# ෆේස්බුක් සුරක්ෂිතව භාවිතා කරන්නේ කෙසේද?

ෆේස්බුක් යනු, ලොව ජනප්‍රියතම සමාජයීය ජාලයකි. සමාජයීය ජාලයක් යනු, පුද්ගලයින් අන්තර්ජාලය මාර්ගයෙන් සමාජ සබඳතා පවත්වාගෙන යෑමේ ක්‍රමවේදයකි.

මෙහි දී ඔවුන් වැඩිපුර ඡායාරූප හුවමාරු කිරීම, වීඩියෝ හුවමාරුව හා එදිනෙදා කටයුතු පිළිබඳ තොරතුරු හුවමාරු කර ගැනීම සිදුකරයි. සංඛ්‍යාලේඛනවලට අනුව, වර්තමානයේ මිලියන 300 කට අධික පිරිසක් විසින් ෆේස්බුක් භාවිතා කරන අතර, දිනකට මිනිත්තු බිලියන 6 කට වැඩි කාලයක් ෆේස්බුක් ජාලය තුල ගත කරයි.

මෑතක දි කරන ලද සමීක්ෂණ වලට අනුව ෆේස්බුක්හි ජනප්‍රියතාවය සඳහා ප්‍රධාන වශයෙන් බලපාන කරුණු ලෙස පහත කරුණු දක්වා ඇත.

- පරිශීලකයින්ට අසීමිත ඡායාරූප හා වීඩියෝ ප්‍රමාණයක් ෆේස්බුක් වෙත එක් කිරීමටත්, ඒවා තම මිතුරන් හා හුවමාරු කරගැනීමටත් හැකිවීම.
- පරිශීලකයන්ට, එදිනෙදා සෑම මිනිත්තුවකදී ම පාහේ තම මිතුරන් යෙදී සිටින කාර්යයන් පිළිබඳ දැනගත හැකිවීම.
- ෆේස්බුක් හි තම මිතුරන් සමඟ අන්තර්ජාලික ක්‍රීඩා වලදී තරඟ වැදිමට හැකි වීම.
- මිතුරනට ඉ-තෑගි (හෝ විදළුත් තෑගි) යැවිය හැකි වීම

කෙසේ නමුදු සෑම තාක්ෂණයක ම දුර්වලතා පවතින්නාක් මෙන් ෆේස්බුක්හිදීද, පුද්ගලික නිදහස පිළිබඳ ගැටලු පවතී. පසුගිය වසර 3-4 තුළ දි ෆේස්බුක් භාවිතා කරන්නන් එල්ල කරගෙන සිදුකරන ලද ප්‍රහාර වැඩි වූ අතර ඒ හේතුවෙන් ඔවුන්ගේ පුද්ගලිකත්වයට තර්ජනයක් විය.

අන්තර්ජාලය ආශ්‍රිත ව සමාජයීය ජාලකරණය ඔබ පිළිබඳ, ඔබගේ කටයුතු පිළිබඳ, ඔබ සිටින ස්ථානය හා ඔබ ඇසුරු කරන්නන් යනාදිය පිළිබඳ ව තොරතුරු අනෙකුත් පුද්ගලයින්ට දැනගැනිමට සලසයි. මෙම තොරතුරු වලට ඔබගේ ජීවිතය අවදානමට ලක් කිරීමට වුවද හැකිය.

ෆේස්බුක් වැනි සමාජයීය ජාල ආශ්‍රිත වෙබ් අඩවි තුල සුරක්ෂිත ව රැඳී සිටීමට ඔබට විවිධාකාර ක්‍රම අනුගමනය කළ හැකිය. පහත සඳහන් වන්නේ එවැනි ක්‍රම කිහිපයකි.

1. https://www.facebook.com භාවිතා කරමින් ෆේස්බුක් වෙත ලොග්වන්න. රහස් වචනය (මුර පදය) සොරා ගැනීමෙන් ඔබගේ ජාලය තුලට හොරෙන් ඇතුලුවන්නන්ගෙන් ආරක්ෂා වීමට මෙය උපකාරී වේ.
2. කෙටි පණිවුඩ මත පදනම් වූ තහවුරු කිරීම භාවිතා කිරීම. (මෙම ක්‍රමය ක්‍රියාත්මක කළ විටදී ෆේස්බුක් වෙතට ඇතුල් වීමට පෙර ඇතුල් කළ යුතු කේතයක් කෙටි පණිවිඩයක් ලෙස ඔබට එවනු ලැබේ.)
3. ෆේස්බුක් වෙත ලබා දෙන ඔබගේ පුද්ගලික තොරතුරු සීමා කරන්න. (විශේෂයෙන් ම ඔබගේ වාසස්ථානය, උපන්දිනය ආදී පුද්ගලික තොරතුරු) පෞද්ගලිකත්ව සැකසුම් (Privacy Settings) මගින් ජනතාවට විවෘත වන තොරතුරු ප්‍රමාණය අවම කළ හැකියි.
4. ෆේස්බුක් වෙතට ඇතුල් වීමේදී ඔබගේ විද්‍යුත් තැපැලට ඒ පිළිබඳ ව දැනුම් දීමක් (Notification) ලැබෙන ලෙස පෞද්ගලිකත්ව දත්ත සැකසුම සකසන්න.
5. නව මිතුරන් එකතුකර ගැනීමේ දි, මුලින් ම ඔවුනට ඔබ පිළිබඳ සීමිත තොරතුරු පෙන්වන පරිදි පෞද්ගලිකත්ව දත්ත සැකසුම සකස් කොට ඔවුන් එකතු කරගන්න. පසුව, ඔවුන් පිළිබඳ දැඩි සෝදිසියකින් පසුවන්න.

6. ෆේස්බුක් ජාලය සේ අනුකරණය කර සාදන ලද ව්‍යාජ වෙබ් අඩවි ඇති නිසා නිතරම වෙබ් අඩවියකට තම තොරතුරු සැපයීමට පෙර සැලකිලිමත් වන්න.

පිෂින් විද්‍යුත් තැපැල් පණිවිඩයක් යනු පරිශීලකයා විසින් ක්ලික් කළ පසු ඔබගේ කිසිදු අනුදැනුමකින් තොරව වයිරස ඉබේම බාගත වී ඔබගේ පරිගණකයට ස්ථාපනය වීම සඳහා විශේෂයෙන් නිර්මාණය කරන ලද්දකි.
ඔබගේ ඇතුල්වීම් තොරතුරු ලබාගැනීමේ අදහසින් නිම වූ සමහර සබැඳි මගින් ෆේස්බුක් වැනිම වූ ව්‍යාජ අතුරු මුහුණතකට ඔබ රැගෙන යා හැක.

ඔබ https://www.facebook.com භාවිතා කරමින් ෆේස්බුක් වෙත ඇතුලු වීමේ දි ලබා දෙන ඩිජිටල් සහතිකය නිරීක්ෂණය කිරීමෙන් ඔබට මෙම අඩවියේ සත්‍යතාවය පරීක්ෂා කළ හැක. ෆේස්බුක් වෝල්, ෆීඩ්ස් සහ පණිවිඩවල අන්තර්ගත සබැඳි මත ක්ලික් කිරීමෙන් ද මේ හා සමාන සිදුවීම් සිදුවිය හැක.

7. ඔබගේ මිතුරෙකු හෝ මිතුරියක ලෙස පුද්ගලයෙකු එකතු කර ගැනීමට පෙර දෙවරක් සිතන්න. ඔහු/ඇය සැබවින් ම ඔබට මිතුරු ආරාධනයක් එවා ඇත්දැයි ඔහුට/ඇයට විද්‍යුත් තැපැල් පණිවිඩයක් යැවීමෙන් හෝ දුරකථන ඇමතුමක් ලබා දීමෙන් ඔවුන් සමග තහවුරු කරගන්න.
8. ෆේස්බුක් මාර්ගයෙන් Chat කිරීමද කලහැක. ඔබ නොහඳුනන සහ සැක සහිත පුද්ගලයන් හා සංවාදයේ යෙදීමෙන් වලකින්න. එමෙන් ම ඔබව හඳුනාගත හැකි තොරතුරු සංවාද හරහා ලබාදීම කිසිවිටෙක නොකරන්න. කරදරකාරී පුද්ගලයෙකු සිටී නම් වහාම ඒ තැනැත්තාව මිතුරන් අතරින් ඉවත් කරන්න.
9. කිසිවෙකුටත් අනුමාන කළ නොහැකි, ශක්තිමත් මුර පදයක් භාවිතා කරන්න. එමෙන් ම එය නිතර මාරු කිරීමටත් වග බලාගන්න. එමෙන් ම, ඔබගේ විද්‍යුත් තැපෑලට හෝ වෙනත් මාර්ගගත උපයෝගීතාවයන් සඳහාත්, ෆේස්බුක් සඳහාත් එකම මුරපදය භාවිතා නොකරන්න.
10. විශ්වාසනීය පරිගණකයක් භාවිතා කිරීමෙන් පමණක් ෆේස්බුක් වෙත පිවිසෙන්න. මක්නිසා ද යත්, ඔබ භාවිතා කරන සියලුම තොරතුරු සටහන් කරගන්නා, Key loggers වැනි මෘදුකාංග සහිත පරිගණක තිබිය හැකි බැවිණි.
11. ඔබගේ මුරපදය හුවමාරු කරගන්නේ කවුරුන් සමඟද යන්න පිළිබඳ ව සැලකිලිමත් වන්න. ඔබ දුර්වල මුරපදයක් භාවිතා කළහොත් එය ලෙහෙසියෙන් හෙළිදරව් විය හැකිය.

සමාජයීය ජාලයක් මගින් ලබන අත්දැකීම් ඔබව අමන්දානන්දයට පත්කරයි. නමුත් සමහරක් විට දී විවිධ තැනැත්තන් තමනුත්, තම මිතුරනුත්, අනතුරට ලක් විය හැකි පරිදි අනාරක්ෂිත ලෙස හැසිරෙති. එමනිසා TechCERT ආයතනය විසින් ඔබ දැනුවත් කර ඇති පරිදි ක්‍රියා කිරීමෙන්, ෆේස්බුක් භාවිතයේ දී සිදුවිය හැකි තර්ජනයන් අවම කරගැනීමට ක්‍රියාකරන ලෙස අප ඔබගෙන් ඉල්ලා සිටිමු.

ඔබට ෆේස්බුක් සිදුවීම් සම්බන්ධයෙන් යම් උපදෙසක් අවශ්‍ය නම් කරුණාකර පහත ලිපිනයෙහි ඇති අපගේ ලේඛනය පුරවා අදාල සිදුවීම් පිළිබඳ අපට වාර්තා කරන්න.

ඔබගේ ගැටලු පහත ක්‍රමයන් මගින් අපට දන්වන්න.

https://techcert.lk/en/report-form
දුරකථන - +94 11 4 462 562
ඉ-තැපැල් - help@techcert.lk

මෙම ලිපිය ලක් වසම් අධිකාරිය සහ අන්තර්ජාල සමාජයේ ශ්‍රී ලාංකීය ශාඛාව එක්ව සකසන ලද්දකි.
වැඩි විස්තර සඳහා පිවිසෙන්න. http://nic.lk/index.php/training-materials.