණක වයිරස යනු එක් පරිගණකයකින් තවත් එකකට, ඊමේල්, ඊමේල් අනුබද්ධ හෝ යූඑස්බී උපාංග ආදිය හරහා පැතිරෙන කුඩා වැඩසටහනකි. වයිරස විසින් දත්ත වෙනස් කිරීම හෝ විනාශ කිරීම ද මෙහෙයුම් පද්ධතියේ සාමාන්‍ය මෙහෙයුම් කඩාකප්පල් කිරීම ද කළ හැකි ය.

- යාවත්කාලීන කරන ලද ප්‍රති වයිරස වැඩසටහනක් පාවිච්චි කරන්න.
- ඔබගේ මෙහෙයුම් පද්ධතිය (වින්ඩෝස් වැනි) සහ වෙබ් බ්‍රවිසර (ෆයර්ෆොක්ස් (FireFox), ක්‍රෝම් (Chrome) වැනි) යාවත්කාලීන කරගන්න. ඒවායේ අලුත් ම පිටපත් මගින් වැඩි ආරක්ෂාවක් සැපයේ.
- ඊමේල් සම්බන්ධතා පිළිබඳ පරිස්සම් වන්න. නොදන්නා ඇමුණුම් හෝ අන්තර්ගතයන් (සම්බන්ධතා) විවෘත නොකරන්න. දන්නා මූලාශ්‍රවලින් එන ඒවා සම්බන්ධයෙන් ද එම ක්‍රියාමාර්ගය ම අනුගමනය කරන්න.
- ඔබගේ බ්‍රවිසරයෙන් මතු වන පොපප් වළක්වාගැනීමේ ක්‍රම යොදාගන්න. බොහෝ පොපප් යනු ස්පයිවෙයා (spyware) හෝ ඇඩ්වෙයා (adware) යනුවෙන් හැඳින්වෙන ද්වේෂ සහගත වැඩසටහන් වන අතර එමගින් ඔබගේ පද්ධතියට හානි සිදු විය හැකි ය.
- ෆයර්වෝලයක් (firewall) පිහිටුවාගන්න. ෆයර්වෝලයක් යනු පැමිණෙන අන්තර්ජාල සහ ජාල දත්ත පරීක්ෂා කරන වැඩසටහනකි. ඔබගේ ප්‍රති වයිරස් වැඩසටහන සමග එක්ව අවසර නැති ප්‍රවේශයන් ඔබගේ පරිගණකයට සිදුවීම වළක්වා ගැනීමට එයට හැකි ය.
- පරිපාලක ගිනුම මුරපදයක් යොදා ආරක්ෂා කරගන්න.

සටහන: වයිරස් ආසාදනයක් සිදු වුවත් උපාංගයෙන් කිසිදු රෝග ලක්ෂණයක් නොපෙනීමට පුළුවන. හැමවිට ම පද්ධති පරීක්ෂා කරන්න. උපාංගය පිරිසිදු බව තහවුරු කරගැනීම සඳහා වයිරස් ස්කෑන් කිරීමක් කරන්න.

වයිරස් ආසාදනයක
රෝග ලක්ෂණ

පහත දැක්වෙන්නේ මැල්වෙයා ආසාදන ඇතුළු සුලබ රෝග ලක්ෂණ කිහිපයකි:

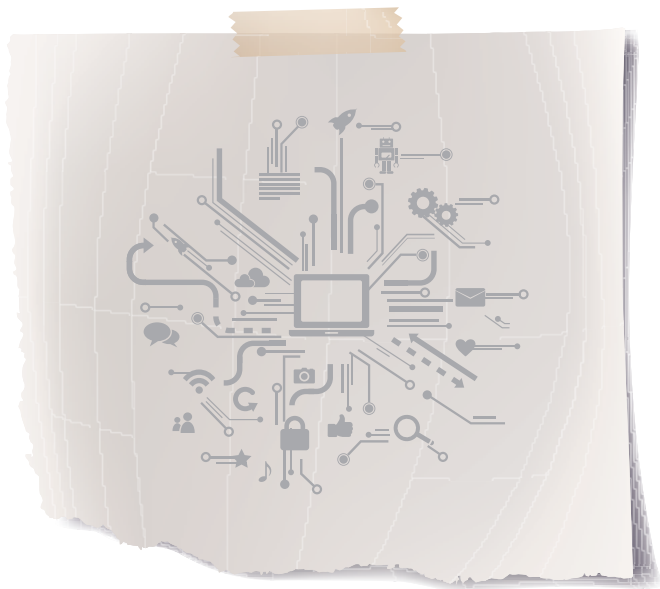
- උපාංගයේ වේගය අඩු වේ. එයට සාධාරණ හේතුවක් සොයාගත නොහැකි ය.
- උපාංගය එකවරම නැවත ආරම්භ වේ. අසාමාන්‍ය චර්යාවක් පෙන්වයි.
- පිහිටුවා තිබෙන යෙදවුම් බලාපොරොත්තු වන අන්දමින් ක්‍රියාත්මක වන්නේ නැත.
- අසාමාන්‍ය (අයහපත් අන්දමින් ලියන ලද) වැරදීම් පිළිබඳ පණිවුඩ ලැබේ.
- පරිශීලක විසින් සිදු කරනු නොලැබූ අලුත් කෙටි පිවිසුම් හෝ වෙනත් අයිකනයන් (**icons**) උපාංගය තුළ පිහිටුවා ඇති ආකාරය දැකිය හැකි ය.
- ගබඩා අවකාශය අඩුවීම හෝ නැති වීම.
- ගොනු හෝ යෙදුම් අවසරයකින් තොරව මැකී යාම.

දත්ත බැකප් කිරීම

දත්ත දෝෂ සහිත වීම හෝ නැතිවීම ඉතා හොඳ දෘඪාංග සහ මෘදුකාංග සමග වුව සිදු විය හැකි ය. දත්ත බැකප් කිරීමේ ක්‍රියාවලිය යනු දත්ත පිටපත් කර, නැති වුණ වේලාවකදී ලබාගැනීම සඳහා වෙනම ගබඩා කර තැබීමයි.

දත්ත බැකප් කිරීමේ සුලබ ක්‍රමයක් වන්නේ දත්ත පරිගණකයේ දෘඪ තැටියෙන් ගෙන තැනකින් තැනකට ගෙන යා හැකි ඉහළ ධාරිතාවක් සහිත යූඑස්බී උපාංගයක් වෙත බාගත (backup) කිරීමයි. ක්ලවුඩ් තුළ හෙවත් දුරස්ථ වෙබ් පාදක අවකාශයක ගබඩා කිරීමේ හැකියාව ද තිබේ. (ගූගල් ඩ්‍රයිව් උදාහරණයකි.)

ක්ලවුඩ් බැකප් මගින් පරිශීලකයන්ට තම දත්ත දුරස්ථ ස්ථානයක දෘඪාංගයක පිටපත් කර තැබිය හැකි ය. පරිශීලකයින්ට එම දත්ත වෙත අන්තර්ජාලය ඔස්සේ නිසි ක්‍රියාමාර්ග හරහා ඕනෑම උපකරණයකින් ඕනෑම වේලාවක පිවිසිය හැකි ය. බොහෝ ක්ලවුඩ් ගබඩා සේවා විශාල ගබඩා අවකාශයක් සපයන අතර දත්ත ආරක්ෂාව සඳහා අන්තර්ගතයන් එන්ක්‍රිප්ට් (encrypt) කිරීම ද කරනු ලැබේ. ගූගල් වැනි ඇතැම් සේවා විසින් මූලික අන්තර්ජාල ගබඩා ධාරිතාවක් අප වෙහි ලියාපදිංචි වූ විගස ලබා දෙයි.



දත්ත එන්ක්‍රිප්ට් (ENCRYPT)කිරීම

එන්ක්‍රිප්ට් කිරීම යනු පරිශීලක අවසරයෙන් තොරව කියැවිය නොහැකි පරිදි ඇල්ගොරිදමක් (algorithm) හෙවත් ස්වයංක්‍රීය මෘදුකාංගයක් භාවිතා කර දත්ත ප්‍රති සැකසීමේ ක්‍රියාවලියයි. මෙමගින් ක්‍රෙඩිට් කාඩ් අංක වැනි ඉතා වැදගත් දත්ත ආරක්ෂා කළ හැකි ය. එහිදී තොරතුරු කේතකරණය කර නොකියවිය හැකි සයිෆර් අක්ෂර (cipher text) බවට පත් කරනු ලැබේ. ඒවා කියවිය හැක්කේ කේතහරණයෙන් හෝ යතුරුපදයක් භාවිතා කිරීමෙනි.

දත්ත එන්ක්‍රිප්ට් කිරීම එය සේප්පුවක බහා තැබීම වැනි ය. ඒවා වෙත ප්‍රවේශ යතුරුපද ඇති අයට පමණක් ඒවා කියැවිය හැකි ය. එන්ක්‍රිප්ට් කිරීම යනු ඩිජිටල් මාධ්‍යයෙන් කරනු ලබන කේතලේඛන ක්‍රමයකි. එහිදී පණිවුඩ අවුල් කිරීම සඳහා ගණිතමය ඇල්ගොරිදමක් භාවිතා කරනු ලැබේ. යවන්නාගේ යතුරුපදය හෝ සයිෆරය ඇති අයට පමණක් ඒවා විකේතීකරණය කරගත හැකි ය. එන්ක්‍රිප්ට් කරන ලද දත්ත දකින වෙනත් අයට ඒවා හුදු සංකේත ගොඩක් පමණි.

එන්ක්‍රිප්ට් කිරීමේ ක්‍රම දෙකකි. සමමිතික එන්ක්‍රිප්ට් කිරීමේදී එක් පෞද්ගලික යතුරුපදයකින් මගින් දත්ත ආරක්ෂා කරනු ලැබේ. අසමමිතික එන්ක්‍රිප්ට් කිරීමේදී බහුවිධ යතුරුද සංකීර්ණයක් භාවිතා කරනු ලැබේ. ඒවා පොදු මෙන් ම පෞද්ගලික ද වේ.

අන්තර්ජාලය හරහා ඊමේල්, චැට් වැනි මාධ්‍යවලින් සන්නිවේදනය කිරීමේදී එන්ක්‍රිප්ට් කිරීම ඉතා වැදගත් ය. පණිවුඩ එන්ක්‍රිප්ට් කර නොතිබුණහොත් අනවසර කියවන්නන්ට ඒවා හඳුනාගැනීමට හෝ වෙනස් කිරීමට පවා පුළුවන.

කෙළවරින් කෙළවරට එන්ක්‍රිප්ට් කිරීම (End-to-end encryption - E2EE) යනු සන්නිවේදනය කරන පරිශීලකයාට පමණක් කියැවිය හැකි පරිදි සන්නිවේදනය කරන ක්‍රමයකි. එමගින් රහසින් කියවීමට ඉඩ තිබෙන විදුලි සංදේශ සේවා සපයන්නන්ට, අන්තර්ජාල සේවා සපයන්නන්ට සහ සන්නිවේදන සේවා සපයන්නන්ට ද පණිවුඩය කේතහරණය කරගැනීම සඳහා අවශ්‍ය යතුරු වෙත පිවිසීම වළක්වයි.

එන්ක්‍රිප්ට් කිරීම හේතුවෙන් ඔබගේ සන්නිවේදනය විශ්වසනීය හා රහස්‍ය වෙයි. එක් කෙළවරක සිට අනෙක් කෙළවරට අන්තර්ජාලයෙන් සන්නිවේදනය පිළිබඳ සලකා බැලීමේදී උදාහරණ ලෙස WhatsApp, iMessage සහ Signal (මෙහිදී E2EE නිතැතින් ම ක්‍රියාත්මක වේ) හෝ Telegram සැලකිය හැකි ය.

සංවේදී දත්ත විනාශ කිරීම

ඔබ ඔබගේ පරිගණකයේ ගොනුවක් මකා දමන විට එය සම්පූර්ණයෙන් ම අතුරුදහන් වන්නේ නැත. එහිදී සිදුවන්නේ පද්ධතිය තුළ ගොනුව සඳහා යොමුව මකා දැමීමයි. එම ගොනුව මත වෙනත් ගොනුවක් නිර්මාණය කරන තෙක් හා ඉන් පසුවත් එය තැටියේ තිබේ. එයින් පසුවත්, එය ආපසු ලබාගත හැකි ය.

ඔබට කිසියම් දත්තයකින් සම්පූර්ණයෙන් ම මිදීමට අවශ්‍ය නම් ඒ සඳහා ආරක්ෂිත මකාදැමීමේ මෙවලමක් භාවිතා කළ යුතු ය. එමගින් සංවේදී තොරතුරු මත ලියා ඒවා විනාශ කරනු ලැබේ. එයින් පසුව පවා ද ඩිජිටල් තොරතුරු හැසිරවීමේ කුසලතා සහිත දත්ත ආපසු ලබාගන්නෙකුට ලබාගත හැකි ය.

වයිපිං (wiping) නමින් හැඳින්වෙන ක්‍රියාවලියක් මගින් අහඹු ලෙස තෝරා ගන්නා දත්ත මගින් ගොනුවක් මත කීප වතාවක් ලියනු ලැබේ. ඉරේසර් යනු වින්ඩෝස් සඳහා වන තවත් උසස් ආරක්ෂක මෙවලමකි. එහිදී පරිශීලකයාට දෘඪ තැටියේ සංවේදී දත්ත මත පරිස්සමෙන් තෝරාගත් රටාවකට කීප වරක් ලිවීමෙන් ඒවා සම්පූර්ණයෙන් ම ඉවත් කළ හැකි ය.
Https://eraser.Heidi.Ie/

අන්තර්ජාලයේ සිටින විට ඔබේ දත්ත ආරක්ෂා කරගැනීම

වයිෆයි (Wi-Fi) හෝ රැහැන් රහිත අන්තර්ජාල ප්‍රවේශයෙන් අදහස් වන්නේ ගුවන් විදුලි තරංග භාවිතා කර අන්තර්ජාලයට සම්බන්ධ වීමයි. ඒ සඳහා රැහැන් අවශ්‍ය නැත. එමගින් පරිශීලකයාට යම් ස්ථානයක තැනින් තැනට යන විට ද අන්තර්ජාලය සමග සම්බන්ධව සිටිය හැකි ය. එහෙත්, මෙම පහසුකම පරිස්සමෙන් පරිහරණය කළ යුතු ය.

පොදු වයිෆයි ගුවන් තොටුපළ, සාප්පු සංකීර්ණ, අවන්හල් සහ හෝටල්වල තිබේ. එමගින් ඔබට අන්තර්ජාලයට නොමිළේ සම්බන්ධ විය හැකි ය. පොදු වයිෆයි ඔබගේ සමාජ මාධ්‍ය පරිහරණයට සහ පුවත් ලිපි කියවීමට යොදාගත හැකි මුත්, ඒ ඔස්සේ ඊමේල් කියවීම හෝ බැංකු ගිනුම් වෙත පිවිසීම ආරක්ෂිත නැත.

එසේ වන්නේ ඇයි? පොදු වයිෆයි ජාලයන් විසින් ඔබගේ දත්ත වෙනත් අය විසින් ග්‍රහණය කරගැනීමට තිබෙන ඉඩ වැඩි කරනු ලැබේ. ඇත්තෙන් ම, ඔබ විශ්වාස නොකරන පුද්ගලයන් විසින් පවත්වාගෙන යන පොදු වයිෆයි හොට් ස්පොට්වලින් ඈත්ව සිටීම ආරක්ෂිත ය. පරිශීලකයාගේ තොරතුරු සොරකම් කිරීම සඳහා අපරාධකරුවන් විසින් ද මෙවැනි හොට්ස්පොට් පාවිච්චි කිරීමට ඉඩ තිබේ.

තවත් අවවාදයක්: හැමවිට ම සමාජ මාධ්‍යවල හා වෙනත් වෙබ් අඩවිවල ඇති පෞද්ගලිකත්වය ආරක්ෂා කිරීමේ සැකසුම් පිළිබඳ අධ්‍යයනය කරන්න. ඔබට පාලක පැනලය හෝ සෙට්ටිං මෙනුව ඔස්සේ පෞද්ගලිකත්ව පාලනය කිරීමේ ක්‍රම සොයාගත හැකි ය. පෞද්ගලිකත්වය පාලනය අලුත් අන්තර්ජාල සේවා ගිනුමකට ලියාපදිංචි වීමේ ක්‍රියාවලියේදී පිරිනමනු ලැබේ. වෙබ් අඩවියක් පරිශීලනය කිරීමට පෙර හැමවිට ම පෞද්ගලිකත්වය පාලනය කිරීම සඳහා එහි තිබෙන ක්‍රම සොයා බලා තේරුම් ගන්න.

මතක තබාගත යුතු තවත් කරුණක් වන්නේ, ඔබ වෙනත් අය සමග බෙදාහදාගන්නා උපකරණයකින් ඊමේල්, සමාජ මාධ්‍ය හෝ වෙනත් ලොගිං (login) විය යුතු සේවාවක් වෙත පිවිසියේ නම්, එය අවසන් කරන විට ගිනුමෙන් පිටවන්න. අන්තර්ජාල ගත වීමට පහසුකම් සපයන පොදු ස්ථානවලදී බොහෝ පරිශීලකයන් හට ගිනුමෙන් පිටවීමට අමතක වේ. එවිට, ඊළඟට එම උපාංගය පරිහරණය කරන පුද්ගලයාට ඔබගේ ගිනුමට පිවිසිය හැකි අතර එය පැහැරගැනීමට ද හැකි ය.

ඩිජිටල් සම්පත් ආරක්ෂා කරගැනීම

සරල, එහෙත්, වැදගත් මූලික ආරක්ෂක පියවර කීපයක් ඔස්සේ ඔබට ඩිජිටල් සම්පත් ආරක්ෂා කරගත හැකි ය.

මුරපදයක් හෝ පාස්වර්ඩ් එකක් යනු, පරිශීලක අනන්‍යතාවක් තහවුරු කිරීම සඳහා මතකයේ තබා ගන්නා රහසකි. ඩිජිටල් සංදර්භය තුළ, එය අක්ෂර, ඉලක්කම් හෝ විරාම ලකුණු විශේෂිත ආකාරයකට පෙළගස්වන ලද බන්ධනයකි.

ආරක්ෂිත මුරපද භාවිතා කිරීම ඩිජිටල් සම්පත් අනවසර ප්‍රවේශයෙන් හෝ හැකිංවලින් (hacking) ආරක්ෂා කරගැනීම සඳහා වැදගත් පියවරකි. මුරපදයක් සත්‍ය වචනයක් වීම අවශ්‍ය නැත. වචනයක් නොවන යෙදුමක් අනුමාන කිරීම අපහසු ය. එය මුරපදයක විශිෂ්ට ලක්ෂණයකි.

පහත දැක්වෙන්නේ වඩා හොඳ මුරපද සඳහා මූලික කරුණු කීපයකි:

- හැමවිට ම, ඔබේ ගිනුම් ආරක්ෂා කිරීම සඳහා ශක්තිමත් මුරපදයක් භාවිතා කරන්න. අංක, සංකේත, කැපිටල් අකුරු සහ සිම්පල් අකුරු සහිත දීර්ඝ මුරපදයක් භාවිතා කරන්න.
- ඔබ පමණක් මුරපදය ලෙස දන්නා පදයක් භාවිතා කරන්න.
- ඔබගේ උපන් දිනය, සංවත්සරයක්, ලිපිනයක්, උපන් නගරය, පාසල, ඥාතීන් හා සුරතල් සතුන් වැනි හඳුනාගත හැකි පෞද්ගලික තොරතුරු මුරපද ලෙස පාවිච්චි කිරීමෙන් වළකින්න.
- ඔබගේ එක් එක් ගිනුම වෙනුවෙන් විශේෂිත මුරපද භාවිතා කරන්න. වැදගත් ගිනුම් වෙනුවෙන් එකම මුරපදය නැවත නැවත භාවිතා කිරීම අවදානම් ය. කිසිවෙකුට ඔබගේ එක් ගිනුමක මුරපදය ලබාගත හැකි වුණහොත්, එමගින් ඔවුන්ට ඔබගේ ඊමේල් ආදියට පමණක් නොව බැංකු ගිනුමට පවා පිවිසිය හැකි ය.
- මුරපදය අමතක වුවහොත්, මුරපදය නැවත සොයාගැනීම සඳහා විකල්ප භාවිතා කරන්න.
- ඔබගේ මුරපදය නිශ්චිත කාලයකට වරක් වෙනස් කරන්න. ඔබ මුරපදය වෙනස් කරන කාලාන්තරය කෙටි වන තරමට හොඳ ය.
- වෙබ් බ්‍රව්සරවලට ඔබගේ මුරපදය මතක තබාගන්නට ඉඩ දීම සුවපහසු විය හැකි ය. එහෙත්, එය අවදානම් භාවිතාවකි. යමෙකු ඔබගේ උපාංගයට පිවිසුණහොත්, ඔවුන්ට ඔබගේ ගිනුමට පහසුවෙන් පිවිසිය හැකි ය

ඩිජිටල් සම්පත්
යනු මොනවා ද?

සරලව දක්වන්නේ නම්, ඩිජිටල් සම්පත් යනු ඩිජිටල් ස්වරූපයෙන් ගබඩා කරනු ලබන අන්තර්ගතයන් ය. ඒවා රූප, ඡායාරූප, වීඩියෝ, ලේඛන ගොනු, ස්ප්‍රෙඩ්ෂීට්, ස්ලයිඩ් කට්ටල ආදිය විය හැකි ය. ඩිජිටල් සම්පත් පරිගණක දෘඪ තැටිවල, සුහුරු දුරකථනයක මතකයේ හෝ අන්තර්ජාලයේ ගබඩා කර තිබිය හැකි ය.

ඊමේල් හා සමාජ මාධ්‍ය වැනි වැදගත් ඩිජිටල් සේවා ද ඩිජිටල් සම්පත් අතරට ගැනේ.

පියවර දෙකේ තහවුරු කිරීම භාවිතා කිරීම

ශක්තිමත් මුරපදයක් යෙදීමෙන් පසු, ඊළඟ වඩාත් වැදගත් පියවර වන්නේ පියවර දෙකේ තහවුරු කිරීම ක්‍රියාත්මක කිරීමයි (මෙය two step authentication ලෙස හැඳින්වේ).

එයින් අදහස් වන්නේ මුරපදයට අමතරව, ඔබ විසින් ඔබගේ ගිනුමට පිවිසීම සඳහා දෙවන තොරතුරක් ද ඇතුළත් කළ යුතු වීම ය. එය සාමාන්‍යයෙන් ලියාපදිංචි ජංගම දුරකථනයට යවනු ලබන කෙටි පණිවුඩයකි. (එය වලංගු වන්නේ විනාඩි කීපයක් තුළ එක් වරක් පමණක් භාවිතා කිරීමට ය.) සියලු ප්‍රධාන සමාජ මාධ්‍ය වේදිකා සහ ගූගල් වැනි සේවාවන් විසින් ද දැන් පියවර දෙකේ තහවුරු කිරීමේ ආරක්ෂක විධිවිධානය හඳුන්වා දී තිබේ.

වෙබ් සේවාවක් විසින් අක්ෂර සහ ඇප් පදනම් කරගත් ආකාර දෙකේ තහවුරු කිරීමක් භාවිතා කරන්නේ නම්, කරුණාකර ඇප් පදනම් කරගත් තහවුරු කිරීම තෝරන්න. එයට හේතුව, කෙටි පණිවඩ එන්ක්‍රිප්ට් කර නොතිබීමයි. එබැවින් ඒවා හඳුනාගත හැකි ය.

මුරපද යනු රහස් ය

මුරපද පෞද්ගලික හා රහස්‍ය විය යුතු ය. ඒවා නිර්මාණය කරගන්නේ අන් අය සමග බෙදාහදා ගැනීම සඳහා නොවේ. එසේම, කිසිදු ආකාරයකින් ප්‍රදර්ශනය කිරීමට ද නොවේ. එහෙත්, මෙය වනාහි බොහෝ පුද්ගලයන් සහ සංවිධාන විසින් කරනු ලබන සුලබ වරදකි. ඒ පිළිබඳ පසුව පසුතැවීමට සිදු වේ. එබැවින්, මුරපදයකට ඔබගේ ඩිජිටල් සම්පත් ආරක්ෂා කළ හැක්කේ ඔබ එය රහසක් ලෙස තබාගන්නේ නම් පමණක් බව මතක තබාගත යුතු ය.

ජංගම දුරකථන ආරක්ෂාව

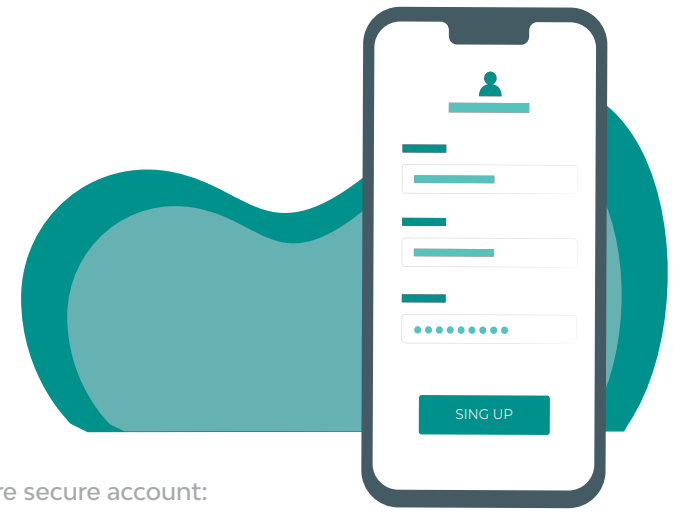
සෑම ජංගම දුරකථනයක් ම, GSM මෝඩමයක් හෝ ඇතුළෙන් ම දුරකථනයක්/ මෝඩමයක් ඇති සෑම උපකරණයක් ම සතුව ඉලක්කම් 15ක ඉමි අංකයක් (IMEI - International Mobile Equipment Identity) හෙවත් ජාත්‍යන්තර ජංගම උපකරණ හඳුනාගැනීමේ අංකයක් තිබේ.

ඉමි අංකය නිර්මාණය කරනු ලැබුවේ සිම්පත උපාංගය සඳහා ස්ථිර හඳුනාගැනීමේ ක්‍රමයක් විය නොහැකි නිසා ය. (සිම්පත පරිශීලකයාට සම්බන්ධ අතර, දුරකථනයකින් තවත් දුරකථනයකට මාරු විය හැකි ය.) ඉමි අංකය මත පදනම්ව, ඔබට උපාංගය පිළිබඳ යම් තොරතුරු පරීක්ෂා කළ හැකි ය. උදා: එහි වර්ගය සහ මාදිලිය

ඕනෑම දුරකථනයක ඉමි අංක පරීක්ෂාව සඳහා පහසුම ක්‍රමය වන්නේ *#06# භාවිතා කිරීමයි.

උපාංගය සේවාවන් සඳහා යවන විට වගකීම් අයදුම්පත් පිරවීමේදී ඉමි අංකය ප්‍රයෝජනවත් ය. ඒ හැරත්, උපාංගය සම්බන්ධ සොරකමක් හෝ නැතිවීමක් පිළිබඳ වාර්තා කරන විට ද පොලිසියට හෝ ජාල සේවා සම්පාදකවරයාට ඉමි අංකය ලබා දිය යුතු ය. ඉන් පසු, ඔබගේ දුරකථනය බ්ලොක් කරන්නැයි ඔබට දැනුම් දිය හැකි ය. ඉන් පසු, සිම් කාඩ්පත වෙනස් කළ ද උපකරණය භාවිතා කළ නොහැකි ය.

ඔබ ඔබගේ දුරකථනයේ ඉමි අංකය දැනගෙන එය කොහේ හෝ ලියා තබන්න.



[1] Google has some useful advice on creating a strong password and a more secure account: https://support.google.com/accounts/answer/32040?hl=en

පහත දැක්වෙන්නේ ඔබේ දුරකථනයේ ආරක්ෂාව ඉහළ නැංවීම සඳහා මූලික උපදෙස් කීපයකි:

- දුරකථනය ආරම්භ කිරීම සඳහා ශක්තිමත් පින් අංකයක් යොදන්න. අවම වශයෙන් ඉලක්කම් හයක කේතයක් යොදන්න.
- නිරන්තරයෙන් මෘදුකාංග යාවත්කාලීන කරගන්න.
- ඔබගේ ජංගම උපකරණයට ප්‍රති වයිරස් හා ප්‍රති මැල්වෙයා ආරක්ෂාව යොදාගන්න.
- විශ්වසනීය සේවාවන්ගෙන් පමණක් ඇප් බාගත කරගන්න (උදා: ගූගල් ප්ලේ ස්ටෝර් (Google play store) සහ ඇපල් ඇප් ස්ටෝර් (Apple app store)
- ඇප් සඳහා ඇති අවසරය පාලනය කරන්න: ඇන්ඩ්‍රොයිඩ් සහ IOS පද්ධති සතුව, ඔබගේ උපාංගයේ කුමන ඇප් එක වෙත පිවිසිය හැකි ද, නොහැකි ද යන්න නිවැරදිව පාලනය කිරීමේ පහසුව සඳහා මෙවලම් තිබේ. ඇප්වලට ඒවා පවත්වාගෙන යා හැකි අත්‍යවශ්‍ය දත්ත වෙත පමණක් පිවිසිය හැකි ආකාරයට අවසරය සීමා කරන්න. (Mypermissions.Com යනු, ඇප් රැසක් හරහා ඔබට අවසර සැකසුම් පරීක්ෂා කරන්නට ඉඩ දෙන සුරුබුහුටි මෙවලමකි. ජංගම දුරකථන හිතවාදී ඇප් සමග අවසරයන් පිරිසිදු කිරීම සඳහා එයින් සිහිකැඳවීම් එවයි. ඇප් ඔබගේ පෞද්ගලික තොරතුරු වෙත පිවිසෙන විට එමගින් අනතුරු ඇඟවීම් එවයි. එවිට ඔබට එක් ක්ලික් එකකින් ඇප් එක ඉවත් කළ හැකි ය.)
- දුරස්ථ ස්ථානගත වීම හා උපාංගය වයිපිං කිරීම සක්‍රිය කරන්න. ඔබගේ උපාංගය නැති වූ හෝ සොරකම් කළ විට, ට්‍රැකිං ඇප්වලට ඔබගේ උපාංගය ඇති තැන ඔබට පැවසිය හැකි ය. මෙම ඇප් මගින් ඔබට සංවේදී තොරතුරු දුර සිට වයිප් කිරීමේ හැකියාව ලැබේ.
- බ්ලූටූත් පාවිච්චි නොකරන විට එය අක්‍රිය කරන්න. බ්ලූටූත් මගින් අවදානම්වලට දොර විවර වේ. බ්ලූටූත් ප්‍රහාර වැල්ල කළ හැක්කේ අවසර ඉල්ලීම් පිළිගැනීමේ ක්‍රියාවලිය අපහරණය මත ය. එය බ්ලූටූත් සම්බන්ධතාවේ කොඳුනාරටියයි. එය අපහරණය කිරීමෙන් ප්‍රහාර වැල්ල කිරීම වැළැක්වීමට තිබෙන එකම ක්‍රමය වන්නේ බ්ලූටූත් භාවිතා නොකරන විට එය ක්‍රියා විරහිත කිරීම යි. එය දැකිය නොහැකි හෝ හඳුනාගත නොහැකි ස්වරූපයට මාරු කිරීමෙන් ද ඔබගේ උපකරණය බ්ලූටූත් ප්‍රහාරවලට ගොදුරු විය හැකි ය.

ඩිජිටල් අනන්‍යතා සොරකම

අනන්‍යතා සොරකම අන්තර්ජාලයේදී මෙන් ම ඉන් බැහැරව ද සිදු විය හැකි ය. එයින් අදහස් වන්නේ පෞද්ගලික තොරතුරු අනවසරයෙන් එකතු කිරීම හා පසුව ඒවා අපරාධකාරී අරමුණු වෙනුවෙන් භාවිතා කිරීමයි. ක්‍රෙඩිට් කාඩ් සහ බැංකු ගිනුම් වෙත හොරෙන් පිවිසීම, ජංගම දුරකථන සම්බන්ධතා ලබාගැනීම ආදිය ඒ අතර වේ. එයින් විඳින්දිතයාට බරපතල ගැටලු වලට මුහුණ දෙන්නට සිදු වේ.

පුද්ගලයකුගේ අනන්‍යතාව සොරකම් කළ හැකි ආකාර රැසක් තිබේ. අන්තර්ජාල සේවා භාවිතා කරන විට මහජනයා මෙම අවදානමට මුහුණ දෙති. එහිදී අපරාධකරුවන්ට විවිධාකාරයෙන් පෞද්ගලික තොරතුරු වෙත පිවිසිය හැකි ය.

අනන්‍යතා සොරකම් කරන්නන් විද්‍යුත් මාර්ගවලින් පෞද්ගලික තොරතුරු ලබාගන්නා ආකාර කීපයක් පහත දැක්වේ.

- ඉවත දමන ලද පෞද්ගලික පරිගණක, ජංගම දුරකථන හෝ යූඑස්බී මතක ගබඩා වැනි විද්‍යුත් උපාංගවල ගබඩා කර තිබෙන දත්ත ලබාගැනීම.
- කීස්ට්‍රෝක් ලොගිං (keystroke logging) වැනි මැල්වෙයා හෝ ස්පයිවෙයා භාවිතා කර පෞද්ගලික තොරතුරු සොරකම් කිරීම.
- පෞද්ගලික තොරතුරු විශාල ප්‍රමාණයන්ගෙන් ලබාගත හැකි පරිගණක පද්ධති හා දත්ත පදනම් හැක් කිරීම.
- ෆිෂිං හෙවත් බැංකු හෝ සිල්ලර වෙළඳ ආයතන වැනි විශ්වාසවන්ත සංවිධාන ලෙස ඊමේල්, කෙටි පණිවුඩ ආදිය හරහා පෙනී සිටිමින් පෞද්ගලික මුල්‍ය තොරතුරු ඇතුළත් කිරීමට පරිශීලකයා පෙළඹවීම.
- දුර්වල මුරපද හඳුනාගැනීම (බොහෝ විට නිවැරදිව අනුමානය කිරීමෙන්) ඔස්සේ පරිශීලක අන්තර්ජාල ගිනුම් වෙත පිවිසීම
- ඊමේල් මුරපද හඳුනාගැනීම සඳහා ප්‍රමාණවත් තරම් පෞද්ගලික තොරතුරු සමාජ ජාල හරහා ලබාගැනීම හෝ අන්තර්ජාලයේදී වෙනත් ආකාරවලින් අදාළ පුද්ගලයා ලෙස පෙනී සිටීම
- බැංකු සහ ණය කාඩ්පත් නිවේදන ආදී පෞද්ගලික තොරතුරු ලබාගැනීම සඳහා විඳින්දිතයන්ගේ ඊමේල් ලිපිනය හරවාගැනීම හෝ තම නමින් අලුත් ගිනුම් ආරම්භ කර තිබෙන බව විඳින්දිතයා සොයාගැනීම වැළැක්වීම.

අනන්‍යතා සොරකම සම්බන්ධ සියලු උපද්‍රවවලින් ආරක්ෂා වීමේ ක්‍රමයක් නැත. එහෙත් අපට දැනුවත් වීමෙන් හා නිරන්තරයෙන් අවධානයෙන් සිටීමෙන් අප ආරක්ෂා කරගත හැකි ය. පහත දැක්වෙන්නේ අන්තර්ජාල මූලාශ්‍ර ඇසුරෙන් ලබාගත් වී සඳහා යෝග්‍ය පියවර කීපයකි :

- ඔබ ආරක්ෂිත යයි සිතෙන ඔබගේ බැංකුවේ වෙබ් අඩවිය වැනි වෙබ් අඩවියක සිටියදී තුන්වන පාර්ශ්වයන් වෙත නැවත යොමුකිරීම පිළිබඳ සැලකිලිමත් වන්න. සැකසහිත අන්තර්ජාල ලිපින ගැන සැලකිලිමත් වෙන්න.

- සැකසහිත ගනුදෙනු සිදු වේ ද යන කරුණ සම්බන්ධයෙන් ඔබගේ ණය කාඩ්පත් සහ බැංකු නිවේදන සම්බන්ධයෙන් පරීක්ෂාකාරී වන්න.

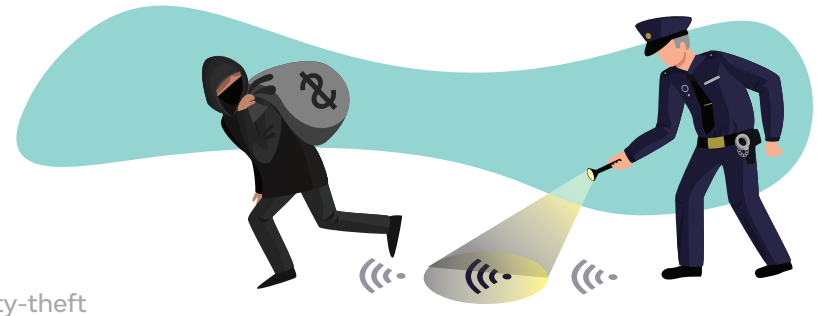
- මුල්‍ය ගනුදෙනු සඳහා සුරක්ෂිත වෙබ් අඩවි පමණක් භාවිතා කරන්න. ඔබ අන්තර්ජාලයේදී මිළදීගැනීමක් සඳහා ණය කාඩ්පත් අංක ඉදිරිපත් කරන්නේ නම්, බ්‍රව්සරයේ ස්ටේටස් බාර් එකෙහි, සාමාන්‍යයෙන් දකුණු කෙළවරේ ඉබි අගුලක සලකුණ තිබේදැයි බලන්න. එසේ නොමැති නම්, ඔබගේ තොරතුරු ඇතුළත් නොකරන්න.

- ඔබගේ බැංකුව හෝ විශ්වවිද්‍යාලය වැනි පිළිගත් ආයතනයක් ලෙස පෙනී සිටිමින් පෞද්ගලික තොරතුරු ඉල්ලා සිටින ඊමේල්වලට පිළිතුරු දීමෙන් වළකින්න. ගැටලු සහගත ආයතනය හා එම ඊමේල් පිළිබඳ දුරකථනයෙන් හෝ ඔවුන්ගේ වෙබ් අඩවිය හරහා විමසන්න.

- යම් දෙයක් අදහාගත නොහැකි තරම් විස්මිත නම් (පැරිසියට නොමිළේ චාරිකාවක් දිනාගන්නට ඔබේ ණය කාඩ්පත් අංකය ඇතුළත් කරන්න!) එය වංචාවක් විය හැකි ය. සාමාන්‍ය බුද්ධිය පාවිච්චි කරන්න.

- පොදු වයිෆයි භාවිතා කරමින් කිසිදු පෞද්ගලික තොරතුරක් යවන්න එපා.

- නෝටන් ඇන්ටි වයිරස් (Norton Anti-Virus) වැනි සමාගම්වලින් එවන බව පෙන්වන, ඔබට යමක් බාගත කිරීමට පොළඹවන ඊමේල් පිළිබඳ සැලකිලිමත් වන්න. ඊමේල්වලට පිළිතුරු නොලියා, තොරතුරු ලබාගැනීම සඳහා අදාළ සමාගම සමග සෘජුව සම්බන්ධ වන්න.



[2] More information at: https://www.imei.info/
[3] Source: https://www.techopedia.com/definition/13637/identity-theft

සිද්ධි අධ්‍යයන

සිද්ධි අධ්‍යයනය 1 : දත්ත ඩෙටොක්ස් කට්ටලය (DETOX KIT)

ඔබගේ දත්ත ධාරාව අවම කිරීම, ඩිජිටල් වශයෙන් වඩාත් සුරක්ෂිත වීම, තාක්ෂණය සමග යහපත් සම්බන්ධයක් ගොඩනගාගැනීම යන කාරණා කොතැනින් ආරම්භ කළ යුතු ද යන්න දැනගැනීම දුෂ්කර ය. අපගේ උපකරණ අපගේ පෞද්ගලික ජීවිත සමග වැඩියෙන් අන්තර් සම්බන්ධිත වන විට අප එහි තුලනයක් සොයාගත යුතු ය.

Data Detox Kit යනු සරල මෙවලම් කට්ටලයකි. එමගින් ඔබ යහපත් ලෙස අන්තර්ජාලය භාවිතා කිරීම වෙත යොමු කරනු ලැබේ. එමගින්, ඔබගේ ඩිජිටල් ජීවිතයේ විවිධ පැතිකඩ ඔස්සේ යමින්, ඔබ දුරකථනයේ ගෙවන කාලයේ සිට ඔබ පාවිච්චි කරන ඇප් සහ ඔබ යොදන මුරපද දක්වා සාකල්‍ය ප්‍රවේශයක් වෙත ඔබ යොමු කරනු ලැබේ.

Data Detox Kit නිෂ්පාදනය කරනු ලැබුවේ Tactical Tech නම් ජාත්‍යන්තර ලාභ නොලබන සංවිධානය විසිනි. එම සංවිධානය පුරවැසියන් සහ සිවිල් සමාජ සංවිධාන සමග කටයුතු කරනුයේ සමාජයේ තාක්ෂණ භාවිතයේ බලපෑම අධ්‍යයනය කිරීමට සහ අවම කිරීමට ය.

එහි මුද්‍රිත පිටපත ලන්දේසි, ප්‍රංශ, ඉන්දුනීසියානු, නෝර්වීජියානු, පෝලන්ත, පෘතුගීසි, ස්පාඤ්ඤ සහ ස්වීඩිෂ් භාෂාවලට පරිවර්තනය කර තිබේ. datadetox@tacticaltech.org වෙත ඔබට එම පිටපත අවශ්‍ය භාෂාව සහ ඔබ එය භාවිතා කරන්නට යන්නේ කෙසේ ද, කොහිදී ද යන කරුණු සමග පණිවුඩයක් යැවීමෙන් ඔබට එහි පීඩීඑෆ් (PDF) පිටපතක් ලබාගත හැකි ය.

Website: https://datadetoxkit.org/en/home

[4] Source: http://www.digitalresponsibility.org/how-to-avoid-online-identity-theft

සිද්ධි අධ්‍යයනය 2: ඩිජිටල් ප්‍රථමාධාර කට්ටලය

ඩිජිටල් හදිසි අවස්ථා පිළිබඳ ක්‍රියා කරන සංවිධාන රැසක් විසින් කරන ලද නිරීක්ෂණයක දී හෙළි වූයේ පුද්ගලයකු ඩිජිටල් වශයෙන් ඉලක්ක වූ විට, එම පුද්ගලයා බොහෝ විට කළ යුතු දේ නොදන්නා බව ත් උදව් ලබාගත යුත්තේ කාගෙන් ද යන්න නොදන්නා බව ත් ය. මේ නිසා ඩිජිටල් ප්‍රථමාධාර කට්ටලය හඳුන්වා දෙන ලදී. මෙය භාවිතයට පැමිණියේ හදිසි අවස්ථා වැළැක්වීම සඳහාත්, කරදරයට පත් වූ විට ප්‍රතිචාරාත්මක ක්‍රියාමාර්ග ගැනීම සඳහාත් සෑම අයෙකුට ම හැකි ය යන විශ්වාසය විසින් වය සැකසීමට අනුප්‍රාණය සැපයිණි.

ඩිජිටල් ප්‍රථමාධාර කට්ටලය විසින් ඉතාම සුලබ ආකාරවලින් ඩිජිටල් තර්ජනවලට මුහුණ දෙන අය සඳහා මූලික සහයෝගය ලබාදෙයි. මානව හිමිකම් ආරක්ෂකයන්ට, බ්ලොග්කරුවන්ට, ක්‍රියාධරයන්ට සහ පුවත්පත් කලාවේදීන්ට තමන් ප්‍රහාරවලට මුහුණ දෙද්දීත්, තර්ජනවලට මුහුණ දෙන වෙනත් පුද්ගලයන්ට ඩිජිටල් වශයෙන් ප්‍රතිචාර දක්වන පළමු උදව්කරුවන් වෙද්දීත් භාවිතා කළ හැකි මාර්ගෝපදේශ මෙහි තිබේ.

කට්ටලය ආරම්භ වන්නේ ඔබගේ සම්බන්ධතා ඩිජිටල් තර්ජනයකට මුහුණ දෙද්දී සහ උපකාර අවශ්‍ය විටදී සුරක්ෂිත සන්නිවේදනයක් ගොඩනගාගන්නේ කෙසේ ද යන්නෙනි. හයිජැක් කිරීම, උපාංග පැහැරගැනීම, මැල්වෙයා ආසාදන සහ DDoS ප්‍රහාර දක්වා උපදෙස් මෙම කට්ටලය විසින් සපයනු ලැබේ.

ස්වයං තක්සේරුවක් කරගැනීමට හෝ පළමු ප්‍රතිචාරකයකුට ඔබ මුහුණ දෙන අභියෝග වඩා හොඳින් තේරුම් ගැනීමට හෝ මගපෙන්වීම මෙම ප්‍රශ්න විසින් සපයනු ලැබේ. වය විවිට ප්‍රශ්නය තේරුම්ගැනීමට හා විසඳිය හැකි ආකාරය පිළිබඳ මූලික පියවර ගනියි. ඔබට හෝ පළමු ප්‍රතිචාරකරුවෙකුට හෝ විශේෂඥවරයකුගේ උපකාර ඉල්ලීමට සිදුවන අවස්ථාව තේරුම් ගැනීමට මෙම පියවර විසින් උපකාර කළ යුතු ය.

සිදුවන්නේ කුමක් ද යන්න තක්සේරු කරගැනීමට හා තමන් විසින් ම ගැටලුව අවම කරගැනීම සඳහා ගත හැකි පියවර තිබේ නම් වී සඳහා අවශ්‍ය උපදෙස් ඩිජිටල් ප්‍රථමාධාර කට්ටලය විසින් ඔබට ලබා දෙයි. මෙහි දක්වා තිබෙන කිසියම් විසඳුමක් ක්‍රියාත්මක කිරීම සම්බන්ධයෙන් ඔබට අවිශ්වාසයක් හෝ අපහසුවක් හෝ ඇති වන ඕනෑම අවස්ථාවක ඔබ, වය සංවර්ධනය කළ අය වැනි පුහුණු වෘත්තිකයකුගේ උපදෙස් ලබාගන්න.

කට්ටලයේ ස්වයංව හඳුනාගැනීමේ ගුණය විසින් පුවත්පත් කලාවේදීන්, බ්ලොග්කරුවන්, ක්‍රියාධරයන් සහ මානව හිමිකම් ආරක්ෂකයන් හට තම ඩිජිටල් සම්පත්වලට සිදුවන්නේ කුමක් ද යන්න තේරුම් ගැනීමටත්, උපකාර පැතිය යුතු අවස්ථාව කඩිනමින් තේරුම් ගැනීමටත්, අවශ්‍ය වන්නේ කුමනාකාරයේ උපකාර ද යන්න තීරණය කිරීමටත්, පුද්ගල ඩිජිටල් ආරක්ෂාව වර්ධනය කරගැනීමටත් හැකියාව ලබාදෙයි.

More: https://www.digitaldefenders.org/digitalfirstaid/

සාකච්ඡා කරුණු

පහත දැක්වෙන්නේ මාතෘකාව පිළිබඳ වැඩිදුර අධ්‍යයනය සඳහා සාකච්ඡා කළ හැකි ප්‍රශ්න කීපයකි.

- ඩිජිටල් සහ සයිබර් ආරක්ෂාව යනු පරිශීලකවරයා හා තාක්ෂණික සේවා සපයන්නා අතර බෙදාහදාගත් වගකීමකි. ඔබ මෙයට එකඟ ද? සාකච්ඡා කරන්න.
- ඔබ වයිරස් හෝ මැල්වෙයා ප්‍රශ්නයකට මුහුණ දී තිබේ ද? එසේ නම් ඔබ හෝ ඔබගේ සංවිධානය විසින් එම ප්‍රශ්නය විසඳීම සඳහා ගන්නා ලද ක්‍රියාමාර්ග මොනවා ද?
- ඔබ ඔබගේ ඩිජිටල් සේවාවන් සඳහා එන්ක්‍රිප්ට් කිරීම භාවිතා කර තිබේ ද? එසේ කර තිබේ නම්, ඔබගේ අත්දැකීම විස්තර කරන්න.
- දත්ත පෞද්ගලිකත්වය උල්ලංඝනය කිරීමකදී කළ හැක්කේ කුමක් ද? ඔබ හෝ ඔබගේ සංවිධානයට ඒ සම්බන්ධයෙන් හදිසි සැලසුමක් තිබේ ද?
- ඩිජිටල් අනන්‍යතා සොරකම් කිරීම සම්බන්ධ අවස්ථාවක් ඔබ දන්නවා ද? එය සිදු වූයේ කෙසේ ද සහ එම ගැටලුව විසඳාගත් ආකාරය කුමක් ද?
- ඔබගේ නිවසින් හා කාර්යාලයෙන් බැහැරදී ඔබ පොදු වයිෆයි භාවිතා කරනවා ද? එසේ නම්, ඔබ අනුගමනය කරන පූර්ව ආරක්ෂක විධිවිධාන මොනවා ද?

ඉගෙනුම් ප්‍රතිඵල

මෙම මොඩියුලය අවසන් වන විට ඔබට පහත දැක්වෙන කරුණු සම්බන්ධයෙන් අවබෝධයක් තිබිය යුතු ය:

- සයිබර් ආරක්ෂාව අදාළ වන්නේ පද්ධති සහ දේවල්වලටයි; සයිබර් සුරක්ෂිතබව මිනිසුන්ට අදාළ ය.
- ඩිජිටල් සහ සයිබර් ආරක්ෂාව පරිශීලකවරයාත්, තාක්ෂණ සේවා සපයන්නාත් අතර බෙදාහදාගත් වගකීමකි. යහපත් ඩිජිටල් සහ සයිබර් ආරක්ෂාව සඳහා පරිශීලක මැදිහත්වීම, වගකීම සහ අවධානය අවශ්‍ය ය.
- ශක්තිමත් මුරපද, පියවර දෙකේ තහවුරුකරණය, දත්ත එන්ක්‍රිප්ට් කිරීම සහ ස්ථාවර දත්ත බැකප් කිරීම යනු සෑම පරිශීලකවරයකු හෝ ඩිජිටල් සේවාවක් විසින් ම අනුගමනය කළ යුතු පූර්වාරක්ෂක පියවරකි. ඒවා අත්‍යවශ්‍ය ඩිජිටල් වගකීමෙහි කොටස් වේ. ඒවාට ඩිජිටල් සනීපාරක්ෂාව යයි ද කියනු ලැබේ.
- ඩිජිටල් සහ සයිබර් ආරක්ෂාව නැංවීම සම්බන්ධයෙන් නොමිළේ අන්තර්ජාලයෙන් ලබාගත හැකි උපදෙස් බොහෝ ය. කෙසේ වෙතත්, මේ සම්බන්ධයෙන් වඩාත් වැදගත් ක්‍රියාවලිය වන්නේ ඔබ හෙවත් පරිශීලකයා ම ය.

වැඩිදුර කියවීම්

Good Digital Hygiene: A guide to staying secure in cyberspace
Book by Ed Gelbstein (2013)
http://index-of.co.uk/IT-managment/good-digital-hygiene.pdf

නෝටන් අන්තර්ජාල ආරක්ෂක උපදෙස්
https://us.norton.com/internetsecurity

ගූගල් උපකාරක මධ්‍යස්ථානය (ගූගල් ගිනුමක් හිමි අයට පමණි)
https://support.google.com/

Security in-a-Box, a guide to digital security for activists and human rights defenders
https://www.frontlinedefenders.org/en/digital-security-resources

Umbrella is digital and physical security for people at risk on your Android phone
https://secfirst.org/

Information security handbook for journalists
http://www.tcij.org/resources/handbooks/infosec

Electronic Frontier Foundation's Surveillance Self Defence
https://ssd.eff.org/en

Tips on good digital hygiene
https://wiobyrne.com/digital-hygiene/

Digital security for activists, by the Electronic Intifada
https://electronicintifada.net/content/guide-online-security-activists/17536