Community Resilience to Foreign Interference

National Cyber Security Centre

අන්තර්ජාලයේ ආරක්ෂිතව කටයුතු කිරීම

මට අන්තර්ජාල ආරක්ෂාව වැදගත් වන්නේ ඇයි?

අන්තර්ජාලය සහ සමාජ මාධ්‍ය යනු අපට තොරතුරු බෙදා ගැනීමට සහ මිතුරන් සහ පවුලේ අය සමඟ සම්බන්ධතා පවත්වා ගැනීමට උපකාරී වන ප්‍රයෝජනවත් වේදිකා වේ.

කෙසේනමුත්, අපරාධකරුවන් සහ අනෙකුත් නීති විරෝධී සංවිධාන ඔබේ මුදල්, ඔබේ තොරතුරු ලබා ගැනීමට හෝ ඔබව බිය ගැන්වීමට ඒවා භාවිතා කරයි.

ඔවුන්ට ලෝකයේ ඕනෑම තැනක සිට ක්‍රියාත්මක විය හැකි අතර, බොහෝ භාෂා චතුර ලෙස කතා කළ හැකි අතර ඒත්තු ගැන්වෙන ව්‍යාජ වෙබ් අඩවි නිර්මාණය කළ හැකිය. ඔවුන් ඔබව ඊමේල්, සමාජ මාධ්‍ය සහ කෙටි පණිවිඩ හරහා සම්බන්ධ කර ගන්නා අතර ඔබට බියක් හෝ කනස්සල්ලක් ඇති කිරීමට උත්සාහ කරනු ඇත, එවිට ඔබ නිවැරදි තීරණ නොගනී.

මේ සියල්ලෙන් අදහස් වන්නේ ඔබ සූදානම්ව සිටිය යුතු බවත් ඔවුන් භාවිතා කරන උපක්‍රම පිළිබඳව සැමවිටම දැනුවත් විය යුතු බවත්ය.

මට අන්තර්ජාලය හරහා මුහුණ දීමට සිදුවිය හැකි පොදු ගැටළු මොනවාද?

මේවා අපට බහුලව දක්නට ලැබෙන තත්වයන් කිහිපයකි.

- **ඔබට ලින්ක් එකක් ක්ලික් කරන ලෙස ඉල්ලා සිටින සැක සහිත ඊමේලයක් හෝ කෙටි පණිවිඩයක් ලැබේ.**
  මෙම ලින්ක් බොහෝ විට ඔබගේ ලොගින් හෝ මූල්‍ය තොරතුරු සොරකම් කිරීම සඳහා නිර්මාණය කර ඇති ව්‍යාජ වෙබ් අඩවි වලට යොමුකරයි.
- **ඔබේ පුද්ගලික තොරතුරු ඉල්ලා සිටින සැකසහිත ඇමතුමක් ලැබේ.**
  ඉහත අයුරින්ම අමතන්නා ඔබේ බැංකුවෙන් බව පවසා ඔබෙන් තොරතුරු ඉල්ලා සිටී.

- **බලධාරියෙකු ලෙස පෙනී සිටිමින්, ඔබට යමක් කිරීමට බල කිරීමට උත්සාහ කරන කෙනෙකුගෙන් ඔබට දැනුම්දීමක් ලැබේ.**
  බොහෝවිට පුද්ගලයා යම්කිසි තර්ජනයක් සිදුකරයි.

- **කෙනෙකු ඔබගේ මාර්ගගත ගිණුම් එකකට හෝ කිහිපයකට .ඇතුළු වේ (ඊමේලය හෝ සමාජ මාධ්‍ය :උදාහරණයක් ලෙස)**
  යමෙකු ඔබගේ මාර්ගගත ගිණුමට ඇතුළු වුවහොත් ඔවුන්ට තොරතුරු සොරකම් කිරීමට, ගෙවීම් නැවත හරවා යැවීමට සහ ඔබ ලෙස පෙනී සිටිමින් ඔබේ මිතුරන් හෝ පවුලේ අය ඉලක්ක කිරීමට හැකිය.

- **ඔබගේ ක්‍රෙඩිට් කාඩ්පත් තොරතුරු සොරකම් කර ඇත, නැතහොත් ව්‍යාජ විකිණීමකින් හෝ ආයෝජනයකින් ඔබ වංචා කර ඇත.**
  වංචාකරුවන් බලාපොරොත්තු වන්නේ ඔබට හොඳ වාසියක් ඇති බව සිතා වැඩිදුර සිතීමකින් තොරව ගෙවීමට පෙළඹීමයි. එසේ නැත්නම් සත්‍ය වෙබ් අඩවියක දත්ත පිටවීමකට ලක්වී ඔබේ දත්ත අන්තර්ජාලයට පිටවී ඇත.

මෙහි තවත් අවස්ථා දක්වා ඇත: දැන්මසහයලබාගන්න– ඔබේමඅන්තර්ජාලයකට

මම අන්තර්ජාලයේ ආරක්ෂිතව සිටින්නේ කෙසේද?

දිගු සහ විශේෂිත මුරපද භාවිතය.

- මුරපදය දිගුවන තරමට, එහි ප්‍රබලත්වයද වැඩිවේ.

- අහඹු වචන හතරක් එකට එකතු කිරීමෙන් අක්ෂර 16 කට වඩා වැඩි මතක තබා ගත හැකි මුරපදයක් සාදන්න (උදාහරණයක් ලෙස: TriangleRhinoOperationShoes) සහ අවශ්‍ය නම් අංක, ලොකු අකුරු සහ සංකේත එකතු කරන්න (උදාහරණයක් ලෙස: Triangle&"Rhino"Operation2Shoes).

- වැදගත්ම දෙය, ඔබේ මුරපදය නැවත නැවත භාවිතා කරන්න එපා. අපරාධකරුවෙකුට ඔබේ මුරපද එකක් ලැබුනොත්, ඔවුන් වෙනත් ගිණුම්වලත් එය උත්සහ කරයි.

- ඔබගේ මුරපද මතක තබා ගැනීමට සහ නව මුරපද නිර්මාණය කිරීමට මුරපද කළමනාකරණ මෘදුකාංගයක් භාවිතා කරන්න.

- හොඳ මුරපද සකසන්න – ඔබේ අන්තර්ජාල අයිතිය හිමි කරගන්න

පියවර දෙකක සත්‍යාපන සක්‍රීයව තබාගන්න.

- මෙය ඔබට වෙබ් අඩවියකට පිවිසීමට අවශ්‍ය අමතර තොරතුරු කොටසකි – සාමාන්‍යයෙන් ඔබේ දුරකථනයේ කේතයකි.
- මෙම ක්‍රමය ඉතාමත් ප්‍රතිඵල අතර ඔබේ ගිණුමට ඇතුල්වීමේ අවස්ථා බොහොමයක් වැලැක්විය හැකිය.
- සහය දක්වන අවස්ථාවලදී 'සත්‍යාපන යෙදුමක්' භාවිතා කිරීමට අප යෝජනා කරන්නෙමු.
- පියවර දෙකක සත්‍යාපනය (2FA) සකසන්න – ඔබේ අන්තර්ජාල අයිතිය හිමි කරගන්න

අන්තර්ජාලයේදී පුද්ගලිකව සිටින්න.

- සමාජ මාධ්‍ය තුළ ආරක්ෂිතව සිටීමට හොඳම විකල්පය වන්නේ ඔබේ රහස්‍යතා පෞද්ගලිකත්ව සැකසුම් සක්‍රීය කර තිබීමයි.
- මෙය සයිබර් අපරාධකරුවන් ඇතුළු අහඹු පුද්ගලයින්ට ඔබගේ සටහන් පෝස්ටු දැකීම හෝ ඔබට පණිවිඩ යැවීම නවත්වනු ඇත.
- තවදුරටත් ඔබ, ඔබේ පවුලේ අය හෝ මිතුරන් පිළිබඳ පුද්ගලික තොරතුරු පළ කිරීමේදී ප්‍රවේශම් වන්න.
- සබඳතා ඔවුන් පෙන්වන අයම බව තහවුරු කරගන්න.
- බොරු මිතුරු ඇරයුම් සඳහා අවධානයෙන් සිටින්න. මාධ්‍යවේදීන් යැයි කියා ගන්නා පුද්ගලයින්ගෙන් හෝ ඔබ හොඳින් නොදන්නා අයගෙන් ප්‍රවේශම් වන්න.
- අන්තර්ජාලයේ ඔබේ පෞද්ගලිකත්වය ආරක්ෂා කරගන්න – ඔබේ අන්තර්ජාල අයිතිය ලබා ගන්න

සියල්ල යාවත්කාලීනව තබාගන්න.

- ඔබ ඔබේ දුරකථනය, පරිගණකය හෝ මෘදුකාංගය යාවත්කාලීන කරන විට, එය ආරක්ෂාවේ ඇති ඕනෑම හිඩැසක් ද පුරවයි.
- අපරාධකරුවන් සැමවිටම ඇතුළුවීමට ක්‍රම සොයමින් සිටින අතර යාවත්කාලීන කිරීම් මඟින් අවදානම් නිවැරදි කරයි.
- ඔබේ උපාංග නිරතුරුව රීස්ටාර්ට් කරන්න.

- [ඔබේ යාවත්කාලීන කිරීම් සමඟ යාවත්කාලීනව සිටින්න – ඔබේ අන්තර්ජාල අයිතිය ලබා ගන්න]()

වංචාවන් පිළිඹද අවධානයෙන් සිටින්න.

- හොඳම උපදෙස නම් මෙම වංචාවන් පිළිබඳව දැනුවත් වී ඒවා ගැන විමසිල්ලෙන් සිටීමයි.
- යම් දෙයක් වැරදි බව පෙනේ නම්, ඔබව සම්බන්ධ කර ගත් පුද්ගලයා සමඟ සම්බන්ධ නොවන්න. ඔවුන් මිත්‍රශීලී බවක් පෙනුනත්, මුදල් ඉල්ලුවොත් විශේෂයෙන් ප්‍රවේශම් වන්න.
- අමුතු සබැඳි සහ ඊමේල් ලිපින පිළිබඳ සැලකිලිමත් වන්න (උදාහරණයක් ලෙස: ඔබේ බැංකුව ඔබට Gmail ගිණුමකින් ඊමේලයක් එවන්නේ නැත).
- *කිසිම අවස්ථාවක* කෙටි පණිවිඩවල සඳහන් සබැඳි ක්ලික් කරන්න එපා.
- නිල ඇප් ස්ටෝර් වලින් පමණක් යෙදුම් බාගත කරගන්න.
- සැකයක් ඇත්නම්, ඔබව සෘජුවම සම්බන්ධ කරගත් සංවිධානය අමතන්න, ඔබට එවන ලද කිසිදු සබැඳියක් හෝ දුරකථන අංකයක් අනුගමනය නොකරන්න.
- ඔබට, ඔබේ ප්‍රජාවට සහ ඔබ අයත් ඕනෑම කණ්ඩායමකට සබැඳි ආරක්ෂක අවදානම් පිළිබඳව දැනුවත්ව සිටීමට උත්සාහ කරන්න.

ඔබේ තොරතුරු ආරක්ෂා කරගන්න.

- Signal වැනි සංකේතනය කළ පණිවිඩ යැවීමේ යෙදුම් භාවිතා කරන්න. මෙමඟින් වෙනත් අයෙක් ඔබේ පණිවිඩ බැලීම වලක්වයි.
- වෙබ් ලිපිනය HTTPS ලෙස ආරම්භ වන වෙබ් අඩවි සමඟ පමණක් තොරතුරු බෙදාගන්න. S අකුරෙන් "Secure (ආරක්ෂිත)" යන්න අදහස් වන අතර එයින් අදහස් වන්නේ ඔබ සහ වෙබ් අඩවිය අතර යවන ඕනෑම තොරතුරක් සංකේතනය කර ඇති බවයි.
- ඔබේ දත්ත ආරක්ෂා කර ඔබේ ස්ථානය සැඟවිය හැකි අතථ්‍ය පෞද්ගලික ජාලයක් (VPN) භාවිතා කිරීම සලකා බලන්න.
- ඔබේ යෙදුම්වලට අවසර දී ඇති දත්ත සහ අවසර පරීක්ෂා කරන්න. උදාහරණයක් ලෙස, සෞඛ්‍ය පිළිඹද යෙදුමකට ඔබේ සබඳතාවලට ඇතුල්වීමට අවශ්‍ය නැත.

Community Resilience to Foreign Interference

මම වංචාවකට හසුවුවහොත් හෝ වඩාත් බරපතල යමක් සිදුවුවහොත් සිදුකළ යුත්තේ කුමක්ද?

සහය ලබාගැනීමට ඔබට යා හැකි ස්ථාන රාශියක් ඇත. ඔබ ඔබේ කැමැත්ත ලබා දෙන්නේ නම් මිස, මෙම සංවිධාන ඔබේ තොරතුරු වෙනත් කිසිවෙකු සමඟ බෙදා නොගනු ඇත.

ඔබට CERT NZ ද්වාරය හරහා NCSC වෙත සයිබර් සිදුවීම් වාර්තා කළ හැකි අතර අපට ඔබට උදව් කිරීමට හෝ වෙනත් ආයතනයක් සමඟ සම්බන්ධ කිරීමට හැකිය: [සිදුවීමක් වාර්තා කරන්න | CERT NZ]

ඔබේ මුදල් නැතිවූයේ නම්, වහාම ඔබේ බැංකුව සම්බන්ධ කරගන්න.

අභ්‍යන්තර කටයුතු දෙපාර්තමේන්තුව විසින් පවත්වාගෙන යනු ලබන සේවාවක් වන 7726 වෙත වංචා කෙටි පණිවිඩ නොමිලේ යොමු කළ හැක.