இணையவெளிப் பாதுகாப்பு

நாளைய தலைமுறைக்கான இணையவெளிப் பாதுகாப்புக் கையேடு

ஹிதவத்தியிடமிருந்து

இணையவெளிப் பாதுகாப்பு

ஹிதவதியிடமிருந்து

சைபர் சுரெகும

இணையவெளிப் பாதுகாப்பு
ஹிதவதியிடமிருந்து

அக்டோபர் 2024

ISBN 978-624-5622-06-1

அட்டை வடிவமைப்பு: புஷ்பானந்த ஏகநாயக்க
ஓவியம் : தனஞ்சா சுபசிங்க
தகவல் அமைப்பு : தம்பரு விஜேசேகர

இந் நூல் ஆக்கப்பூர்வ பொது அனுமதிப்பத்திரத்தின் (Creative Commons License) கீழ் இலங்கைத் தகவல் தொடர்பாடல் தொழில்நுட்ப முகவர் நிறுவனத்தினால் வெளியிடப்பட்ட “AdBhashitha” (யுனிகோட்) எழுத்துருவை பயன்படுத்தி பிரசுரிக்கப்பட்டுள்ளது.

வெளியீடு

இலங்கை தள பதிவாளர்
பெர்னார்ட் வணிக பூங்கா
106, துடுகெமுனு வீதி, தெஹிவளை.

முழுப்பதிப்புரிமையும் உடையது

முதலாம் பதிப்பு: ஆகஸ்ட் 2021
இரண்டாம் பதிப்பு: பெப்ரவரி 2024

தொலைபேசி: (011) 421-6062
மின்னஞ்சல்: help@hithawathi.lk
இணையத்தளம்: www.hithawathi.lk

இன்று நமக்கு இணையம் இன்றியமையாத ஒன்றாகி உள்ளது. எமது பிரத்தியேக நடவடிக்கைகள், தொழில் நடவடிக்கைகள் மட்டுமன்றி கல்வி நடவடிக்கைகளையும் நாம் கணினியின் மூலமாக அல்லது தொலைபேசியின் மூலமாக மேற் கொண்டு வருகிறோம். நாம் முன்னொருபோதும் எண்ணாத வகையில் எமது பெரும்பாலான நடவடிக்கைகளை நிகழ்நிலை வாயிலாக செய்ய முடியும் என்பது தற்போது நிரூபிக்கப்பட்டுள்ளது.

இணையத்தில் பல நல்லவற்றைப் போலவே தீய பக்கங்களும் உண்டு. சுற்றும் முற்றும் பார்க்காது சாலையின் குறுக்கே ஓடுவது ஆபத்தானது. அதே போலவே கவனக்குறைவாக இணையத்தில் உலா வருவதும் ஆபத்தானது. குறிப்பாகப் பாடசாலை சிறுவர்களுக்கு இந்த ஆபத்துக்கள் குறித்து நன்கு அறிவுறுத்தி, செய்யக் கூடியவை எவை, செய்யக் கூடாதவை எவை என்பது தொடர்பாக விழிப்புணர்வை ஏற்படுத்துவது மிகவும் அவசியமாகும். இவ்வாறு இன்றைய நாட்களில் எமது பாதுகாப்பைப் பேணி இணையத்தின் ஊடாக மிகவும் சிறந்த பயனைப் பெற்றுக் கொள்ள வேண்டும்.

இதற்காக ஹிதவதி திட்டம் மிகவும் பயனுள்ள முயற்சியை இச் சிற்றேடு மூலம் முன்வைக்கிறது. பெண்கள், இளைஞர் மற்றும் சிறுவர்கள் ஆகியோருக்கு இணையம் மற்றும் அதன் சேவைகளைப் பயன்படுத்தும் போது நிகழும் சிரமங்கள், தவறான வழிகாட்டல்கள், குற்றங்கள் மற்றும் தேவையற்ற அழுத்தங்கள் ஆகியன தொடர்பாக உங்களுடன் பேசவும், உங்களை அறிவுறுத்தவும் ஹிதவதி தயாராக உள்ளாள்.

அவ்வாறான சந்தர்ப்பங்களில் செய்ய வேண்டியவற்றையும், அவ்வாறான ஆபத்துக்களை தவிர்த்துக் கொள்ளும் விதம் குறித்தும் ஹிதவதி உங்களுக்குச் சொல்லித் தருவாள். ஹிதவதி இலங்கை தள பதிவாளரினால் (LK Domain Registry) மேற்கொள்ளப்பட்டு வரும் ஒரு திட்டமாகும்.

பேராசிரியர் கிஹான் டயஸ்

ஹிதவதி பற்றி...

இணையத்தைப் பயன்படுத்தும் போது சந்திக்கும் பல்வேறு வகையான நபர்கள் மற்றும் செயற்பாடுகளால் ஏற்படும் சிக்கல்களுக்கு முகம் கொடுக்கவும், அதைப் பற்றிய சரியான புரிந்துணர்வைப் பெற்றுக் கொள்ளவும், அதிலிருந்து பாதுகாப்பாக இருப்பதற்கும் பொதுமக்களுக்கு வழிகாட்டல்களை வழங்குவது இத்திட்டத்தின் முக்கிய நோக்கமாகும்.

இலவசமாக வழங்கப்படும் சேவையான "ஹிதவதி" உதவிச் சேவை இலங்கை தள பதிவாளரின் (LK Domain Registry) பிரதான அனுசரணையுடன் பல வருடங்களாக இலங்கையர்கள் பலருக்கு நன்மை பயக்கும் வகையில் இச்செயற்பாட்டில் இடைவிடாது ஈடுபட்டுவருகின்றது. இதைத் தவிர, சிறந்த சேவையை வழங்குவதற்காக அரச, அரச சார்பற்ற மற்றும் சர்வதேச அமைப்புக்களினதும் ஒத்துழைப்பைப் பெற்று ஹிதவதி திட்டம் செயற்படுத்தப்படுகின்றது.

சமர்ப்பணம்

உங்கள் நெருங்கிய ஹிதவதியிடமிருந்து

அன்புடன் அனைத்துச் சிறுவர்களுக்கும்

உள்ளடக்கம்

அறிமுகம் ... i

1. எமது தகவல்கள் மிகவும் முக்கியமானவை ... 1

2. இணையவெளித் தாக்குதல்களுக்கு ஆதரவு வழங்காதிருப்போம் ... 9

3. கருவிகளின் பாதுகாப்பை குறைமதிப்பீடு செய்யாதிருப்போம் ... 14

4. இணையத்தள மோசடிகளில் அகப்படாதிருப்போம் ... 19

5. சமூக ஊடகங்களைப் பற்றி அறிந்து அதனைப் பயன்படுத்துவோம் ... 24

6. இணையவெளி துன்புறுத்தல்களுக்கு அஞ்ச வேண்டாம் ... 29

7. சட்டத்தொகுதி உங்களுக்காகத் தயாராக உள்ளது ... 34

8. உளநலச் சிக்கல்களுக்கு வழிகோலும் இணையவெளிக் குற்றங்கள் ... 39

9. தொழில்நுட்பம் என்பது மிகவும் பெறுமதி வாய்ந்ததொன்றாகும் ... 44

10. இணையவெளி துன்புறுத்தல்களுக்கு முகம் கொடுத்தால் நீங்களும் அழையுங்கள் ... 49

கலைச் சொற்களஞ்சியம் ... 53

உசாத்துணை ... 56

உங்கள் அறிவை சோதித்து பார்க்கவும் ... 57

அறிமுகம்

ஹிதவதி அமைப்பால் கொண்டு வரப்படும் இக் கைநூல், பாடசாலை மாணவர்களுக்கும், இணையத்தைப் புதிதாகப் பயன்படுத்துவோருக்கும் இணையவெளிப் பாதுகாப்புத் தொடர்பாக அதாவது இணையத்தில் உலாவருவதற்கு முன் அதிலுள்ள ஆபத்துக்களைப் பற்றி அறிந்திருக்க வேண்டிய அடிப்படை விடயங்களை உள்ளடக்கியுள்ளது.

இது பிள்ளைகளுக்கு மிகவும் எளிதாகப் புரிந்து கொள்ளக் கூடிய வகையில் அமைந்துள்ள வசன நடைகளையும், உருவப் படங்களையும், உரையாடல்களையும் கொண்டு தொழில்நுட்ப அறிவை மிக எளிமையாக முன்வைக்கிறது. எந்தவொரு வயதினரும், தொழில்நுட்ப அறிவைக் கொண்டிராதோரும் கூட விளங்கிக் கொள்ளும் வகையில் தமிழ் கலைச் சொற்களை அளவு கடந்து பயன்படுத்தாது, பொதுவான சொற்பிரயோகங்களைப் பயன்படுத்தி இது அறிவூட்டுகின்றது.

காலாவதியான தகவல்களுக்குப் பதிலாக இந்நூலைத் தொகுக்கும் வரையான சமீபத்தியத் தகவல்கள் இங்கே உள்ளடக்கப்பட்டுள்ளன. அத்துடன் சமூக வலையமைப்புக்கள் உட்பட இணையம் என்பது பிள்ளைகளுக்குத் தகாத இடமன்றி, புரிந்துணர்வுடன் பாவிப்போமானால் பல நன்மைகளைப் பெற்றுக் கொள்ளக் கூடியதொன்றெனும் கருத்தை சமூகத்திடையே விதைப்பதற்கும், பிள்ளைகள் கணினி / தொலைபேசியைப் பயன்படுத்துவது அழிவை ஏற்படுத்துமெனும் தவறான கருத்தை உடைத்தெறிவதன் ஊடாக இந் நாட்டில் கணினி அறிவைக் கொண்ட இளைய தலைமுறையொன்றைக் கட்டியெழுப்புவதற்கான முயற்சியாக இது அமைகிறது.

1. எமது தகவல்கள் மிகவும் முக்கியமானவை

இப்பகுதியில் உள்ளடங்கும் விடயங்கள்

- தகவல்கள் உங்களது சொத்து என்பதும்
- தனியுரிமைக் கொள்கை (Privacy Policy) வாசிக்கப்பட வேண்டும் என்பதும்.

தரவுப் பாதுகாப்புத் (Data Security) துறை எமது தரவுகளையும், அவற்றிலிருந்து நிர்மாணிக்கப்படும் தகவல்களையும் சொத்துக்களென வரைவிலக்கணப்படுத்துகின்றது. அவை பெறுமதி மிக்கவை. எனவே அவற்றை நாம் உயிர் போல் காக்க வேண்டும்.

தரவுகளுக்கு நிதிப் பெறுமதி உண்டு

கணினி மென்பொருட்கள், இணையம் உள்ளிட்ட அனைத்து சேவைகளும் எமது தகவல்களை (தொலைபேசி இலக்கம், பிறந்த திகதி, புகைப்படம், கருத்துக்கள் மற்றும் சில சமயம் வங்கித் தகவல்கள்) ஒன்று திரட்டுவதற்கு காத்திருக்கின்றன.

வலைத்தளமொன்றை அல்லது சேவையொன்றை உருவாக்குவதைப் போலவே பராமரிப்பதற்கும் பெரிய கூட்டமொன்று பாடுபடுகின்றது. அவர்களுக்குச் சம்பளங்களை வழங்கவும், நிறுவனச் செலவினங்களை ஈடுசெய்வதைப் போலவே உற்பத்திகளை விளம்பரப்படுத்தவும் வேண்டும்.

இனி இந்தளவு செலவினங்களுடன் அவர்கள் அவற்றை இலவசமாக எப்படித் தருவது?

அவர்கள் திரட்டும் தரவுகளுக்கிடையே எமக்குப் பிடித்த / பிடிக்காத விடயங்கள், காண விரும்பும் காணொளிகள் / புகைப்பட வகைகள், தேடும் விடயங்கள் என, அனைத்தும் உள்ளடக்கியுள்ளது. நமக்கு இலவசமாகத் தரப்படும் சேவைக்கு எமது பிரத்தியேகத் தகவல்களையே கட்டணமாகச் செலுத்துகின்றோம்.

உங்களையும், உங்கள் குடும்பத்தினரையும் போலவே அது நாட்டையும் பாதிக்கின்றது

எனது தகவல்களை எடுத்துக் கொண்டால் எனக்கென்ன?

நான் அமெரிக்க ஜனாதிபதியா? இல்லையே!

கூகுல் மெப்ஸ் (வரைபடம்) போன்ற சேவைகளின் மூலம் ஜீ.பீ.ஸ் (GPS) தரவுகளைப் பயன்படுத்தி நாம் செல்ல வேண்டிய பாதையை தேடிக் கண்டுபிடிப்பதற்கு உதவி செய்வதைப் போலவே, அந் நிறுவனத்துக்கும் நீங்கள் இருக்கும் இடத்தைக் காண முடிகிறது.

இதனால் என்ன தீங்கு நேரக் கூடும்?

சிந்தியுங்கள்... ஏதேனுமொரு தீவிரவாத அமைப்பொன்று இலங்கை முழுவதிலும் உள்ள வீதித் தரவுகளைப் பெற்றுக் கொண்டால் அதிகளவானோர் ஒன்று கூடியிருக்கும் இடங்களை அவர்கள் கண்டறிந்து பாரிய தாக்குதலை நடத்த முடியும்.

முகநூலைப் போலவே Truecaller போன்ற செயலிகளை நிலைநாட்டும் போது (Install) எமது தொலைபேசியில் சேமித்து வைத்திருக்கும், ஏனையோரின் தொலைபேசி இலக்கங்களையும் அவர்களுக்குத் தருமாறு அறியத் தரப்படும். சிலவேளைகளில் இவை மூன்றாம் தரப்பினரின் கரங்களுக்கும் கிட்டக் கூடும்.

இதனால் நீங்கள் குடும்பத்தவர்கள், நண்பர்கள் உள்ளிட்ட சகலரினதும் தரவுகளை கவனயீனமாக மூன்றாம் தரப்பினருக்கு வழங்குகின்றீர்கள்.

தரவுகள் எவ்வாறு பயன்படுத்தப்படுகின்றன என்பது குறித்து அறிந்து கொள்ளுங்கள்

இணையத் தளங்களில், செயலிகளில் தனியுரிமைக் கொள்கை (Privacy Policy) எனும் ஒரு ஆவணம் காட்சிப்படுத்தப்படும்.

அதில் அவர்கள் தரவுகளைப் பாவிக்கும் விதம், சேமித்து வைத்துக் கொள்ளும் காலப் பகுதி உள்ளிட்ட விபரங்கள் உள்ளடங்கப்படும். அதனை வாசித்து அச் சேவையைப் பாவிப்பதா வேண்டாமா எனத் தீர்மானித்துக் கொள்ளலாம்.

எமது தகவல்களை எவ்வாறு பாதுகாப்பது?

உங்களது பெற்றோரின் அனுமதியின்றி முழுப்பெயர், விலாசம், பாடசாலையின் பெயர் அல்லது தொலைபேசி இலக்கம் போன்ற தனிப்பட்ட தகவல்களை எவருக்கும் கொடுக்க வேண்டாம்.

ஒருவர் உங்களின் பிரத்தியேகத் தகவல்களைக் கேட்ட உடனே அவற்றைக் கொடுக்க வேண்டிய அவசியமில்லை என்பதை நன்கு நினைவில் கொள்ளுங்கள். அவ்வாறான அந்தரங்கத் தகவல்களை எழுதி வைத்திருப்பதையோ அல்லது சேமித்து வைத்திருப்பதையோ தவிர்ப்பது நல்லது.

நீங்கள் Vlogs (YouTube Videos / TikTok) போன்றவற்றை செய்வதானால் வீட்டின் உட்புறம், முகம் போன்ற உங்களது அடையாளத்தை உறுதிப்படுத்தும் விதத்திலான காட்சிகளை உள்ளடக்க வேண்டாம். பாவிக்காத சந்தர்ப்பங்களில் கூட மடிக்கணினியின் கமராவையும் மூடி வையுங்கள்.

தகவல் பாதுகாப்பு தொடர்பான மேலதிக விபரங்களைத் தெரிந்துக் கொள்ளுங்கள்.
https://www.hithawathi.lk/ta/help-center-ta/cyber-security-tips-ta/internet-safety-tips-for-children-and-teens-ta/

எம்மைப் பாதுகாத்துக் கொள்வது எப்படி?

என்று சசினி அவளது IT ஆசிரியையிடம் வினவினாள். ஆசிரியர் அவற்றை இவ்வாறு பட்டியலிட்டார்.

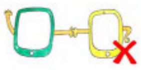
கடவுச்சொற்களைப் பாதுகாத்தல்

உங்களது கடவுச் சொற்களை உங்களின் பெற்றோரைத் தவிர வேறொருவரிடமும் கூற வேண்டாம். நீங்கள்

பொதுக்கணினியொன்றை அல்லது வேறொருவரின் கணினியைப் பயன்படுத்தும் போது ப்ரவுசரை மூடுவதற்கு (Close) முன் நீங்கள் பிரவேசித்த சகல கணக்குகளிலிருந்தும் Log out (வெளியேற்றம்) ஆகுங்கள்.

புகைப்படங்களைப் பிரசுரிக்க வேண்டாம்

பெற்றோர்களின்/ பாதுகாவலர்களின் அனுமதியின்றி புகைப்படங்களையோ அல்லது காணொளிகளையோ இணையத்தில் போட வேண்டாம். மற்றவர் அவற்றை எடுத்து அவர்களின் சுயவிபரங்களை (புரோபைல்) உருவாக்குவதற்கும், பக்கங்களில் பகிரவும் (Share) வாய்ப்புக்கள் உண்டு.



இணைய நண்பர்கள் (Online Friends) ஆபத்தானவர்கள்

பெற்றோர்களின்/ பாதுகாவலர்களின் அனுமதியின்றி இணைய நண்பர்களைச் சந்திக்கச் செல்ல வேண்டாம். துரதிஷ்டவசமாக சிலர் போலியாகவும், மோசடியான முறையிலும் தம்மை அடையாளப்படுத்துகின்றனர்.

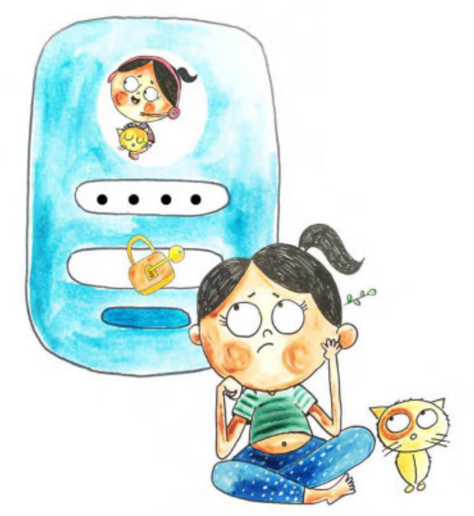
அவர்கள் உங்களுக்கு உதவுவதாகவும், துன்பத்தில் ஆதரவளிப்பதாகவும் கூறி நெருங்கிப் பழகி உங்களைத் துஷ்பிரயோகத்தில் ஈடுபடுத்தக் கூடும்.

பொய்யான செய்திகள் பற்றி விழிப்புணர்வுடன் இருங்கள்

நீங்கள் இணையத்தில் வாசிக்கும் அனைத்தும் உண்மையானதல்ல. நம்புவதற்கு முன் அவை உண்மையானதா பொய்யானதா என ஆராய்ந்து பாருங்கள்.

“புரிஞ்சுதா?” என ஆசிரியர் கேட்ட போது சசினி தலையை ஆட்டி “ஆம்” எனக் கூறினாள்.

கடவுச்சொற்களை பயன்படுத்தும் போது இவற்றைப் பற்றி கவனத்தில் கொள்ளவும்



கடவுச்சொல் என்பது வீட்டுத் திறப்பு போன்றதாகும். நீங்கள் அதனை வீட்டாரைத் தவிர வேறு எவருக்கும் கொடுக்காததைப் போலவே கடவுச்சொல்லையும் மிகவும் பாதுகாப்பாக வைத்திருக்க வேண்டும்.

குறிப்பாக மின்னஞ்சல் கணக்கின் கடவுச்சொல்லை எங்காவது எழுதி வைத்திருந்து வேறொருவரின் கரங்களுக்கு கிடைத்தால் அதனைப் பாவித்துப் பதிவு செய்த முகநூல், ஸ்கைப் போன்ற பல கணக்குகளை ஒரே தடவையில் அவர்களின் உடைமையாக்கிக் கொள்ளும் வாய்ப்புக் கிட்டுகிறது.

இப்படித் தான் சிறந்ததொரு கடவுச்சொல்லை அமைத்துக் கொள்வது

ஆங்கிலக் கெப்பிட்டல் (பெரிய) எழுத்துக்களையும், சிம்பல் (சிறிய) எழுத்துக்களையும் கலந்து உருவாக்கவும்.

இடையிடையே இலக்கங்களையும் உள்ளடக்குங்கள்.

விஷேட குறியீடுகளை (உதாரணமாக ?, !, -, %) பயன்படுத்தவும்

மற்றவர்களால் இலகுவில் கண்டுபிடிக்கக் கூடிய பிறந்த திகதி, நெருக்கமானவர்களின் பெயர், தேசிய அடையாள அட்டை இலக்கம் போன்றவற்றைப் பயன்படுத்த வேண்டாம்.

சிறந்ததொரு கடவுச்சொல்லை அமைத்துக் கொள்ள பின்வரும் இணையத் தளங்களைப் பயன்படுத்த முடியும்.

- https://passwordsgenerator.net
- https://www.lastpass.com/password-generator
- https://www.dashlane.com/features/password-generator
- https://1password.com/password-generator/
- https://www.avast.com/random-password-generator

நினைவில் வைத்துக் கொள்ளவதற்கு இலகுவானதொரு சொல்லைப் போட வேண்டுமாயின், உதாரணமாக SriLanka1948 என்பதை 1$ri9L@n4K@8 என அமைத்துக் கொள்ளலாம். ஒருபோதும் ஒரே கடவுச் சொல்லை எல்லாக் கணக்குகளுக்கும் பாவிக்க வேண்டாம்.

LastPass, DashLane, Keeper போன்ற சேவையொன்றைப் பயன்படுத்தல் அதனை விட மிகவும் சிறந்த வழிமுறையாக அமைகிறது. அப்போது குறித்த சேவையின் பிரதான (master) கடவுச்சொல்லை மாத்திரமே நினைவில் வைத்திருக்க வேண்டும்.

அதன் போது பிரவேசிக்கும் ஒவ்வொரு கணக்குகளுக்கும் கடவுச்சொல்லை தட்டச்சிடுவதற்கு (type) அவசியமில்லாததால் எமது விசைத் தட்டில் (Keyboard) தட்டச்சிடுபவற்றைக் கண்டறியும் கீலொகர் (Keylogger) போன்ற வன்ம மென்பொருட்களுக்குக் கடவுச் சொல்லைத் திருட முடியாது போகும்.

தொலைபேசி பூட்டுக்கு (LOCK) பெயர், விரலடையாளம் அல்லது முக அடையாளங்களை (FaceID) இட்டுக் கொள்வது இலகுவாக இருப்பினும், நீங்கள் உறங்கிக் கொண்டிருக்கும் போது வேறொருவர் உங்களின் விரலை வைத்தோ அல்லது முகத்திற்கு முன் தொலைபேசியை கொண்டு சென்றோ திறந்து (Unlock) கொள்ளமுடியும். அதனால் கடவுச்சொல்லொன்றை இடுவது எந்நேரத்திலும் பாதுகாப்பான முறையாகும்.

2. இணையவெளித் தாக்குதல்களுக்கு ஆதரவு வழங்காதிருப்போம்

இப்பகுதியில் உள்ளடங்கும் விடயங்கள்

- பதிவு செய்யப்பட்ட மென்பொருள் பாவனையில் உள்ள முக்கியத்துவம்.
- தன்னை அறியாமலே இணையவழித் திருடர்களின் கூலியாதல்.
- வைரசுகளிடமிருந்து பாதுகாத்துக் கொள்ளும் முறை.

சிரஸ்தி- எனக்குக் கடிதமொன்றை டைப் செய்து கொள்வதற்கு ஒபீஸ்ஸை (Office) போட்டுக் கொள்ள வேண்டும். உங்களிடம் கிரக் பண்ணினதொன்று இருக்கா?

பிரபோத- கிரக் செய்த சொப்ட்வெயார் ஒன்றை பாவிக்கிறது சட்டத்துக்கு விரோதமானது. அதைத் தவிர கணினிக்கு வைரஸ் வரவும் கூடும். நான் உங்களுக்கு ஒபன் ஒபீஸ் (OpenOffice) போட்டுத் தாரன்.

கணினிக்குள் செயற்பாட்டுத் தொகுதியையும், மென்பொருட்களையும் தாபிக்கும் போது கட்டணம் செலுத்த நேரிடுகின்றது. பலர் அவ்வாறு கட்டணம் செலுத்தாது திருட்டு (கிரக் செய்து) மென்பொருட்களைப் பாவிக்கின்றனர். அதன் போது நாம் இணையவெளித் தாக்குதல்களுக்கு (botnet ஒன்றுக்கு) உதவுபவர் ஆகிறோம். அத்துடன் கணினியில் உள்ள பெறுமதி வாய்ந்த தரவுகளை அழிக்கும் ரென்சம்வெயார் (Ransomware) வைரஸ்களுக்கு இரையாகும் வாய்ப்புகளுமுண்டு.

திருட்டு (கிரக்) மென்பொருட்களைத் தயாரிக்கும் திருடர்கள் (கிரக்கர்ஸ்) எம்மீதுள்ள அன்பில் அவற்றைத் தயாரிப்பதில்லை. அவர்களும் அதில் நன்மை அடைவதனாலேயே அவர்கள் அத்தகைய டொரன்ட்களை (Torrents) தயாரிக்கின்றனர்.

வைரஸ் பாதுகாப்பை செயலிழக்கச் செய்ய வேண்டாம்

திருடிய (கிரக்) மென்பொருட்களில் வைரஸ் உண்டு. அதனால் அவற்றை தாபிக்கும் கட்டங்களில் வைரஸ் பாதுகாப்பைச் செயலிழக்கச் செய்யுமாறு காட்டப்படும். அதன் போது நீங்கள் பணம் செலுத்தி வைரஸ் பாதுகாப்பை (Virus guard/Antivirus software) போட்டிருந்தாலும், இப்போது நீங்கள் விருப்பத்துடனே வைரஸ்களுக்கு இடமளிக்கின்றீர்கள்.

அவ்வாறு பிரவேசித்ததன் பின், அவர்களுக்கு எமது கணினியைப் பாவித்து இணையவெளித் தாக்குதல்களை மேற்கொள்ள (Cyber-attacks) முடியும்.

அதைத் தவிர, எமது கோப்புக்கள் அனைத்தையும் மறைகுறியாக்கம் (Encrypt) செய்து, அதனை மீண்டும் பெற்றுத் தருவதற்கு கட்டணம் செலுத்துமாறு சொல்லும் ரென்சம்வெயார் வைரஸ்களும் தற்போது துரிதமாக பரவி வருகின்றன. பிரச்சினை என்னவென்றால் நாம் அக் கட்டணத்தைச் செலுத்தினால் இன்னும் ஒரு தடவை மறைக்குறியாக்கம் செய்து மீண்டும் மீண்டும் பணம் பறிப்பதற்கு அவர்களால் முடியும்.

ரென்சம்வெயாரிலிருந்து தப்பிப்பதற்கான வழியை hithawathi.lk எனும் இணையத் தளத்திலுள்ள குறிப்பைப் பார்க்க இக் QR Code ஐ ஸ்கேன் செய்து கொள்ளுங்கள்.

https://www.hithawathi.lk/ta/help-center-ta/security-alerts-ta/cyber-security-alert/

எந்நேரமும் நீங்கள் எதைப் பதிவிறக்கம் செய்கிறீர்கள் என்பது குறித்தும், அந்த மென்பொருளைத் தாபிப்பதற்கு அவசியமா என்பது குறித்தும் கவனத்தைச் செலுத்துங்கள். சில சமயங்களில் வீடியோவையோ அல்லது திரைப்படங்களையோ பதிவிறக்கம் செய்யும் போது வீடியோ கோப்பு வடிவில் வைரசுக்களும், எட்வெயார்களும் (Adware) நுழையக் கூடும். வைரஸ் பாதுகாப்பை எப்பொழுதும் இற்றைப்படுத்திக் (Update) கொள்ளுங்கள்.

வைரஸ் ஒன்றை எவ்வாறு இனம் காண்பது?

அனுராதாவின் கணினி வழக்கத்தை விட வேகம் குறைந்து விட்டதை அவளால் உணர்ந்து கொள்ள முடிந்தது. கணினிக்கு உயிர்ப்பளிக்கும் போதும் மென்பொருட்களினுள் நுழையும் போதும் தாமதம் ஏற்படுவதுடன், திரையில் பல்வேறு செய்திகளும் தோன்றத் தொடங்கியது. இதைப் பற்றி மேலும் தெரிந்து கொள்ள நினைத்த அவள் 'reasons why a computer runs slow என கூகுலில் தேடினாள்.

அதன் போது கணினியின் வேகம் குறைவதற்கான காரணங்களாக வைரஸின் நுழைவும் காரணமாக அமையக் கூடுமென்பதை அவள் கண்டாள். அதற்குப் பின்வரும் அறிகுறிகளைக் காண முடியுமென அங்கு குறிப்பிடப்பட்டிருந்தது.

- கணினி வழமையான வேகத்தை விட குறைந்த வேகத்தில்

இயங்குதல்.

- அடிக்கடி கணினி தானியங்கியாக மீள உயிர்ப்படைதலும், அசாதாரணமான முறையில் இயங்குதலும்.
- கணினியில் உள்ள நிகழ்ச்சிகள் உரிய முறையில் இயங்காமை.
- வழமைக்கு மாறான, பிழையான செய்திகள் காட்சியளிக்கும்.
- நீங்கள் உருவாக்காத புதிய அயிகன்கள் கணினித் திரையில் காட்சியளிக்கும்.
- நீங்கள் கணினியிலிருந்து நீக்காத நிகழ்ச்சிகள் கணினியிலிருந்து நீக்கப்பட்டுள்ளதாக காட்சியளிக்கும்**.**

கணினியை வைரஸ்களின் ஆக்கிரமிப்புக்களிலிருந்து தவிர்த்துக் கொள்வது எப்படி?

பயர்வோல் பயன்பாடு

மென்பொருட்களை இற்றைப்படுத்தல்

போலி அனுமதிப் பத்திரங்களைக் கொண்ட மென்பொருட்களின் பாவனையைத் தவிர்க்கவும்.

நம்பகமான வைரஸ் எதிர்ப்பு மென்பொருட்களைப் பாவித்தல்.

சந்தேகத்திற்கிடமான இணைப்புகளை (Links) கிளிக் செய்யாதிருத்தல்

இனந் தெரியாதோரிடமிருந்து வரும் மின்னஞ்சல்களின் இணைப்பைத் திறக்காதிருத்தல்

இலவசமான, திறந்த மென்பொருட்களைப் பயன்படுத்தவும்

அபிவிருத்தி அடைந்து வரும் நாடான எமக்கு எல்லா மென்பொருட்களையும் வாங்கிக் கொள்ள இயலாதென்பது உண்மையாகும். இருப்பினும் திருட்டு மென்பொருள் பாவனையை ஒருபோதும் நியாயப்படுத்த முடியாது. அதற்குப் பதிலாக இலவசமாக வழங்கப்பட்டுள்ள மென்பொருட்களைப் பயன்படுத்தலாம். பின்வருவன அவற்றுக்கான சில மாற்றீடுகளாகும்.

கட்டணம் செலுத்திப் பெற்றுக் கொள்ள வேண்டிய மென்பொருட்கள்/ இணையச் சேவைகள்/ செயற்பாட்டுத் தொகுதிகள்	இலவசமாக பெற்றுக் கொள்ளக் கூடிய மாற்றீடுகள்
Microsoft Windows	Linux (Ubuntu, Linux Mint)
Microsoft Office	OpenOffice.org, LibreOffice
Adobe Photoshop	GIMP
Autodesk 3ds Max	Blender
Shopify	WordPress (WooCommerce)

3. கருவிகளின் பாதுகாப்பை குறைமதிப்பீடு செய்யாதிருப்போம்

இப்பகுதியில் உள்ளடங்கும் விடயங்கள்

- கருவி வேறொருவரின் கைகளுக்குக் கிட்டினால் ஏற்படும் விளைவுகள்
- காணாமல் போனால் செய்ய வேண்டியவை

தனுஷ்கி அவளது போனில் டிஸ்பிளே இயங்காததால், அதனை பழுதுபார்க்கும் சேவை நிலையத்துக்குக் கொடுத்தாள். மீண்டும் வீட்டுக்குக் கொண்டு வந்த பின் அவளுக்கு அடிக்கடி பல்வேறு இனந்தெரியாத இலக்கங்களிலிருந்து அழைப்புக்கள் வந்தன. “தங்கச்சி இப்ப போன் வேலை செய்யுதா?” “உங்கட போனில இருக்கிற

போட்டோ நல்ல வடிவு" போன்ற தேவையற்ற செய்திகள் அவளுக்குக் கிடைக்க ஆரம்பித்தன. பல்வேறு இடங்களுக்கு வந்து சந்திக்குமாறும், அல்லாதுவிடில் அவளது புகைப்படங்களை இணையத்தில் வெளியிடுவதான அச்சுறுத்தல்களும் அவற்றிடையே இருந்தன.

அறிமுகமில்லாதவர்களுக்கு கருவியைக் கொடுக்கும் போது கவனமாகவிருங்கள்

கடவுச் சொற்களை இட்டாலும் வன்தட்டுக்களில் (Hard disk) உள்ளவற்றை வேறு முறைகளால் பார்க்க முடியும்.

உங்கள் தொலைபேசியையோ அல்லது மடிக்கணினியையோ வேறொருவருக்குக் கொடுக்க நேருமானால், அங்குள்ள சகல பிரத்தியேகத் தரவுகளையும் backup செய்து, சாதனத்திலிருந்து நீக்கி விடுங்கள். முகநூல், ஜீமெயில் போன்றவற்றிலிருந்து logout ஆகுங்கள். தொலைபேசியின் டிஸ்பிளேயைப் பழுதுபார்ப்பதற்குக் கொடுக்கும் போது அதனை அன்லொக் செய்யத் தேவையில்லை. அவ்வாறானவற்றைக் கூறி உங்களை ஏமாற்றி உங்களின் தரவுகளை பெற்றுக் கொள்ள எடுக்கும் முயற்சிகளில் அகப்பட்டுக் கொள்ள வேண்டாம்.

தொலைந்து போனால் என்ன செய்வது?

தொலைபேசியொன்று தொலைந்தாலும் அதிலுள்ள மொபையில் டேடா செயற்பாட்டு நிலையில் இருக்குமெனில், ஜீ.பீ.எஸ் (GPS) பாவிப்பதன் மூலம் அது இருக்கும் இடத்தை கண்டறிய முடியும். என்ரொயிட்களுக்கு https://www.google.com/android/find மூலமும் அப்பல்களுக்கு https://www.apple.com/icloud/find-my/ மூலமும் கணினியொன்றால் பிரவேசித்து இடத்தைக் கண்டறிய முடியும். தொலைபேசியை மீளப் பெற்றுக் கொள்வதில்

அசௌகரியங்கள் இருப்பின் குறித்த இணையப் பக்கங்களிலுள்ள Erase உத்தரவைப் பயன்படுத்தி சாதனத்தின் சகல தரவுகளையும் நீக்கி விடவும்.

பின்னர் தொலைபேசி சேவை வழங்குனருக்கு (சிம் அட்டையைப் பெற்றுக்கொண்ட நிறுவனம்) அழைத்து செயலிழக்கச் செய்யவும். அத் தொலைபேசி இலக்கத்தை வேறொரு சிம் அட்டையின் மூலம் பெற்றுக் கொள்ளலாம். கூகுல், முகநூல் கணக்குகளில் கடவுச் சொல்லையும் மாற்றுங்கள். இப்பொழுது, https://www.ineed.police.lk/ineed/ எனும் இணையத்தளத்தின் மூலம் தொலைபேசியின் இமி (IMEI) இலக்கத்தினை இட்டு முறைப்பாடொன்றை பதிவு செய்யுங்கள்.

கருவியொன்றை விற்பனை செய்வதற்கு முன்

பழைய மடிக்கணினியொன்றையோ, தொலைபேசியொன்றையோ வேறொருவருக்குக் கொடுப்பதற்கு முன், உங்கள் தரவுகளை மற்றுமொரு கருவிக்கோ அல்லது கூகுல் டிரைவ் போன்ற சேவைக்கோ (Google Drive) பிரதி செய்து நீங்கள் பிரவேசித்திருக்கும் அனைத்துக் கணக்குகளிலிருந்தும் லொக்அவுட் (Logout) ஆகுவதுடன், ஸ்ரீடர் (Shredder) மென்பொருளைப் பயன்படுத்தி தரவுகளை முற்றாக நீக்கி விடுங்கள். அல்லாதுவிடில் நீங்கள் நீக்கியவற்றை புதிய உரிமையாளரால் மீளப் பெற்றுக் கொள்ள முடியும்.

CONFIDENTIAL

சகல பிரத்தியேகக் கோப்புக்களையும் Recycle Bin அல்லது Trash மூலம் நீக்கி விட மறக்க வேண்டாம்.

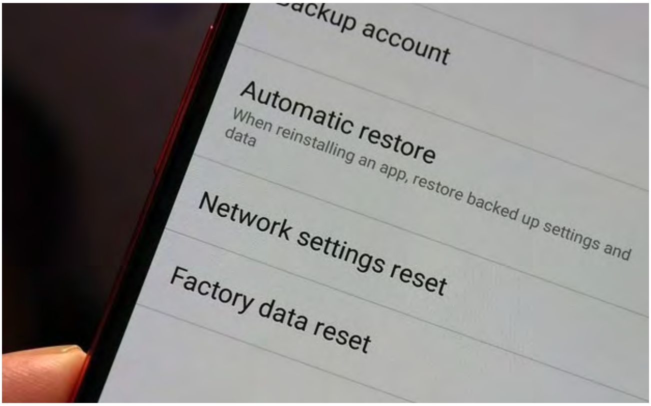
அவ்வாறான சில ஸ்ரீடர் மென்பொருட்கள் பின்வருமாறு

- Blancco Drive Eraser - https://www.blancco.com/products/drive-eraser/
- DBAN - https://dban.org/
- BCWipe - https://www.jetico.com/data-wiping
- BleachBit - https://www.bleachbit.org/download

வன் தட்டுடன் கூடிய (Hard Disk - HDD) கணினிக்கு மேற்குறிப்பிட்ட பட்டியலிலுள்ள மென்பொருட்களை தாபித்து, தரவுகளை முற்றாக நீக்கி விடுங்கள்.

என்ரொயிட்களுக்கு, பின்வரும் படிமுறைகளைப் பயன்படுத்தி தொலைபேசியிலுள்ள அனைத்துத் தரவுகளையும் ஒரே தடவையில் நீக்கி விட முடியும்.

Settings > Backup & Reset > Factory data reset > Reset phone


ackup account
Automatic restore
When reinstalling an app, restore backed up settings and data
Network settings reset
Factory data reset

தொலைபேசியில் அமைப்புக்களுக்குச் சென்று (Settings) மேற்காட்டப்பட்டுள்ள படிமுறைகளினூடாக தொலைபேசி மீளமைப்பு (Reset Phone) எனும் உத்தரவைத் தெரிவு செய்யுங்கள். இப் படிமுறை தொலைபேசி உற்பத்தி நிறுவனத்துக்கு அமைய வேறுபடக் கூடும்.

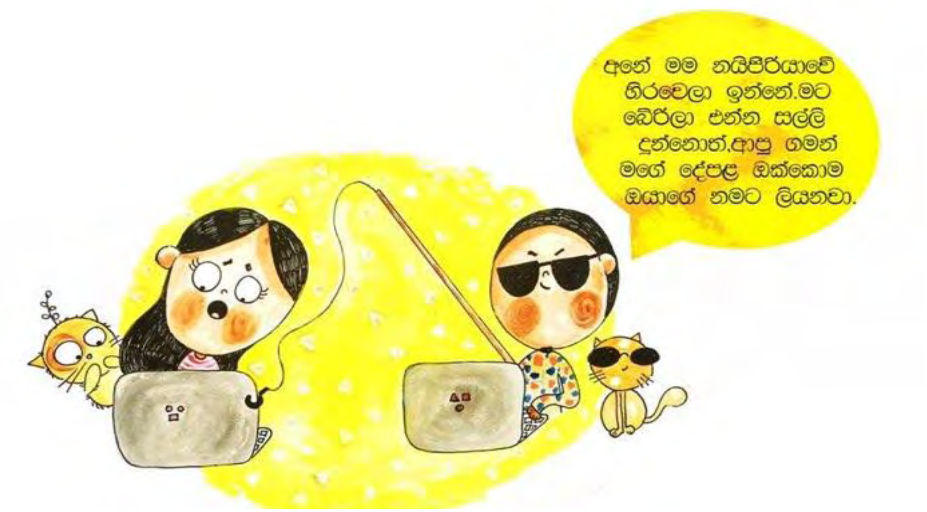
Apple தொலைபேசிகளுக்கு, கீழ்வரும் படிமுறைகளின் ஊடாக மீளமைப்பைச் (reset) செய்யுங்கள்.

Settings > General > Reset > Erase All Content and Settings

4. இணையத்தள மோசடிகளில் அகப்படாதிருப்போம்

இப்பகுதியில் உள்ளடங்கும் விடயங்கள்

- மோசடிகள் (Scams) செயற்படுத்தப்படும் விதம்
- மோசடிகளுக்குப் பயன்படுத்தும் முறைகளும், அவற்றைத் தவிர்த்தலும்,


අනේ මම නයිජීරියාවේ හිරවෙලා ඉන්නේ.මට බේරිලා එන්න සල්ලි දුන්නොත්,ආපු ගමන් මගේ දේපළ ඔක්කොම ඔයාගේ නමට ලියනවා.

ஐயோ நான் இப்ப நைஜீரியாவில் சிக்கிக் கொண்டிருக்கிறன். திரும்பி வரக் காசு தந்தால் வந்தவுடனே எனது அனைத்துச் சொத்துக்களையும் உங்கள் பெயருக்கு எழுதித் தருகிறேன்.

பணம், தகவல்கள் போன்றவற்றைத் திருடிக் கொள்ளும் நோக்கில் மின்னஞ்சல், முகநூல் செய்திகள் போன்றவற்றின் ஊடாக மோசடிகள் (Scams) இடம்பெறுகின்றன. அவை பின்வரும் வழிகளில் நேரிடலாம்.

- நீங்கள் கட்டளையிடாத, உங்களுக்கு உரித்தான பொருளொன்று சுங்கத்தில் உள்ளதாகவும், அதனை நீங்கள் பணம் செலுத்திப் பெற்றுக் கொள்ள வேண்டும் எனவும் கூறுதல்.
- பிரச்சனைக்கு ஆளாகியுள்ளதாகக் கூறிப் பணம் கோருதல்.
- போலி நண்பர்கள் அல்லது திருமணம் முடிப்பதாகக் கூறுதல்.

ஸ்பெமாக (Spam) வரும் மோசடிகள்

எம்முடன் தொடர்பில்லாத, பெரும்பாலும் எமக்குத் தெரியாதவர்கள் அனுப்பும் தேவையற்ற செய்திகளே ஸ்பெம் (Spam) எனப்படும்.

மோசடியாளர்கள் இவற்றின் ஊடாக எமது கவனத்தை ஈர்க்க முயற்சிப்பர். இதன் மூலம் பின்வரும் விடயங்கள் நடைபெறலாம்.

- நாம் பங்குபற்றாத போட்டியொன்றில் பெருமளவுப் பணத்தை வென்றுள்ளதாகக் கூறுதல்.
- போலி நிதி திரட்டல்.
- முதலீட்டை மேற்கொண்டு அதன் மூலம் அதிகளவுப் பணத்தைப் பெற்றுக்கொள்ள முடியுமென கூறுதல்.
- எமது புகைப்படங்கள் அவர்களிடம் இருப்பதாகக் கூறி மிரட்டி பணம் பறித்தல்.

இது தொடர்பாக மேலும் தெரிந்துக் கொள்வதற்கு விரும்பினால் hithawathi.lk இணையத்தளத்திலுள்ள முகவரியைப் பார்க்க இந்தக் QR Codeஐ ஸ்கான் செய்யுங்கள்.

https://www.hithawathi.lk/ta/help-center-ta/cyber-security-tips-ta/
spam-vs-scam/

ஒரு பாடசாலையின் இல்ல விளையாட்டுப் போட்டியில் எடுக்கப்பட்ட புகைப்படங்கள் பாடசாலை நிர்வாகப் பிரிவு முகநூலில் பிரசுரித்திருந்தது. சில நாட்களின் பின் 10 ஆம் தரத்தில் கல்வி கற்கும் அனுராதாவின் முகநூல் கணக்கில் அந்தப் புகைப்படம் பிரசுரிக்கப்பட்டிருந்ததாக அவரது தாயின் நண்பி ஒருவர் கண்ட போதிலும், அக் கணக்கு அனுராதாவின் கணக்கில்லை என்பதையும் அறிந்து கொண்டாள்.

மெசேஜ் பண்ணி அப் போலிக் கணக்கை நீக்குவதற்கு முயற்சித்தாலும், மோசடியாளர்கள் பணம் செலுத்தவில்லையெனில் மென்மேலும் புகைப்படங்களைப் பிரசுரிப்பதாகக் கூறினார்கள். (உண்மை கதையைத் தழுவியது. இதில் வரும் பெயர்கள் கற்பனையாகும்.)

இணையத்தளத்திலுள்ள மேலும் பல உண்மைக் கதைகளையும், எடுக்க வேண்டிய நடவடிக்கைகளையும் பற்றி அறிந்து கொள்வதற்கு இந்தக் QR Code யை ஸ்கேன் செய்து கொள்ளுங்கள்.

https://www.hithawathi.lk/ta/help-center-ta/real-time-cases-ta/

மோசடியாளர்களிடமிருந்து தப்பிக்கும் விதம்

- உங்களுக்குப் பழக்கமில்லாதவர்களிடமிருந்து வரும் செய்திகளுக்குப் பதிலளிக்க வேண்டாம்.
- போலி சமூக வலைத்தளங்களின் கணக்குகளை முறையீடு (Report) செய்தல்.
- பங்குபற்றாத போட்டியொன்றில் வெற்றி பெறுவது எங்ஙனம் என்பதை பகுத்தறிவுடன் சிந்தித்தல்.
- ஜீமெயில் போன்ற தானியங்கியாக ஸ்பேம் மின்னஞ்சல்களைப் பிரித்தெடுக்கும் சேவையொன்றைப் பாவித்தல்.

பிஸ்ஸிங் (Phishing) முறை காணப்படக் கூடுமென்பதால் அந்நியர்களிடமிருந்து வரும் இணைப்புக்களைக் (Link) கிளிக் (Click) பண்ணாதிருப்பது முக்கியமானதாகும். அந்த இணைப்பினூடாக பிரவேசித்தால் குறிப்பிட்ட சமூக ஊடக/ மின்னஞ்சல் Login பக்கத்தைப் போலவே போலிப் பக்கமொன்று தோன்றும். அதன் மீது உங்கள் கடவுச் சொல்லை உட்செலுத்தியதுடன் மோசடியாளர்களுக்கு / திருடர்களுக்கு உங்கள் கடவுச் சொல்லைப் பெற்றுக் கொள்ள முடியும்.

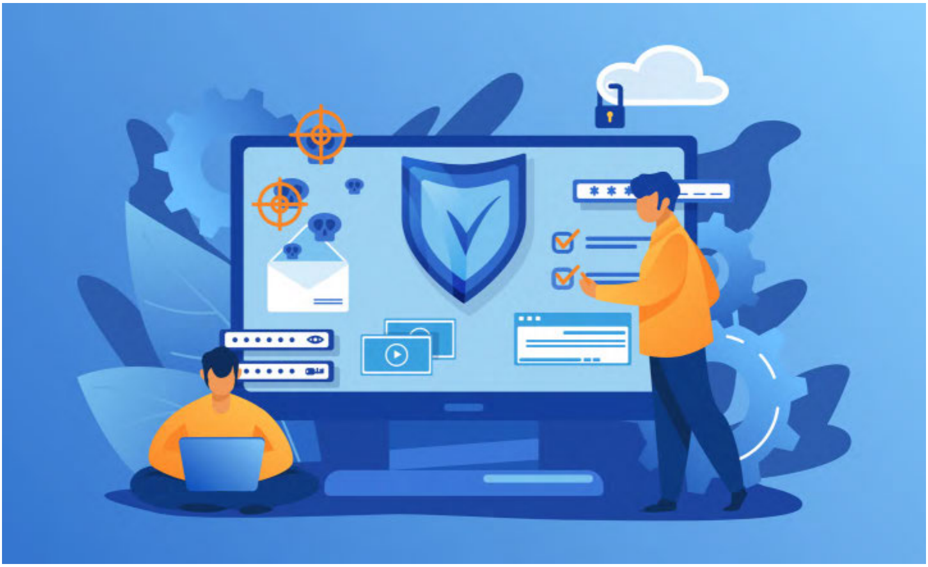
அதனால் இணையத் தளத்தின் உண்மை நிலையை சந்தேகமின்றி அறிந்து கொள்ளுதல் முக்கியமாகும்.

போலி/பிஸிங் இணையத்தளமொன்றை இவ்வாறு இனங்காணலாம்

இணைய முகவரியில் கவனம் செலுத்துங்கள். இணையத் தளமொன்றினுள் நுழையும் போதோ அல்லது இணைப்பைக் (Link) கிளிக் செய்யும் முன்னரோ குறித்த யூ.ஆர்.எல் (URL) ஐப் பரிசோதித்துப் பார்த்து உண்மையான இணையத்தளம் தானா என்பதனை உறுதிப்படுத்திக் கொள்ளவும்.

https://transparencyreport.google.com/safe-browsing/search அல்லது https://www.virustotal.com/gui/home/url இக்குச் சென்று Search by URL எனும் கூட்டினுள் குறித்த முகவரியை உட்சேர்ப்பதன் மூலம் இதனை இலகுவாக கண்டறிந்து கொள்ளலாம்.

அத்துடன் உங்களுக்கு facebook.com இக்குப் பிரவேசிக்க வேண்டுமெனில், அங்கு அந்த எழுத்துக்கள் இருப்பதையும், faecbook, facebok, facbook, facboook, faceb00k போன்ற எழுத்துக்கள் இல்லையென்பதையும் உறுதிப்படுத்திக் கொள்ளுங்கள்.



போலி வலைத்தளங்களை இனங்காணக் கூடிய மேலும் பல முறைகளைப் பற்றி அறிந்து கொள்ள hithawathi.lk கட்டுரையை.

இணையத் தளத்திலுள்ள கடிதங்களைப் பார்க்க இந்த QR Code யை ஸ்கேன் செய்துக் கொள்ளுங்கள்.

https://www.hithawathi.lk/ta/help-center-ta/knowledge-base-ta/you-decide-whether-it-is-a-fake-or-a-real-weblink-url/

பார்வைக்குச் சில

சாதாரண மக்களைத் தவறான வழிக்குக் கொண்டு செல்லும் மோசடிக்காரர்களை ஏமாற்றி அவர்களின் மோசடிகளை உலகுக்கு வெளிச்சம் போட்டுக் காட்டும் யூ டியுப் செனல் இருப்பதை அறிவீர்களா?

- Kitboga
- IRLrosie
- Trilogy Media

மேற்குறித்த செனல்களின் பெயர்களை யூ டியுப்பில் search பண்ணிப் பாருங்கள்.

5. சமூக ஊடகங்களைப் பற்றி அறிந்து அதனைப் பயன்படுத்துவோம்

இப்பகுதியில் உள்ளடங்கும் விடயங்கள்

- சமூக ஊடகங்களின் (Social Media) அனுகூலங்களும், பிரதிகூலங்களும்,
- பிரச்சனைகளைத் தவிர்க்கும் முறை

அடிமையாவதன் கெடுதி

பல்வேறு முறைகளில் எம்மை சமூக ஊடகங்களில் கட்டி வைத்திருக்க சமூக ஊடகத் தயாரிப்பாளர்கள் முயற்சிக்கின்றனர். ஒருவர் ஆசைப்படுபவற்றை இனங்கண்டு அவற்றையே காண்பித்து அவரை இணையத் தளங்களில் வெகு நேரம் உலாவ வைத்திருப்பதும், அதற்கிடையே வர்த்தக விளம்பரங்களைக்

காட்டுவதும் அதன் பிரதான பணியாகும். இதற்கு அடிமையானால் கல்வி சீர்குலையும். எனவே அதன் நன்மைகளைப் பெற்று, கவனமாகப் பாவிக்க வேண்டும்.

நல்லதும் கெட்டதும் சரி நிகராக

பெரும்பாலானோர் சமூக ஊடகங்கள் கெடுதியானதென வரைவிலக்கணப்படுத்த முயற்சித்தாலும், அவற்றில் ஏராளமான நன்மைகளும் உண்டு.

- தொலைவிலிருக்கும் பழைய நண்பர்களுடன் பேசுவதற்கு,
- உங்கள் திறமைகளை வெளிக்காட்டுவதற்கு,
- நூல்களுக்கு அப்பாற்பட்ட சமூகப் புரிந்துணர்வைப் பெற்றுக்கொள்வதற்கு சமூக ஊடகங்கள் உதவி புரிகின்றன.

> நடைமுறை வாழ்க்கைக்கும், சமூக ஊடகங்களுக்கும் இடையே எவ்வித வேறுபாடுகளும் இல்லை.

நல்லவர்களும், கெட்டவர்களும் நடைமுறை வாழ்க்கையில் இருப்பதைப் போலவே சமூக ஊடகங்களிலும் உள்ளனர். நடைமுறை வாழ்க்கையைப் போலவே சமூக ஊடகங்களிலும் அவர்களைக் கண்டறிய வேண்டும்.

தேவையற்ற விடயங்களையும், தேவையற்றோரையும் முறையீடு செய்யுங்கள் (ரீபோட்) / தடுத்திடுங்கள் (பிளோக்)

முகநூலில் எவரேனும் ஒழுக்கமற்ற எதையெனும் போஸ்ட் ஒன்றை பதிவிட்டிருப்பின், போஸ்ட்டின் வலது பக்க மேல் மூலையிலுள்ள மூன்று புள்ளிகளைக் கொண்ட குறியீட்டைக் கிளிக் செய்து Find support or report post என்பவற்றை தெரிவு செய்யுங்கள். கிடைக்கும்

கூட்டினுள் அந்தப் பதிவு ஆபாசமானது (Nudity), வன்முறையானது (Violence/Harassment), போலியான செய்தி (Fake News) போன்றவற்றில் பொருத்தமானதைத் தெரிவு செய்து அதன் கீழுள்ள Next பொத்தானை அழுத்தவும்.

முகநூலில் பிரத்தியேகத் தன்மையைக் காக்கும் இன்னுமொரு முறையைத் தெரிந்து கொள்வதற்கு hithawathi.lk இணையத் தளத்திலுள்ள தகவல்களைப் பார்க்க இவ் QR Code யை ஸ்கேன் செய்து கொள்ளுங்கள்.

https://www.hithawathi.lk/ta/help-center-ta/social-media/facebook/#Privacy-and-Safety

போலியான செய்திகளைக் கண்டறிதல்

பலர் தமது உள் நோக்கங்களை நிறைவேற்றுவதற்காக சமூக ஊடகத்தின் ஊடாக அங்குள்ளவர்களின் மனதுக்கு பல்வேறுபட்ட கருத்துக்களைப் பதிவிடுவர். இதனால் அமெரிக்கா, மியன்மார் மாத்திரமன்றி இலங்கையிலும் இனக்கலவரங்கள் ஏற்பட்டன.

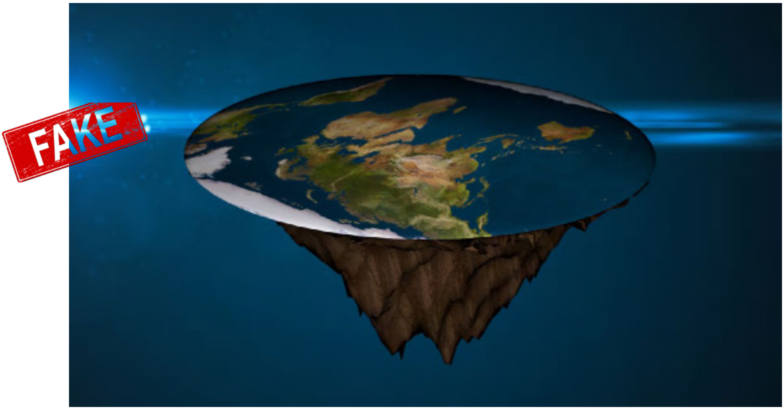
அரசியல் நோக்கங்களுக்காகவும் வியாபார நோக்கங்களுக்காகவும் பல்வேறான முகநூல் / இண்ஸ்டகிரேம் பக்கங்களைப் பயன்படுத்தி நீண்ட காலமாகவும், படிப்படியாகவும் இக் கருத்துக்களைப் பயனர்களின் மனதில் புகுத்துவர்.

அதனால், ஏதேனுமொரு பதிவைக் கண்டதும், அதனை உடனே பகிராது (Share) பகுத்தறிவுடன் அதன் உண்மை நிலையை ஆராய்ந்து பார்ப்பது நம் அனைவரதும் கடமையாகும்.

சமூக ஊடகங்கள் மூலம் வேகமாகப் பரவி வரும் சர்ச்சைக்குரிய பதிவுகளின் உண்மைத் தன்மையை சரிபார்க்க Fact Crescendo Sri Lanka முன்வந்துள்ளது.

எதையும் கண்டவுடன் பகிர (Share) வேண்டாம்.

உண்மைக் கதை - உலகம் தட்டையானது!



ஈர்ப்புச் சக்தி என்று ஒன்றுமில்லை.

உலகம் தட்டையானது என்பதாலே அனைத்தும் கீழே விழுகிறது.

விஞ்ஞானம் என்பது பொய்

அடுத்தவரும் அறிந்து கொள்ள பகிரவும். (Share)

போலிச் செய்திக்கு ஓர் எடுத்துக்காட்டு

உங்களுக்குத் தெரியுமா?

இந் நாட்டு சட்டத்துக்கு அமைய எந்தவொரு ஊடகத்தின் ஊடாகவும் பொய்யான செய்திகளைப் பிரசுரிப்பவர்களுக்கு எதிராகக் கடுமையான தண்டனை விதிக்கப்படலாம்.

கருத்துப் பிரச்சாரம் என்பது தனக்குத் தேவையான ஒரு உள் நோக்கத்தை அடைவதற்கான திட்டமிடப்பட்ட மூளைச் சலவையாகும்.

இதன் மூலம் தமது கருத்துக்கு அடுத்தவரை இசைவாக்கிக் கொள்ளும் வாய்ப்புக் கிட்டுகிறது. பிரபலமான சில பக்கங்களுக்குப் பணம் செலுத்தி அவர்களின் மூலமாக அடிக்கடி அக் கருத்தை சமூகமயப்படுத்துவது மாத்திரமே அச் சமூக ஊடகங்களின் ஊடாக மேற்கொள்ளப்படுகிறது.

தம்புரு விஜயசேகர (“சமூக ஊடக வலையமைப்பில் பெயர்போன அடிமைத் தனம்”

தினமின - த்வார 2020/10/05)

சட்ட ரீதியான நடவடிக்கைகளை எடுத்தல்

பிரச்சினை களுக்கு முகம் கொடுக்க நேரும் சந்தர்ப்பங்களில், மௌனமாக இருப்பதன் மூலம் குற்றவாளிகள் சுதந்திரமாக நடமாடுவதற்கு நீங்கள் இடமளிக்கின்றீர்கள். அதன் மூலம் இன்னுமொருவர் பிரச்சினைகளில் சிக்கக் கூடும். அதனால் அதிகாரிகளுக்கு அது குறித்து அறிவிக்கவும்.

சமூக ஊடகங்கள் (Facebook, Twitter, TikTok, Wiki இணையத் தளம், Blog) ஊடாக ஏதேனுமொரு தொந்தரவுக்கு முகம் கொடுக்க நேர்ந்தால் உங்கள் உதவிக்கு ஹிதவதி செயற்திட்டம் உள்ளது.

அது தொடர்பான ஆலோசனைகளைப் பெறுவதற்கு 011-421-6062 எண் மூலம் ஹிதவதியை அழைக்க முடிவதுடன், https://www.telligp.police.lk/ எனும் இணையத்தள முகவரிக்கு சென்று அங்குள்ள மாதிரிப் படிவத்தின் மூலம் Cybercrime ஐத் தெரிவு செய்து சாட்சிகளுடன் பொலிஸுக்கு இணையவழி முறைப்பாடுகள் செய்யவும்.

6. இணையவெளி துன்புறுத்தல்களுக்கு அஞ்ச வேண்டாம்

இப் பிரிவில் உள்ளடங்கும் விடயங்கள்

- இணையவெளித் துன்புறுத்தல்களை உதாரணங்களுடன் அறிமுகம்செய்தல்
- பாதிப்புகள் மற்றும் அதிலிருந்து விடுபட செய்ய வேண்டியவை

இணையவெளி துன்புறுத்தல்கள் (Cyber bullying) என்பது உலகின் அனைத்து நாடுகளிலும் வயது வேறுபாடின்றி பெரும்பாலானோர் முகம் கொடுக்கும் ஒரு பிரச்சினையாகும். நாம் எவ்வளவு நன்றாகச் செயற்பட்டாலும், இதனூடாக அதனை வன்மையாக விமர்சித்தல், அச்சுறுத்தல் அல்லது கௌரவத்திற்கு கேடு விளைவித்தல் போன்றவை நேரலாம். பின்வரும் உண்மைச் சம்பவங்கள் இதற்கு நல்ல உதாரணங்களாகும்.

2018 ஆம் ஆண்டில் ஒரு பெண்பிள்ளையும் இன்னுமொரு ஆண் பிள்ளையும் பல்கலைக்கழகத்தில் இடம்பெற்ற விருந்து ஒன்றின் போது நடைபெற்ற போட்டியில் கலந்து கொண்டதை அங்கு வருகை தந்திருந்த உத்தியோகபூர்வப் புகைப்படப் பிடிப்பாளர் தனது புகைப்படக் கருவியின் வில்லையில் பதிவு செய்து கொண்டார்.

ஏனைய புகைப்படங்களுடன் இதுவும் இணையத்தில் வெளியிடப்பட்ட போது, இதனைக் கண்ட தீவிரவாத மதப் பக்தர் ஒருவர் இவ்வாறு பெண் பிள்ளைகள் ஆண் பிள்ளைகளுடன் புகைப்படம் எடுக்கக் கூடாதெனக் கடுமையாக விமர்சித்திருந்தார். பழிச்சொற்கள், துன்புறுத்தல்களுடன், கொலை மிரட்டல்களும் அவளுக்கு விடுக்கப்பட்டமையால் வீட்டிலிருந்து வெளியே செல்வதற்கும் அவள் அஞ்சினாள்.

2017 ஆம் ஆண்டில் இலங்கையில் நடந்த ஒரு வினோத உடைப் போட்டியில் இது நடந்தது. இரண்டு இளம்பெண்கள் திரைப்பட கதாபாத்திரங்கள் போன்று தோற்றமளிக்கும் புகைப்படங்கள் சமூக வலைதளங்களில் வெளியானதையடுத்து, அவர்களின் உடல் தோற்றத்தை பலர் கேலிக்கு உட்படுத்தினர்.

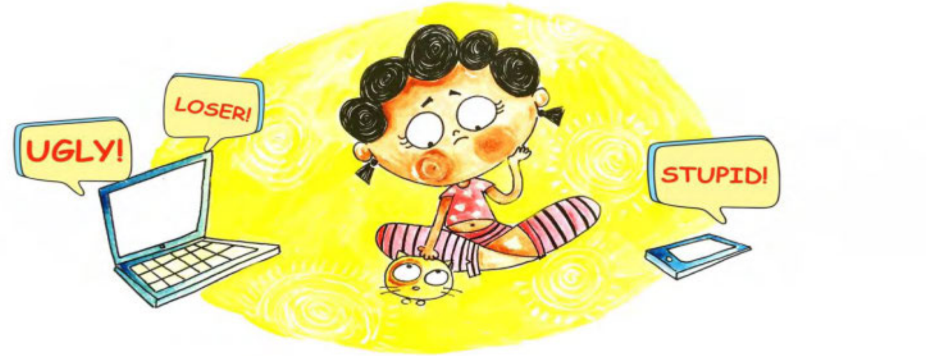
எனினும், அவர்களுக்கு எதிரான வன்முறைக்கு எதிராக, குறிப்பிட்ட கதாபாத்திரத்தில் நடித்த நடிகை அவர்கள் இருவரையும் தனது ட்விட்டர் (இப்போது எக்ஸ்) கணக்கு மூலம் உலகின் முன்னிலையில் பாராட்டியிருந்தார்.

நீங்களும் இது போன்றதொரு சந்தர்ப்பத்துக்கு முகம் கொடுப்பீர்களாயின், குற்றவியல் ஆராய்ச்சித் திணைக்களத்தின் (CID) கணினிக் குற்றப் புலனாய்வுப் பிரிவு (CCID) அல்லது dir.ccid@police.gov.lk அல்லது 0112381045 எனும் தொலைபேசி இலக்கத்தினூடாகவோ தெரிவிக்கவும்.

இணையவெளித் துன்புறுத்தல்களின் (Cyberbullying) தாக்கங்கள்

ஆபாசக் கருத்துக்களைத் தெரிவிப்பது அல்லது பொதுவில் துன்புறுத்தப்படுவது காரணமாக ஒருவருக்கு வலியையோ, கவலையையோ அல்லது கோபத்தையோ ஏற்படுத்தக் கூடும். இது மன அழுத்தம், சோர்வு அல்லது சுயகௌரவம் தொடர்பான பிரச்சினைகளுக்கு வழிவகுக்கும்.

பெரும்பாலானோர் வீட்டில் இருக்கும் போதே தமது தொலைபேசியைப் பாவிக்கின்றனர். வீடு என்பது தமக்குப் பாதுகாப்பான, மன மகிழ்வைத் தரும் இடமான போதிலும், அங்கும் கூட ஆபாச கருத்துக்களையும், துன்புறுத்தல்களையும் (இணையத் தளத்தின் ஊடாக) எதிர்கொள்ளும் நிலை ஆபத்தாக அமைய வாய்ப்புக்கள் அதிகம்.


LOSER!
UGLY!
STUPID!

விலகிச் செல்ல முடிந்தாலும், வார்த்தையால் கூறியதை சிறிது நேரத்தில் மறந்து போனாலும், சமூக ஊடகங்களில் எழுதி பதிவிட்டதை மீண்டும் மீண்டும் வாசிக்க முடிவதால் அவரது மனம் தொடர்ந்தும் அழுத்தத்துக்கு உள்ளாக்கப்படும்.

துன்புறுத்துபவர் அதற்கு முகம்கொடுப்பவரின் (பாதிக்கப்பட்டவர்) எண்ணங்களை/ நடத்தையை தொலைபேசித் திரையின் ஊடாக காண முடியாததால் மென்மேலும் கேலி செய்ய முனைவார். அது பாதிக்கப்பட்டவரின் அழுத்தத்தை மேலும் அதிகரிக்கும்.

அவ்வாறானதொரு சூழ்நிலையில் செய்ய வேண்டியவை

குறித்த நபரை தடை (பிளோக்) (block) செய்யவும்

- பிரச்சினை எல்லை மீறும் முன், ஸ்கிரீன் ஷாட்களை (Screenshots) எடுத்து, பின்னர் அவர்களுடனான தொடர்புகளைத் துண்டித்து (Block) விடவும்.

அவர்கள் சொல்பவற்றைக் கவனத்தில் கொள்ள வேண்டாம்

- நீங்கள் சரியென உங்களுக்குத் தெரியுமாயின், அவர்களின் வார்த்தைகளில் வெளிப்படுவது அவர்களது இயலாமையென்பதைப் புரிந்து கொள்ளுங்கள். அறியாமையால் உங்கள் மூலம் ஏதேனும் தவறு நடந்திருந்தால், சமூக வலைதளங்களால் அல்ல, சட்டத்தின் மூலமே உரிய நடவடிக்கை எடுக்கப்பட வேண்டும் என்பதை நினைவில் கொள்ளுங்கள்.

அவர்கள் பதிவிட்டதை மீண்டும் மீண்டும் வாசிக்க வேண்டாம்.

- அது உங்களுக்குக் கோபத்தை ஏற்படுத்துமே தவிர அதனால் எந்தவித நலனும் ஏற்படப் போவதில்லை. நிகழ்வை report பண்ணவும்.

எல்லோருக்கும் ஒரே மாதிரியான சிந்தனை இல்லை என்பதைப் புரிந்து கொள்ளுங்கள்.

- திட்டுவதாகத் தோன்றினாலும், ஒருவேளை அது அவர்களின் கருத்துகளை வெளிப்படுத்தும் விதமாகக் கூட இருக்கலாம்.

ஆதரவளிக்கும் நிறுவனங்களுக்குத் தெரியப்படுத்துங்கள்

- ஹிதவதி, பெண்கள் மற்றும் சிறுவர் துஷ்பிரயோகத் தடுப்பு பொலிஸ் பணியகம், தேசிய சிறுவர் பாதுகாப்பு அதிகார சபை போன்ற நிறுவனங்களுக்குத் தெரியப்படுத்துங்கள்.

7. சட்டத்தொகுதி உங்களுக்காகத் தயாராக உள்ளது

இப் பிரிவில் உள்ளடங்கும் விடயங்கள்

- கணினி தொடர்பிலான தேசிய கட்டளைச் சட்டங்கள்

போலி மென்பொருட்களைப் பயன்படுத்த வேண்டாம்

2003 இலக்கம் 36ஐக் கொண்ட அறிவுசார் சொத்துரிமைச் சட்டத்தின் 6 (1)(அ) பிரிவின் கீழ் கணினி மென்பொருட்களுக்கு பதிப்புரிமை வழங்கப்படுகிறது. இதனால் நீங்கள் தயாரித்த மென்பொருளை மற்றவர்களால் திருட முடியாது.

அதைப் போன்று மைக்ரோசாப்ட் மற்றும் அடோபி போன்ற நிறுவனங்களின் மென்பொருட்களைத் திருடி (Crack) வியாபார நிறுவனமொன்றில் பயன்படுத்தினால் அந் நிறுவனத்தின் மேலதிகாரிகளுக்கும் அதற்குப் பொறுப்புக் கூற நேரிடும். கடையில் மலிவான விலையில் வாங்கும் குறுந்தட்டுக்கள் (CDs). கூட இதில் அடங்கும்.

ஆபாசக் காட்சிகளைத் தவிர்க்கும் உரிமை உங்களுக்கு உண்டு

சஷேனுக்கு அவனது அண்ணாவின் நண்பன் ஒருவன் தொலைபேசியிலிருந்த சில காணொளிகளைக் காட்டினான். அவற்றில் இருந்தவை ஆபாசமானவை என்பதை உணர அவனுக்கு வெகு நேரம் ஆகவில்லை.

"விருப்பமில்லையா தம்பி இது போல ஒன்றைச் செய்து சம்பாதிக்க? நிரம்பக் காசு தாறன் உங்களுக்கு" என்று அந்த அண்ணா எதுவும் அறியாதவரைப் போலக் கூறினார்.

இலங்கையின் தண்டனைச் சட்டக் கோவை பற்றிய அறிவைக் கொண்டிருந்த சஷேன் அதைக் கடுமையாக எதிர்த்தான். 18 வயதிற்குக் குறைந்த தனக்கு இது போன்ற காணொளிகள் காட்டப்படுவதைப் போலவே, அதில் ஈடுபடுமாறு ஒருவர் அழைத்தால் அவர்களுக்கு 2 வருடத்துக்குக் குறையாத சிறைத் தண்டனை கிட்ட வாய்ப்புண்டு என்பதை அவன் விளக்கினான்.

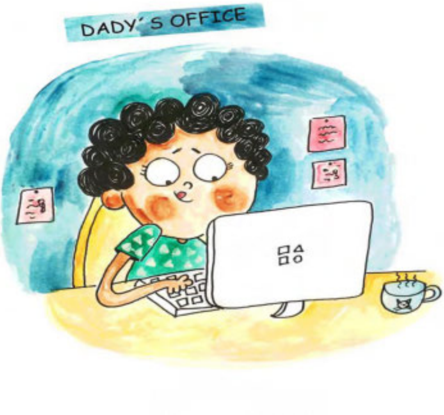
ஒருபோதும் நிர்வாண அல்லது மிகவும் அந்தரங்கமான புகைப்படங்களை எடுக்க வேண்டாம். அவ்வாறான புகைப்படங்களை அடுத்தவர்கள் எடுப்பதற்கு அனுமதியளிக்காதிருக்கும் உரிமையும் உங்களுக்கு உண்டு.

இணைய கஃபேக்களில் துஷ்பிரயோகத்திற்கு இடமில்லை.

2006 இல் இலங்கையின் தண்டனைச் சட்டக் கோவையில் சேர்க்கப்பட்ட திருத்தத்தின் (2006 இலக்கம் 16 ஐக் கொண்ட தண்டனைச் சட்டக் கோவை (திருத்தங்களுடன் கூடிய) சட்டம்) மூலம் பிள்ளைகள் பாலியல் துஷ்பிரயோகத்துக்கு உள்ளாவதைத் தடுப்பதற்குப் பொறுப்புடையவர்களாக கணினிச் சேவை வழங்குநர்களை (உதாரணத்திற்கு:- சைபர் கேஃபேக்கள்) அடையாளம் காட்டுகிறது.

தமது கணினியின் ஊடாக ஒரு பிள்ளை பாலியல் துஷ்பிரயோகத்திற்கு ஆளாகின்றார் எனின், அவர் அது குறித்து அருகில் உள்ள காவல் நிலையத்துக்குத் தெரிவிக்க வேண்டும். அல்லாது விடில் அவருக்கு 2 ஆண்டுகள் சிறைத் தண்டனையும்/ அல்லது அபராதமும் விதிக்கப்படலாம்.

அடுத்தவரின் கணினிகள் / தொலைபேசிகளைத் தொட வேண்டாம்



பாடசாலை விட்டு வந்து, அப்பா வேலை செய்து முடியும் வரை அவர் பணியாற்றும் அரச அலுவலகத்தில் காத்திருக்கும் சுபுனுக்கு அங்கிருக்கும் கணினிகளில் உள்ளவற்றை பார்க்க ஆவலாக இருந்தது.

அவற்றில் இருந்த வாடிக்கையாளர் சந்தா விபரங்கள், போக்குவரத்துத் தரவுகள் போன்ற அனைத்தையும் பார்க்க சுபுன் முயற்சி செய்கையில் அதனைக் கண்ட அவனது அப்பா எச்சரித்தார்.

மகன், கணினிக்கோ அல்லது கணினியில் உள்ள தகவல்களுக்கோ பிரவேசிப்பதற்கு உனக்கு சட்ட ரீதியான உரிமை இல்லையென்பதை நன்றாக அறிந்திருந்தும் அதனுள் அனுமதியின்றி பிரவேசித்தல் 2007 இலக்கம் 24 ஐக் கொண்ட இலங்கை கணினி குற்றவியல் சட்டத்துக்கு அமைய பெரும் குற்றமாகும். அவற்றில் அனுமதியற்ற மாற்றங்களைச் செய்தல், சேதத்தை ஏற்படுத்தல், கடவுச் சொற்களை மற்றவர்களுக்குக் கொடுத்தல் போன்ற பல விடயங்கள் அதன் கீழ் உள்ளடங்கும். அதனால் ஒருநாளும் உனக்குச் சொந்தமில்லாத கணினிகளில் எதுவும் செய்யாதே, சரியா?

அப்பாவின் விளக்கத்தைச் சுப்புன் ஏற்றுக்கொண்டான். அதனால் சிறைத் தண்டனையிலிருந்தும், அபராதத் தொகையிலிருந்தும் அவனால் தப்பிக்க முடிந்தது.

ஒருவர் கடவுச்சொல்லை தட்டச்சிடும் போது கூட நாம் வேறு புறம் திரும்பியிருக்கப் பழகிக் கொள்ள வேண்டும். அது ஒரு சிறந்த தனி மனிதப் பண்பாகும்.

2024 ஆம் ஆண்டின் 9 ஆம் இலக்க நிகழ்நிலைப் பாதுகாப்புச் சட்டம், தவறான அறிக்கைகளை வெளியிடுவது, வேறு ஒருவராக நடிப்பது, மற்றொருவரின் தனிப்பட்ட தகவல்களை வெளியிடுவது, இணைய விசாரணைகளில் சாட்சியங்களை மாற்றுவது போன்றவற்றை உள்ளடக்கியது.

8. உளநலச் சிக்கல்களுக்கு வழிகோலும் இணையவெளிக் குற்றங்கள்

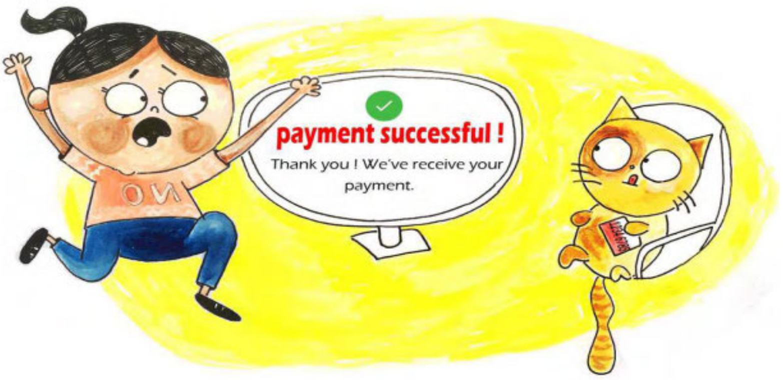
இப் பிரிவில் உள்ளடங்கும் விடயங்கள்

- ஏற்படக்கூடிய உளநலக் கோளாறுகள் மற்றும் அவற்றைத் தீர்ப்பதற்கு மேற்கொள்ள வேண்டியவை

ஒரு நாள் சகன் இணையத்தில் உலாவும்போது அவன் அந்த இணையத் தளத்துக்கு வந்த 1,000,000,000 நபராவதால் அமெரிக்க குடியுரிமை கிடைப்பதாக ஒரு இணையத் தளத்தில் இருந்தது. ஆனால் அதற்கு ஒரு சிறிய கட்டணமொன்றைச் செலுத்த வேண்டுமெனவும் குறிப்பிட்டிருந்தது. மகிழ்ச்சியில் திளைத்த சகன் குறித்த தொகையை அவரது கிரெடிட் அட்டையின் மூலம் செலுத்தினார்.

"நான் இப்போது அமெரிக்காவுக்குச் செல்லப் போகிறேன். இப்போது நான் கரை சேர்ந்து விட்டேன்!" என சகன் தன் நண்பர்கள் அனைவருக்கும் கூறினான். ஊராரும் அவருக்கு வாழ்த்துக்களைத் தெரிவித்தனர்.

ஆனால் அதன் பிறகு அவருக்கு அது பற்றிய எந்த தகவலும் கிடைக்கவில்லை. அவரது அட்டையின் ஊடாகச் செலுத்திய தொகைக்கு மேலதிகமாக பல தடவைகள் தானியங்கியாக ஒரு இலட்சத்துக்கு அண்மித்த தொகை செலுத்தப்பட்டிருப்பதாக வங்கியிலிருந்து வந்த அழைப்பில் தெரிவிக்கப்பட்டது.


payment successful !
Thank you ! We've receive your payment.
ON

சகன் சமூகத்துக்கு முகம் கொடுக்கச் சங்கடப்பட்டான். நண்பர்களின் கேலிப் பேச்சுக்களுக்கும் முகம் கொடுக்க நேர்ந்தது.

கோபம், மோசடிக்கு ஆளாகியமை, ஏமாற்றம், அவமதிப்பு மற்றும் நிராதரவு (ஆற்றாமை) போன்ற பல உணர்வுகள் சகனின் முழு மனதையும் ஆக்கிரமித்தது.

மோசடி செயல்களுக்கும், அவமானங்களுக்கும் அஞ்ச வேண்டாம்

சமூக ஊடகங்களைச் சார்ந்து

- போலி காதல் உறவுகள்
- துஷ்பிரயோகம்
- ஏமாற்றியோ அல்லது மிரட்டிக் கப்பமாகவோ பணத்தைப் பெறுதல்
- கடிந்துரைத்தல் (Hate speech)
- துன்புறுத்தல் (ஏளனம் செய்தல்) (Cyberbullying)

தொடர்பில் பல சம்பவங்கள் இடம்பெற்று வருகின்றன. இவற்றுக்கு முகம் கொடுக்க நேர்கையில், முறையான உளநல ஆலோசனை கிட்டாமல் போனால் உயிர் இழப்புகள் கூட நேரலாம்.

எனவே, அது போன்றதொன்றுக்கு முகம்கொடுக்க நேர்ந்தால் எந்தவேளையிலும் அதற்கு அஞ்ச வேண்டாம். தேவையான சட்ட நடவடிக்கைகளை எடுத்து அப் பிரச்சினையை நேரடியாக எதிர்கொள்ளுங்கள்.

மௌனம் வஞ்சகர்களுக்கு ஊக்கமளிக்கும்

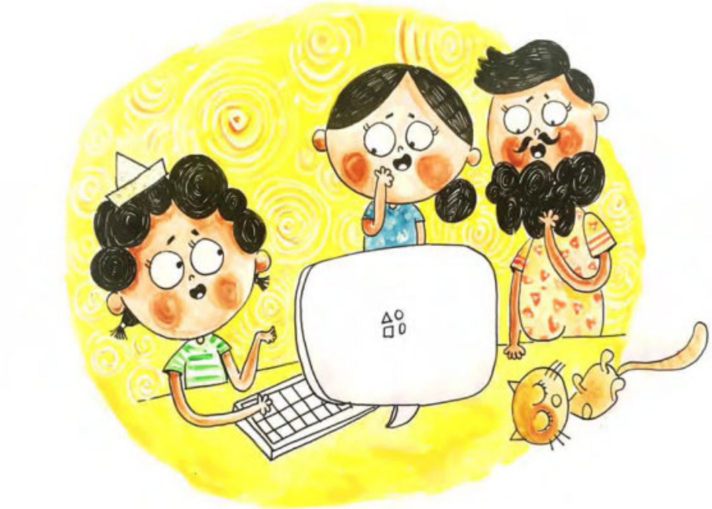
சமூக ஊடகங்கள் தொடர்பான உண்மை நிகழ்வுகள் குறித்து hithawathi.lk எனும் இணையதளத்தில் உள்ள தகவலைப் பார்க்கவும். இந்த QR குறியீட்டை ஸ்கேன் செய்யவும்.

https://www.hithawathi.lk/ta/help-center-ta/news-papers-ta/

வயதில் மூத்தவர்களுக்குத் தெரிவிக்கவும்

நீங்கள் இது போன்ற சிக்கலுக்கு முகம் கொடுப்பீர்களாயின் உடனடியாக ஆசிரியருக்கு, வயதில் மூத்தவருக்கு இது பற்றித் தெரிவிக்கவும். இந்த கைநூலின் இறுதியில் நீங்கள் உதவியை நாடக் கூடிய நிறுவனங்கள் / அமைப்புகளின் தொலைபேசி இலக்கங்கள் உள்ளன.

சமூக ஊடகங்களால் அறிவு, சமூகத் திறன்கள், படைப்பாற்றல், கல்வி சாதனை, பல்வேறு கலாச்சாரங்கள், மதங்கள் தொடர்பான அறிவு வளர்ச்சி மற்றும் சுய மதிப்பைக் கட்டியெழுப்பல் போன்ற பல நன்மைகள் கிட்டுகின்றன. ஆகவே சமூக ஊடகங்களையும் இணையத் தளங்களையும் எப்போதும் புரிந்துணர்வுடன் பாவிக்கப் பழகிக் கொள்ளுங்கள்.



ரந்திமாவின் முகநூல் கணக்கில் இருந்த நண்பர் ஒருவர் அடிக்கடி அவளது சுக நலன்களை விசாரித்து மிகவும் நெருக்கமானார். பேசுவதற்கு நண்பர் ஒருவர் கிடைத்ததையிட்டு மகிழ்ச்சியடைந்த அவள் படிப்பையும் மறந்து ஒருநாளும் கண்டிராத நண்பருடன் அரட்டையடிக்க முனைந்தாள். தனது பிரச்சனைகளைப் பகிர்ந்து கொள்வதற்கு நண்பன் ஒருவன் கிடைத்ததையிட்டு அவள் மிகவும் மகிழ்வடைந்தாள். படிப்படியாக இருவருக்கும் இடையே காதல் அரும்பியது.

எனினும், அந்தக் காதலை நிரூபிப்பதானால் சினிமா திரையரங்குகள் போன்ற பல்வேறு இடங்களுக்கு வந்து அடிக்கடி சந்திக்க வேண்டுமென அந்த நண்பர் கூறினார்.

இது குறித்து சந்தேகித்த அவள் விரைந்து தன் தாயிடம் முழு விபரத்தையும் கூறினாள். ஹிதவதி போன்ற இணையதளங்களின் ஊடாக இணையங்களில் இடம்பெறும் மோசடிகள் குறித்து சிறந்த அறிவைக் கொண்டிருந்த அந்தப் புத்திசாலிப் பெற்றோர் ரந்திமாவுக்கு

அது குறித்து இவ்வாறு விளக்கமளித்தனர்.

மகள், மனதில் உள்ளதைக் கூறுவதற்கு நண்பர் ஒருவர் இருப்பது நல்லதுதான். அதுவும் 17 வயது நிறைந்த உனக்கும் ஆண் பிள்ளைகள் மீது ஈர்ப்பு ஏற்படுவது இயல்பான ஒன்றுதான்.

எனினும் அந்தச் சந்தர்ப்பத்தைத் தமக்கு சாதகமாக்கி நம் வாழ்வையே அழிப்பதற்குப் பெரிய கும்பல் ஒன்று காத்திருக்கிறது. கவலைகளைக் கேட்டறியும் தோரணையில் அவர்கள் இன்னும் நிறைய கஷ்டங்களைக் கொடுத்து விட்டுத்தான் அவர்கள் நம்மை விட்டு அகன்று செல்வர்.

நீ இதைப் பற்றி எங்களிடம் முன்பே கூறியதையிட்டு மகிழ்ச்சி அடைகிறோம். அவரது சுயவிவரம் (புரோபைல்) குறித்து நாம் பொலிசிடம் முறைப்பாடு செய்வோம். உன்னுடன் அரட்டை அடித்தவற்றையும் ஸ்கிரீன் ஷாட் (Screenshot) எடுத்து சாட்சியமாக அனுப்ப வேண்டும். அப்போதுதான் மீண்டும் உன்னைப் போன்ற அப்பாவிப் பிள்ளைகளை பலி எடுக்க அவர்களுக்கு வாய்ப்புக் கிடைக்காது. நாம் வாயை மூடிக் கொண்டிருந்தால் இன்னும் இது போன்ற மிகப் பயங்கரமான விடயங்கள் இடம்பெறக் கூடும்.

9. தொழில்நுட்பம் என்பது மிகவும் பெறுமதி வாய்ந்ததொன்றாகும்.

இப் பிரிவில் உள்ளடங்கும் விடயங்கள்

- இணையத் தளமென்பது அச்சம் கொள்ள வேண்டிய ஒன்றல்ல எனவும்
- சரியான அறிவைக் கொண்டிருந்தால் எந்தவொரு பிரச்சினையையும் தீர்க்க முடியும் எனவும்

தாயுடன் ஞாயிறு சந்தைக்குச் சென்ற சசந்தி சனக் கூட்டத்திடையே தனது தாயைத் தவறவிட்டாள். அங்குமிங்கும் அலைந்து திரிந்து தாயின் முகம் தென்படுகிறதா என ஒவ்வொரு முகத்தையும் உற்றுப் பார்த்துக் கொண்டிருக்கையிலே, தன்னையும் அறியாமல் கண்கள் கண்ணீரால் நனைய ஆரம்பித்தன.

அதிர்ஷ்டவசமாக அவளது ஆசிரியரும் அன்று சந்தைக்கு வந்திருந்ததால் தற்செயலாக சசந்தியைக் கண்டார்.

ஆசிரியர் – பிள்ளை, ஏன் நீ தனியாக இருக்கிறாய்?

சசிந்தி – ஐயோ, டீச்சர், நான் எனது தாயைத் தவற விட்டு விட்டேன். தேடிப் பிடிக்க முடியவில்லையே.

ஆசிரியர் - நீ அம்மாவுக்குக் கோல் ஒண்டு எடுத்துப் பார்க்கவில்லையா மகள்?

சசிந்தி - என்னிடம் போன் இல்லையே டீச்சர், அது பிள்ளைகளுக்கு நல்லதல்ல என்று அம்மா சொல்லுவாங்க.

ஆசிரியர் - அது ஒரு தவறான கருத்து மகள், கவனமாகப் பாவிக்கும் விதத்தை உனக்குக் கற்றுக் கொடுக்க வேண்டுமே தவிர தொழில்நுட்பத்திலிருந்து விலக்கி வைப்பது நல்லதல்ல. இருங்களேன் நான் கோல் எடுக்கிறன். கொஞ்சம் கூட பயப்பட வேண்டாம் மகள் சரி தானே?

பென்சில் என்பது நாம் அனைவரும் எழுதக் கற்றுக் கொள்ள உபயோகிக்கும் ஒன்றாகும். ஆனால் ஜான் விக்கின் John Wick திரைப்படத்தைப் பார்த்த ஒருவர் பென்சிலைக் கொலை செய்யும் ஆயுதமாக அர்த்தப்படுத்தினால் இந்த உலகில் எந்தவொரு பிள்ளைக்கும் எழுத முடியாது போகும்.

பல வயதில் மூத்தவர்கள் அவர்களுக்குத் தொழில்நுட்பம் பற்றிய அறிவு குறைவாக உள்ளதாலும், சில ஊடகங்களால் உணர்ச்சிப்பூர்வமாக அறிக்கையிடும் விடயங்களாலும் இணையத்தளத்தையும் கணினியையும் ஒட்டுமொத்தத் தொழில்நுட்பத்தையும் பயங்கரமானதொன்று என சமூகத்திடையே கெட்ட கருத்தொன்றை உருவாக்கி வருகின்றனர்.

எனினும், ஹிதவதி நிகழ்ச்சித் திட்டம் கொண்டு வரும் இந்தக் கைநூலை வாசித்த உங்களுக்கு இப்போது எந்தவொரு பிரச்சனையையும் எதிர் கொள்வதற்குத் தேவையான அறிவு உள்ளது. இங்குள்ள ஆங்கிலச் சொற்களைத் தேடிப் பார்த்து இன்னும் அறிவை வளர்த்துக் கொள்வதற்கும், எந்தவொரு இணையத்தின் ஊடாகவும் தேடிப் படித்து எதிர்காலத்தில் உருவாகும் தொழில்நுட்பம் பற்றிய தமது அறிவை வளர்த்துக் கொள்ளும் பழக்கமும் உங்களுக்குக் கிடைக்கும்.

பொறுப்புடன் பாவிப்போம்

இணையத்தைப் பாவிக்கும் போது தமது பாதுகாப்பைப் போலவே மற்றவரின் பாதுகாப்புப் பற்றியும் நாம் சிந்திக்க வேண்டும். முன்னைய அத்தியாயங்களில் விவரிக்கப்பட்டுள்ளவாறு உங்கள் மனம் புண்படுமாறு பேசும் ஒருவரிடமிருந்து விடுபட வேண்டுமே தவிர திரும்பி அவர்களைத் தாக்கினால் நீங்களும் ஒரு இணையவெளி துன்புறுத்துபவராக (Cyberbullying) நேரிடும்.

நல்ல பழக்கங்களைக் கற்றுக் கொள்வோம்

உங்களது தரவுகளைப் போன்றே மற்றவர்களின் தரவுகள், கடவுச்சொற்கள் போன்றவற்றுக்கு அதிகபட்ச பாதுகாப்பை வழங்குவதற்கும், வேறொருவர் கடவுச்சொல்லை தட்டச்சிடும் போது பார்வையை வேறு புறம் திருப்பிக் கொள்ளுதல் போன்ற நல்ல பழக்கங்களை உருவாக்கிக் கொள்வோம்.

நீங்கள் பழக்கப்படுத்திக் கொள்ள வேண்டிய சில நற் பழக்கங்கள் கீழே காட்டப்படுகின்றன.

நான் ஒருபோதும் இணையத்தின் ஊடாக அடுத்தவரைத் துன்புறுத்த மாட்டேன்.

நான் இணையத்தின் ஊடாக மற்றவரின் படைப்புகளைத் திருட மாட்டேன்.

நான் அடுத்தவரின் சாதனத்திலிருந்து தனிப்பட்ட தகவல்கள், புகைப்படங்கள் போன்றவற்றைத் திருட மாட்டேன்.

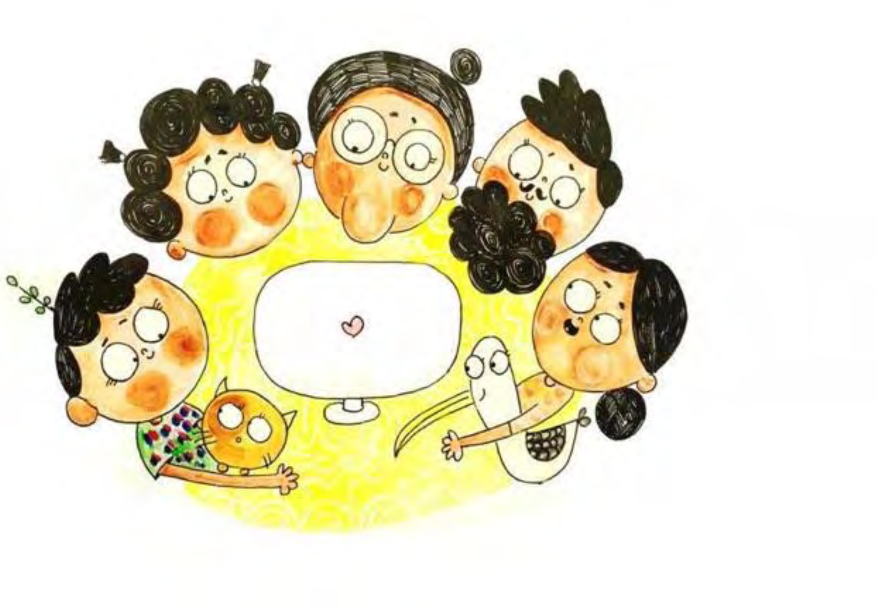
நான் இணையத்தின் ஊடாக எதையும் செய்வதற்கு முன், அதனால் ஏற்படக் கூடிய பின்விளைவுகள் குறித்து ஒருமுறைக்கு இருமுறை சிந்திப்பேன்

நான் இணையத்திலிருந்து அதிக பட்சமாகப் பெற்றுக் கொள்ளக் கூடிய சிறந்த பயன்களைப் பெற்று எனது அறிவை வளர்த்துக் கொள்வேன்.

இணையத்தினுள் சிறந்த பிரஜைகளாக இருப்போம்

நாம் சமூகத்தில் வாழும்போது பொதுநலமாகவும், நிதானத்துடனும் செயற்பட்டு கல்வியில் முன்னுக்குச் சென்று நாட்டுக்குச் சேவை ஆற்றுவதுடன், இணையத்தினுள்ளும் சிறந்த பிரஜையாக ஆகினால் அது அனைவருக்கும் பயனளிக்கக் கூடிய அறிவுச் சுவர்க்கமாக அமையும்.

இப்போது நீங்களும் பொறுப்புள்ள ஒரு சிறந்த இணைய பிரஜை ஆவீர்



10. இணையவெளி துன்புறுத்தல்களுக்கு முகம் கொடுத்தால் நீங்களும் அழையுங்கள்

ஹிதவதி செயற்றிட்டம்

தகவல் தொழில்நுட்பம் மற்றும் இணையத்துடன் தொடர்புடைய செயல்பாடுகளால் சிரமத்திற்கு ஆளாகிய அல்லது சித்திரவதைகளுக்கோ, தொந்தரவுகளுக்கோ இரையாகியவர்களுக்கு உதவிச் சேவைகளை வழங்குவதற்காக மூன்று மொழிகளிலும் (சிங்களம்/தமிழ்/ஆங்கிலம்) ஹிதவதி திட்டம் அர்ப்பணிப்புடன் உள்ளது. இது இணைய சங்கத்தின் இலங்கை அத்தியாயம் (ISOC-LK) மற்றும் LK டொமைன் பதிவேடு (LK Domain Registry) எனும் நிறுவனங்களின் உறுப்பினர்களால் செயல்படுத்தப்படுகிறது.

முக்கியமாக குழந்தைகள், கட்டிளம் பருவத்தினர், இளைஞர் மற்றும் பெண்களை இலக்காகக் கொண்டிருந்தாலும், எவரொருவருக்கும் இதன் மனமார்ந்த

உதவியைப் பெற்றுக் கொள்வதற்கான வாய்ப்பிருத்தல் இதன் தனிச்சிறப்பாகும்.

தொலைபேசி இலக்கம்: 011 421 6062
மின்னஞ்சல்: help@hithawathi.lk
வாட்ஸ் அப் மற்றும் வைபர்: +94 77 771 1199
இணையத்தளம்: www.hithawathi.lk

இலங்கை கணினி அவசர தயார்நிலை அணி | ஒருங்கிணைப்பு மையம்

அறை இலக்கம் 4-112, பண்டாரநாயக்க சர்வதேச
மாநாட்டு மண்டபம், பௌத்தாலோக மாவத்தை, கொழும்பு
07.

தொலைபேசி: +94 11 269 1692, அவசர அழைப்பு எண்: 101
மின்னஞ்சல்: cert@cert.gov.lk
இணையத்தளம்: www.cert.gov.lk

தேசிய சிறுவர் பாதுகாப்பு அதிகார சபை

தேசிய சிறுவர் பாதுகாப்பு
அதிகார சபை,
இலக்கம்.330,
தலவத்துகொடை வீதி,
மாதிவெலை,
ஸ்ரீ ஜயவர்த்தனபுர.

தொலைபேசி: +94 11 2 778 911 - 4

அவசர அழைப்பு இலக்கம்: 1929
மின்னஞ்சல்: ncpa@childprotection.gov.lk
இணையத்தளம்: www.childprotection.gov.lk

இலங்கை பொலிஸ் இணையக் குற்றப் புகார் மையம்

அவசர அழைப்பு எண்: 119, 118
இணையத்தளம்: www.police.lk
இணையத்தள முறைப்பாடுகளுக்கான
இணைய இணைப்பு: www.telligp.police.lk

குற்றப் புலனாய்வுத் திணைக்களத்தின் கணினி குற்றப் புலனாய்வுப் பிரிவு

தொலைபேசி இலக்கம்: 011 238 1045
மின்னஞ்சல் முகவரி: dir.ccid @police.gov.lk

குழந்தைகள் மற்றும் பெண்கள் துஷ்பிரயோகத் தடுப்புப் பணியகம்

இலக்கம்: 78, முதலாம் மாடி, முக்தார் பிளாஸா
கட்டடம், கிரேன்ட்பாஸ் வீதி, கொழும்பு 14.
தொலைபேசி: 011 244 4444, அவசர அழைப்பு எண்: 109
மின்னஞ்சல்: cwb.online@police.gov.lk
இணையத்தளம்: www.police.lk/?page_id=14746

பெண்கள் உதவி

ஆலோசனை சேவை எண்: 077 567 6555
சட்ட சேவை: 076 868 655
மின்னஞ்சல்: connect@winsl.net
இணையத்தளம்: www.winsl.net

கலைச் சொற்களஞ்சியம்

Privacy Policy - பிரைவசி பொலிசி

இரகசியக் கொள்கை என்பது ஒரு தரப்பினரால் தனது வாடிக்கையாளரின் அல்லது சேவை பெறுநர்களின் தரவுகளைச் சேகரித்து, அவற்றைப் பயன்படுத்தும் விதத்தையும், முகாமைத்துவம் செய்யும் முறையையும் வெளிப்படுத்தும் ஒரு கூற்று அல்லது ஒரு சட்ட ஆவணம்.

Malicious software / Malware - மெல்வெயார்

தீங்கு மென்பொருள் என்பது, ஒரு கணினித் தொகுதிக்குள் அத்துமீறி நுழைவதற்கு, தொகுதியை சீர்குலைப்பதற்கு, சேதப்படுத்துவதற்கு அல்லது தரவுகளைப் பெற்றுக் கொள்வதற்கு விசேடமாக வடிவமைக்கப்பட்டுள்ள மென்பொருளாகும்.

Spam - ஸ்பேம்

ஸ்பேம் என்பது வர்த்தக விளம்பரங்களை அனுப்புதல், தீங்கு மென்பொருட்களைப் பரப்புதல் போன்றவற்றுக்கு சாதாரணமாக பெருமளவு பயனர்களுக்கு ஒரே தடவையில் இணையத்தினூடாக அனுப்பப்படும் தேவையற்ற மின்னஞ்சல் செய்திகளாகும்.

Botnet - பாட்நெட்

தீங்கு மென்பொருட்களிலிருந்து தாக்கப்படும் மற்றும் உரிமையாளர்களின் அனுமதியின்றி குழுவாக கட்டுப்படுத்தப்படும் தனிப்பட்ட கணினி வலையமைப்பாகும். உதாரணமாக: ஸ்பேம் மின்னஞ்சல்களை அனுப்புவதற்கு

Ransomware - ரென்சம்வெயார்

பணம் செலுத்தும் வரை கணினித் தொகுதிக்குள் பிரவேசிப்பதை தடங்கல் செய்வதற்காக வடிவமைக்கப்பட்ட ஒரு வகையான தீங்கு மென்பொருளாகும். இவை கோப்புக்களை குறியீடுகளாக்கி பயன்படுத்த முடியாத நிலைக்கு உட்படுத்தக் கூடிய தீங்கு மென்பொருள் வகையாகும்.

Hate speech - வெறுப்பு பேச்சு

முக்கியமாக சாதி, மதம் அல்லது பாலியல் வேறுபாட்டை அடிப்படையாகக் கொண்டு குறித்த குழுவுக்கு எதிராக தவறான அபிப்பிராயத்தை வெளிப்படுத்துவதற்காக ஆபாசமாக அல்லது அச்சுறுத்திப் பேசுதல் / காண்பித்தல்.

Cyberbullying - சைபர் மிரட்டல்

ஒருவரைத் துன்புறுத்துவதற்காக இலத்திரனியல் தொலைத் தொடர்பு சாதனங்களைப் பயன்படுத்தி பயமுறுத்துதல் அல்லது அச்சுறுத்தும் விதத்தில் செய்திகளை அனுப்புதல்.

IMEI number - இமி எண்

தொலைபேசி சாதனங்களை வேறுபடுத்தி இனங்காண்பதற்காக வழங்கப்பட்டுள்ள ஒரு தனித்துவமான (unique) எண் ஆகும். செருகிக் கொள்ளக் கூடிய சிம் அட்டைகளின் எண்ணிக்கைக்கு ஏற்ப சாதனத்துக்கு இருக்கும் இமி இலக்கமும் தீர்மானிக்கப்படலாம்.

QR code - கியூவ் ஆர் குறியீடு

ஸ்மார்ட் கையடக்கத் தொலைபேசியில் கேமரா மூலம் வாசிப்பதற்காக இணைய முகவரிகளையோ அல்லது ஏனைய தகவல்களையோ களஞ்சியப்படுத்திக் கொள்ளக் கூடிய இயந்திரவியல் குறியீடாகும். பிளே ஸ்டோர் Play Store அல்லது ஆப் ஸ்டோருக்குச் App Store சென்று “qr code scanner” எனத் தேடி அவ்வாறான செயலிகளைத் தாபித்துக் கொள்ளலாம்.

உசாத்துணை

இந் நூல் தொகுப்பில் பின்வரும் மூல ஆதாரங்கள் பயன்படுத்தப்பட்டன.

- பயனுள்ள மற்றும் பாதுகாப்பான டிஜிட்டல் தொழில்நுட்பத்தைப் பயன்படுத்துவதன் மூலம் பாதுகாப்பான பாடசாலை கல்வி - பயிற்சி கையேடு
- தினமின பத்திரிகை
- ஹித்தவத்தி இணையத்தளம் (www.hithawathi.lk)
- www.stopbullying.gov
- www.freepik.com

உங்கள் அறிவை சோதித்து பார்க்கவும்

இந்த கைநூலில் இருந்து பெற்றுக் கொண்ட அறிவையும், உங்களது நாளாந்தப் பிரச்சினைகள் தொடர்பாகவும் பெற்றுக் கொண்ட தேடல் அறிவைப் பயன்படுத்தி ஹித்தவத்தி இணையதளத்தில் உள்ள வினாத் தொடருக்கு விடையளித்து இணையவெளிப் பாதுகாப்புப் பற்றிய உங்களது அறிவின் மட்டத்தைச் சோதியுங்கள்.

1. உங்கள் தொலைபேசியை விற்பதற்கு முன், அதன் தரவுகளைப் பாதுகாப்பதற்காக மேற் கொள்ள வேண்டிய சரியான நடவடிக்கையைத் தெரிவு செய்யவும்.
   - a. தொலைபேசியின் கடவுச்சொல்லை மாற்றுதல்.
   - b. எல்லா தரவுகளையும் அழித்து விடுவதற்கு Factory reset செய்தல்
   - c. வால்பேப்பரை மாற்றுதல்
   - d. சிம் அட்டையினை அகற்றுதல்

2. இணையத்தின் ஊடாக யாராவது உங்களை திட்டினால், நீங்கள் அதற்கு உடனடியாக பதிலளிக்க வேண்டுமா?
   - a. ஆம்
   - b. இல்லை

3. கீழ்வருவனவற்றில் ஹித்தவத்தி அமைப்பால் நிறைவேற்றப்படாதது எது?

a. பெண் பிள்ளைகளுக்கு மட்டும் உதவியளித்தல்

b. ஆலோசனை சேவைகளை வழங்குதல்

c. சட்ட நடவடிக்கைகளை எடுப்பதற்கு உதவுதல்

d. அழைப்புச் சேவையொன்றை நடத்திச் செல்லல்

4. இரட்டைக் காரணி அங்கீகாரம் (Two-factor Authentication / 2FA) என்றால் என்ன?

a. ஒரு தீங்கு மென்பொருள்

b. ஒரு குறுஞ் செய்தி

c. ஃபிஷிங்கிற்காக அனுப்பப்படும் செய்தியொன்று

d. கடவுச்சொல்லுக்கு மேலதிகமாக தனித்துவத்தை உறுதிப்படுத்தும் ஒரு முறையாகும்.

5. உங்கள் புகைப்படத்தை அனுமதியின்றி வெளியிட்டிருந்தால் அதற்கு எதிராக எடுக்கக் கூடிய சிறந்த நடவடிக்கை என்ன?

a. கருத்து (கமென்ட்) தெரிவிப்பதன் ஊடாக திட்டுதல்.

b. மெசேஜ் செய்து அதை நீக்கச் சொல்லுவது.

c. முறையீடு செய்தல் அல்லது ஹித்தவத்தி திட்டத்திற்கு அறிவித்தல்

d. நிரந்தரமாக சமூக வலையமைப்புக்களின் பாவனையைத் தவிர்த்தல்

6. வலுவான கடவுச் சொல் என்பது?

a. உங்களது தொலைபேசி இலக்கம்

b. உங்கள் பிறந்த தினம்

c. வாக்கியத்தில் முதலெழுத்துக்கள் மற்றும் எண்களின் கலவை

d. பெயருக்கு முன்னால் 123 என குறிப்பிடல்

7. நிகழ்நிலையில் சிறுவர் மற்றும் இளைஞர்கள் முகங்கொடுக்கின்ற அபாயம் அல்லாதது

a. சைபர்புல்லிங்

b. இணையத்திற்கு அடிமையாதல்

c. சைபர் குற்றங்களுக்கு உட்படுதல்

d. இணையத்ினூடான கற்றல்

8. இணைய உலாவல் தொடர்பான தவறான கூற்று

a. குற்றச் செயல்களில் ஈடுபடுகின்ற போலிக் கணக்கொன்றின் பின்னணியில் உள்ள நபரை கண்டுபிடிக்க முடியாது.

b. நாம் அறிந்திராத பல விடயங்களை இணையத்தினூடாக கற்க முடியும்.

c. சிலர் இணையத்தை தவறாகப் பயன்படுத்தி மற்றவர்களை ஏமாற்றி துஷ்பிரயோகம் செய்கின்றனர்.

d. இணையவெளியில் எவ்வாறு பாதுகாப்பாக இருக்க வேண்டும் என்பதனை ஹித்தவத்தி உங்களுக்கு அறியப்படுத்துகிறது.

9. இணையம்/ சமூக ஊடகத்துக்கு அடிமையாதல் பற்றிய தவறான கூற்றைத் தெரிவுசெய்யவும்

a. குக்கிஸ் மூலம் இணையத்தில் நீங்கள் பார்வையிடும் இணையத்தளங்களையும் விருப்பங்களையும் வணிகர்கள் இனங்காண்கின்றனர்.

b. சமூக ஊடகம்/ இணையம் உங்களை எல்லாச் சந்தர்ப்பங்களிலும் நன்மைகளை செய்ய ஊக்கமளிக்கின்றன.

c. கடந்த காலத்தில் நீங்கள் தேடிய விடயத்துடன் தொடர்புடைய கவர்ச்சிகரமான விளம்பரங்கள்/ முன்மொழிவுகள் இன்னும் தோன்றலாம்.

d. சமூக வலைப்பின்னலானது எமது மனத்தின் செயற்பாடுகளை அவதானித்து கவனம் செலுத்த முயற்சிக்கின்றன.

10. இணைப்புகளை (லிங்க்ஸ்) அழுத்தும் போது அல்லது இணைப்பினை பதிவிறக்கம் செய்யும் போது நீங்கள் ஏன் கவனமாக இருக்க வேண்டும்

a. அவை உங்கள் கணினியை பாதிக்கின்ற வைரஸ்களைக் கொண்டிருக்கலாம்.

b. அவை பொருத்தமற்ற விடயங்களை உள்ளடக்கியிருக்கலாம்.

c. இதன் மூலம் உங்கள் கணினியின் தகவல்களைத் திருடுவதற்கும் வாய்ப்புள்ளது.

d. மேற்குறிப்பிட்ட அனைத்தும்

பதில்கள்

(1-b, 2-b, 3-a, 4-d, 5-c, 6-c, 7-d, 8-a, 9-b, 10-d)

தேச எல்லைத் தடைகளைக் கடந்து, உலகை ஒரு தனித் தொகுதியாக மாற்றுவதில் தகவல் தொழில்நுட்பம் ஆற்றியுள்ள சேவைகள் அளப்பரியதாகும். தற்போது உலகளாவிய கிராமிய எண்ணக்கரு, உலகளாவிய குடும்ப எண்ணக்கரு என்பன எம் கண்முன்னே யதார்த்தமாக மாறிக் கொண்டிருக்கின்றன. நம் பார்வையிலே உலகளாவிய கிராமமென்பது அழகானதொரு எண்ணக்கருவாகும். அந்த அடிப்படையில் உலகம் என்பது ஒரு கிராமமாகும். பிரச்சனை அதுவல்ல. அருகில் செல்லச் செல்ல நன்மைகளைப் போலவே தீமைகளும் கணப்பொழுதில் உருவாகின்றன. அழிவுகரமான வைரஸ்களும் கூட கணப்பொழுதில் பரவுகின்றது. உலகை ஒரு கிராமமாக்கும் இணைய வெளியினூடாக நவீன அறிவு, அன்பு, பாசம், கருணை, நட்பு, போன்ற உன்னதமான மனிதாபிமானங்களைப் போன்றே உளவியல் வைரசுகளும் பரவிச் செல்லாம். சுருக்கமாகக் கூறின் இவை உலகை அழிவுப் பாதைக்கு இட்டுச்செல்கின்றன. தகவல் தொழில்நுட்ப வசதிகளை விஸ்திகரிப்பதுடன், அது தொடர்பான அறிவியல் ரீதியான அறிவுடன், அவ் வசதிகளை பாதுகாப்பாகப் பயன்படுத்துவது பற்றிய அறிவையும் மென்மேலும் வழங்குவது மிகவும் முக்கியமானதாகும். அந்த வகையில் நோக்கும் போது "ஹிதவத்தி" யினால் பிரசூரிக்கப்படும் "இணையவெளிப் பாதுகாப்பு" விலைமதிக்க முடியாத சேவையை ஆற்றுகின்றது.

கலாநிதி ஹசந்த ஹெட்டியாராச்சி
நிறைவேற்றுப் பணிப்பாளர்
சுயாதீன தொலைக்காட்சி ஊடக வலையமைப்பு
(2021)

ISBN 978-624-5622-06-1
9 786245 622061

www.hithawathi.lk

இலவச விநியோகத்திற்காக