Community Resilience
to Foreign Interference

National Cyber Security Centre

අන්තර්ජාලයේ ඔබේ ආයතනය ආරක්ෂිතව තබාගැනීම

අන්තර්ජාල ආරක්ෂාව ප්‍රජා කණ්ඩායම් සහ සංවිධානවලට වැදගත් වන්නේ ඇයි?

මෙම පිටුවේ ඔබේ ප්‍රජා කණ්ඩායම හෝ සංවිධානය අන්තර්ජාල ආරක්ෂණ තර්ජන වලින් ආරක්ෂා කර ගැනීම සඳහා උපදෙස් සහ ඔබට ගත හැකි පියවර කිහිපයක් අඩංගු වේ. පුද්ගලයින් සඳහා වෙනම මාර්ගෝපදේශයක් ඇත.

මෙම උපදෙස් සකසා ඇත්තේ වඩාත් බහුල හා බරපතල තර්ජන පිළිබඳවයි.

යාවත්කාලීන කිරීම්

ආරක්ෂාවට ඇති ඕනෑම අඩුපාඩුවක් ඉවත් කිරීමට ඔබගේ උපාංගවල මෘදුකාංග යාවත්කාලීනව තබා ගන්න

- ඔබේ ප්‍රජා කණ්ඩායමේ හෝ සංවිධානයේ උපාංග යාවත්කාලීනව තබා ගන්න. මෙයට දුරකථන, පරිගණක, WiFi රවුටර සහ අන්තර්ජාලයට සම්බන්ධ වන ස්මාර්ට් උපාංග ඇතුළුව වෙනත් ඕනෑම දෙයක් ඇතුළත් වේ.
- හැකි සෑමවිටම ස්වයංක්‍රීය යාවත්කාලීනකිරීම් භාවිතා කරන්න.

ද්වි-සාධක සත්‍යාපනය (2FA)

මුරපදයක් සහ ඔබගේ දුරකථනයේ යෙදුමකින් කේතයක් වැනි තවත් පියවරක් අවශ්‍ය කිරීමෙන් ඔබගේ ගිණුම්වලට අමතර ආරක්ෂාවක් එක් කරයි.

- සටහන: මෙය බහු-සාධක සත්‍යාපනය (MFA), ද්වි-පියවර සත්‍යාපනය (2SV) සහ තවත් බොහෝ නම් ලෙස හැඳින්වේ.

- ඔබගේ සියලුම ප්‍රජා කණ්ඩායම් හෝ සංවිධානයේ ගිණුම්වල 2FA ක්‍රියාත්මක කරන්න.
- හැකි නම්, තතුබෑම් (phishing) වලට ප්‍රතිරෝධී 2FA ආකාරයක් භාවිතා කිරීමට උත්සාහ කරන්න, එයින් ඔබව රැවටීමට ලක් කර එය ලබා දිය නොහැකි බව තහවුරු කෙරේ. මෙය භෞතික ආරක්ෂක යතුරක් හෝ ඇඟිලි සලකුණු හෝ මුහුණු හැඳුනුම්පතක් (Face ID) වැනි දෙයක් විය හැකිය.

ඔබගේ සබැඳි ගිණුම් නිරීක්ෂණය කරන්න

ප්‍රජා කණ්ඩායමෙන් හෝ සංවිධානයෙන් ඉවත් වූ පසු හිටපු සාමාජිකයින් ගිණුම් වෙත ප්‍රවේශය තබා නොගන්නා බවට වග බලා ගන්න.

- එකම ගිණුමට එක් අයෙකුට වඩා පිවිසෙන්නේ නම්, ඔවුන් සියලු දෙනාටම වෙනස් පිවිසුම් ඇති බවත්, සියල්ලන්ටම 2FA සක්‍රීය කර ඇති බවත් සහතික කර ගන්න.
- සියලුම පරිශීලක ගිණුම් ලැයිස්තුවක් තබාගෙන කාර්ය මණ්ඩලය ඉවත්වන විට ?අවශ්‍ය නොවන ඒවා අක්‍රිය කරන්න.
- ඔබ ඔබේ සාමාජිකයින්ට ලබා දී ඇති ඕනෑම උපාංගයක ලේඛනයක් තබා ගන්න, එම පුද්ගලයා සංවිධානයෙන් ඉවත් වුවහොත් ඒවා නැවත ලබාගෙන කර්මාන්තශාලා සැකසුම් වෙත නැවත සැකසීමට මතක තබා ගන්න. ගොඩනැගිලි ප්‍රවේශය සඳහා භෞතික කේත වෙනස් කිරීමටද ඔබට අවශ්‍ය විය හැකිය.

ඔබේ මාර්ගගත ගිණුම්වලට ප්‍රවේශය ඇත්තේ කාටදැයි පරීක්ෂා කරන්න

ඔබේ ප්‍රජා කණ්ඩායමේ හෝ සංවිධානයේ පුද්ගලයින්ට ප්‍රවේශය තිබිය යුත්තේ ඔවුන්ට අවශ්‍ය දේවල් සඳහා පමණි.

- එක් පුද්ගලයෙකුගේ ගිණුමක් 'හැක්' (hack) වුවහොත්, මෙම පියවර මඟින් ප්‍රහාරකයෙකුට කළ හැකි හානිය සීමා කරයි.
- අනවශ්‍ය අවසරයන් නිතිපතා පරීක්ෂා කර ඉවත් කරන්න.
- ඔබට බහු පුද්ගලයින් භාවිතා කරන තනි "පරිපාලක" ගිණුමක් තිබේ නම්, අසාමාන්‍ය ක්‍රියාකාරකම් සඳහා එය නිරීක්ෂණය කරන්න. විශේෂයෙන්ම දෛනික කාර්යයන් සඳහා මෙවැනි ගිණුම් භාවිතය සීමා කිරීමට උත්සාහ කරන්න.
- මෙම නීති රවුටර වැනි උපාංග වෙත පරිපාලක ප්‍රවේශයට ද අදාළ වේ.

ඔබ වෙනුවෙන් IT සේවා පවත්වාගෙන යාමට යමෙකු සේවාවට ගෙන තිබේ නම්

සේවා සපයන්නන් සමඟ ඔබේ ගිවිසුම් සමාලෝචනය කරන්න.

- ඔබේ ප්‍රජා කණ්ඩායමේ හෝ සංවිධානයේ අවශ්‍යතා සපුරාලීම සඳහා ඔවුන්ට අන්තර්ජාල ආරක්ෂණ ක්‍රමවේද ඇති බවට වග බලා ගන්න.

ඔබගේ සියලුම ගිණුම් සහ පද්ධති එකට ක්‍රියා කරන ආකාරය දැන ගන්න

සම්බන්ධතා තේරුම් ගැනීම ප්‍රහාරකයෙකුට ඇතුළු විය හැකි ස්ථානය හඳුනාගැනීමට උපකාරී වේ.

- ඔබගේ පද්ධති අතර සම්බන්ධතා සමාලෝචනය කරන්න, උදාහරණයක් ලෙස, ඊමේල්, ක්ලවුඩ් ස්ටොරේජ් (cloud storage) සහ ගිණුම්කරණ වේදිකා.
- අමතර මාර්ගගත ආරක්ෂාව සඳහා අතථ්‍ය පුද්ගලික ජාලයක් (VPN) භාවිතා කිරීම සලකා බලන්න. VPN එකක් භාවිතා කිරීමෙන් ඔබව නිරීක්ෂණය කිරීමට උත්සාහ කළ හැකි ඕනෑම අයෙකුගෙන් ඔබගේ සබැඳි ක්‍රියාකාරකම් සඟවයි. ඔබේ ප්‍රජා කණ්ඩායමේ හෝ සංවිධානයේ ඕනෑම සාමාජිකයෙකු දුරස්ථව සම්බන්ධ වන්නේ නම් මෙය විශේෂයෙන් අවශ්‍ය වේ.

ඔබේ ජනතාව 'සයිබර් බුද්ධිමත්' ලෙස තබා ගන්න

ඔබේ පද්ධතිවලට වඩා ඔබේ ප්‍රජා කණ්ඩායමේ හෝ සංවිධානයේ පුද්ගලයින් ඉලක්ක කර ගැනීමට ඉඩ තිබේ.

- ඔබේ සේවකයින්ව මූලික අන්තර්ජාල ආරක්ෂාව පිළිබඳ පුහුණු කරන්න. ඔබේම අන්තර්ජාල වෙබ් අඩවිය ඔබේ අන්තර්ජාල අයිතිය ලබා ගන්න |NCSC හි ඔබව මාර්ගගත ආරක්ෂිතව තබා ගැනීමට සහ වංචා හඳුනා ගන්නේ කෙසේද යන්න පිළිබඳ පුළුල් පරාසයක උපදෙස් සහ ඉඟි ඇත.
- මෙය ඔවුන්ගේ පුද්ගලික ගිණුම් සඳහා මෙන්ම ඔවුන් ඔබේ සංවිධානය සඳහා භාවිතා කරන ගිණුම් සඳහාද වැදගත් බව ඔවුන්ට මතක් කර දෙන්න.
- පුද්ගලයන් සඳහාද අප සතුව උපදෙස් තිබේ. අන්තර්ජාලයෙහි ආරක්ෂිතව සිටීම | ජනවාර්ගික ප්‍රජා අමාත්‍යාංශය Keeping safe online

අවදානම් අවස්ථාවක් සඳහා සැලසුම් කරන්න

සිදුවීමක් සිදු වූ විට ජනතාව භීතියට පත්වීම වළක්වා ගැනීම සඳහා ප්‍රතිචාර සැලැස්මක් තිබීම වැදගත් වේ.

- අවධානම් සිදුවීමක් අතරතුර කවුරුන් කුමක් කරන්නේද යන්න සිදුවීම් ප්‍රතිචාර සැලැස්මක් මඟින් දක්වයි. සිදුවීම් කළමනාකරණය |NCSC සඳහා සැකිලි මෙහි ඇත.
- දුරකථන, පරිගණක හෝ වෙනත් පද්ධති අසමත් වුවහොත් කුමක් කළ යුතුද යන්න පිළිබඳ සැලැස්මක් ඇතුළත් කරන්න. මෙම සැලැස්ම යාවත්කාලීනව තබාගන්න.
- අවශ්‍ය සියලු දෙනාගේ සම්බන්ධතා තොරතුරු තබා ගන්න සහ ඔවුන් සම්බන්ධ කර ගැනීමට ප්‍රධාන ක්‍රමය අක්‍රීයව ඇත්නම් (ඊමේල් වැනි) අමතර තොරතුරු තබා ගන්න.
- ඔබට එයට ළඟා විය නොහැකි නම්, සැලැස්ම ඔබේ පද්ධතියෙන් පිටත කොතැනක හෝ තබා ගන්න.