பாதுகாப்பான சகோதரிகள்

பெண்களுக்கும் சிறுமிகளுக்குமான டிஜிட்டல் பாதுகாப்பு தொடர்பான பொது அறிவு வழிகாட்டி

பாதுகாப்பான சகோதரிகள்

பெண்களுக்கும் சிறுமிகளுக்குமான டிஜிட்டல் பாதுகாப்பு தொடர்பான பொது அறிவு வழிகாட்டி

கற்கை திட்டம்:

ஆராய்ச்சி:

முதல் உள்ளூர்மயமாக்கப்பட்ட அச்சு: ஏப்ரல் 2021

ISBN 978-624-5789-02-3

உள்ளூர் கலை: பாக்கியா மதனசிங்கவின் 'Moving Doodles'

கனடா அரசாங்கத்தின் அமைதி மற்றும் உறுதிப்படுத்தல் செயல்பாட்டு திட்டத்தின் (PSOPs) ஆதரவுடன் இன்டர்நியூஸ் இலங்கையால் வெளியிடப்பட்டது.

வழிகாட்டியை பதிவிறக்கம் செய்யவும் மேலும் விபரங்களை அறிந்து கொள்ளவும் *https://safesisters.net* இணையத்தளத்தினை நாடுங்கள்.

இது என்ன கையேடு?

எமது இந்த கையேட்டைத் தெரிவு செய்தமைக்கு நன்றி இணையப் பாவனையின் போது எமது சகோதரிகள் எதிர்கொள்கின்ற பல்வேறு பிரச்சினைகளின் (தனிப்பட்ட படங்கள் களவாடப்படல், அவை அனுமதியின்றி வெளியிடப்படல், வைரஸ்கள் மற்றும் மோசடிகள்) போது நாம் எவ்வாறு எம்மை நாளாந்தம் பாதுகாத்துக் கொள்வது என்பதுடன், இணையப் பாவனையை எவ்வாறு எமக்கான, எமது குடும்பத்திற்கான, ஏனைய அனைத்து சகோதரிகளுக்குமான மிக பாதுகாப்பான செயற்பாடாக மாற்றிக் கொள்வது என்பது தொடர்பில் வழிகாட்டும் நோக்கத்துடன் இந்த கையேட்டை நாங்கள் வடிவமைத்துள்ளோம்.

நாங்கள் யார்?

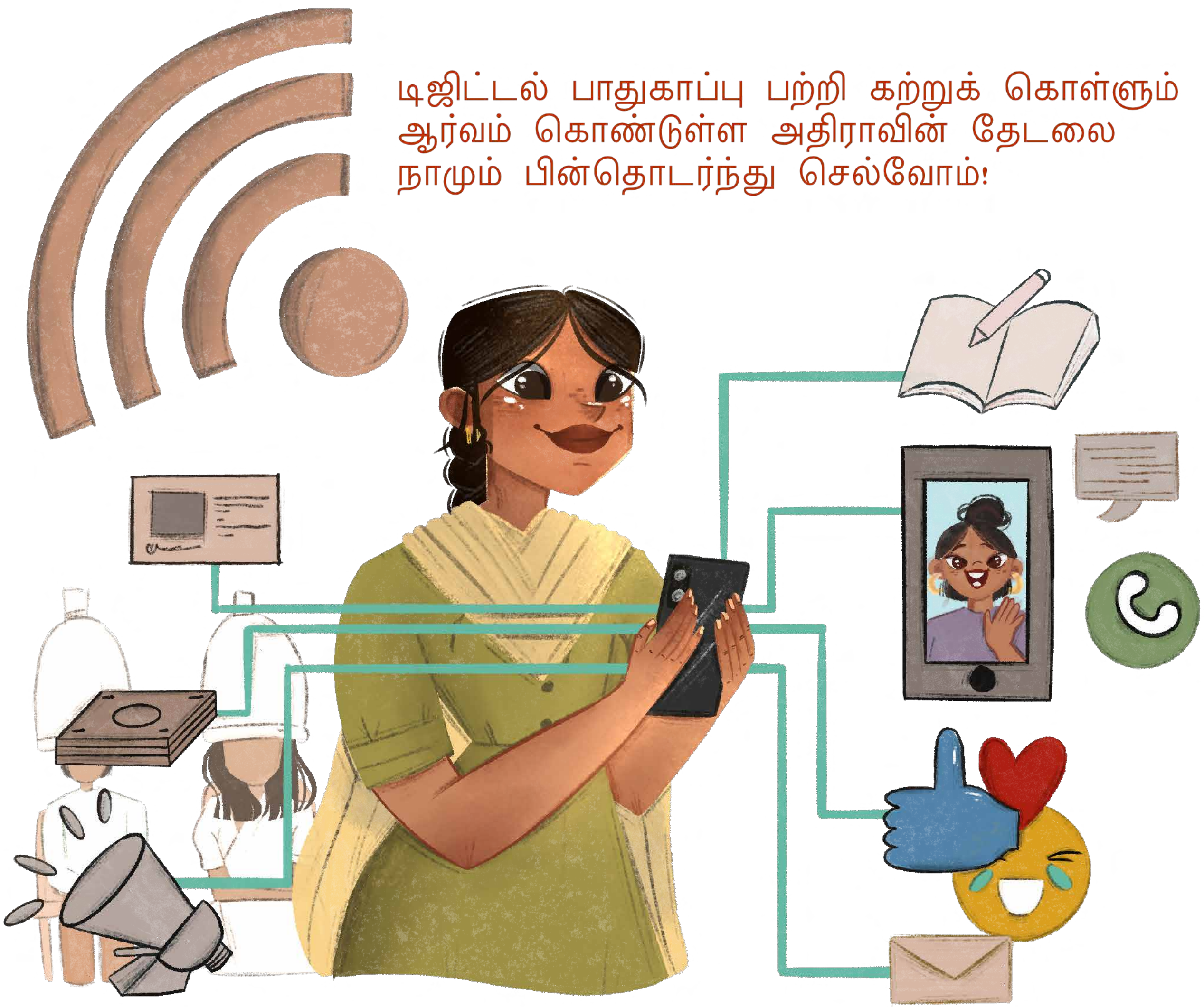
இன்டர்நியூஸ், டிபென்ட் டிபென்டர்ஸ் மற்றும் 2017 - 2018 பாதுகாப்பான சகோதரிகள் தோழமை திட்டத்தின் கூட்டு முயற்சியினால் இந்த கையேடு உருவாக்கப்பட்டுள்ளது. டிஜிட்டல் பாதுகாப்பினை இலகுபடுத்தல், உண்மையான பயனாளிகளுக்கு ஏற்றவாறு பொருத்தமானதாக மாற்றுதல், அனைத்து பெண்களும் சிறுமிகளும் இணையப் பாதுகாப்பினை தங்கள் கரங்களில் எடுத்துக் கொள்வதனை ஊக்குவித்தல் ஆகியன எமது நோக்கங்களாகும். இந்த கையேடானது வினைத்திறன் வாய்ந்த முறையில் ஒன்லைனிலிருந்து பாதுகாப்பு பெற வாசகர்களுக்கு உதவும் என்று நம்புவதுடன், ஒன்லைனில் நாம் இல்லாத வேளைகளிலும் பின்பற்றக் கூடிய பொது அறிவு உபாயங்கள் இதில் உள்ளடங்கியுள்ளன.

அதிராவை சந்திப்போம்!

இலங்கையின் தலைநகரான கொழும்பில் வசிக்கும் இளம் பெண்ணான அதிராவுக்கும் அவரது தோழிகளுக்கும் இன்டர்நெற் என்பது வாழ்வின் ஓர் முக்கியமான அங்கமாக உள்ளது. முகநூலில் பதிவுகளை இடுதல், இன்ஸ்ட்டகிராமில் படங்களை பதிவிடுதல், டுவிட்டரில் கருத்துக்களைப் பகிர்ந்துகொள்தல், வட்ஸ் அப் மற்றும் மெசெஞ்சரில் நண்பர்கள் மற்றும் குடும்ப உறுப்பினர்களுக்கு குறுஞ்செய்திகளை அனுப்புதல், கூகுளில் விடயங்களை தேடுதல் மற்றும் உத்தியோகம் தொடர்பில் ஈமெயில் அனுப்புதல் போன்ற விடயங்களை அவர்கள் மேற்கொள்கின்றனர்.

அதிராவுக்கு சிறு மகள் இருக்கின்றார். அவர் பெயர் அனிஷா. அவர் அதிராவின் தாய், தந்தை மற்றும் இளைய சகோதரி அபிஷாவுடன் அதே வீதியில் வசிக்கின்றார். அதிராவின் தோழிகளின் சமூக ஊடகக் கணக்குகள் ஹெக் செய்யப்பட்டுள்ளன. அவர்கள் அறியாமல் படங்கள் பிறரால் அத்துமீறி பதிவிடப்பட்டுள்ளன. அதனால் அவரும் அவரது குடும்பத்தாரும் ஒன்லைன் பாதுகாப்பினை எப்படி பெற்றுக் கொள்வது என்பது தொடர்பில் கவலையடைந்துள்ளனர்.

இணையத்தில் அவரது தகவல்கள் வெளியாகும் போது என்ன நடக்கும் என்பது குறித்தும், பாதுகாப்பான இணையப் பாவனைக்கான வழிவகைகள் குறித்தும், அவற்றை அவரது மகளுக்கும் நண்பர்களுக்கும் எவ்வாறு கற்பிப்பது என்பது தொடர்பிலான தகவல்களை அனைவருக்கும் வழங்கும் வகையில் இந்த கையேடு முழுவதும் அதிரா முக்கியமான பல்வேறு வினாக்களை வினவுகின்றார்.



அதிரா வினவுகின்றார்

என் சமூக ஊடகக் கணக்கினை எவராலும் ஹெக் செய்ய முடியுமா?

அதிராவின் உறவினரான மதுராவின் முகநூல் கணக்கு கடந்த ஆண்டு ஹெக் செய்யப்பட்டது. அவர் எழுதாத விடயங்களை யாரோ ஒருவர் எழுதி பதிவிட்டிருந்தார். பேஸ்புக் நிறுவனத்தினை மதுரா தொடர்பு கொண்டு அது பற்றி முறைப்பாடு ஒன்றை செய்தார். அவரின் முகநூல் கணக்கினை அவரின் கட்டுப்பாட்டுக்குள் கொண்டு வருவதற்கு அவர்கள் உதவிய போதிலும், எவ்வாறு அவரது கணக்கு ஹெக் செய்யப்பட்டது என்பது பற்றி அவருக்கு இன்று வரை தெரியாது!

அதிராவின் முகநூலுக்குள் ஒருவர் அத்துமீறி பிரவேசிப்பதற்கு பல வழிகள் உள்ளன. சிலநேரங்களில் அவரின் கடவுச்சொல்லை அதாவது பாஸ்வேர்ட்டை யாராவது பெற்றிருப்பார்கள். கடவுச்சொற்களை களவாடுவதற்காகவே பலர் உள்ளனர். உண்மையில் இந்த தொழில் நன்றாக வளர்ச்சிப் பெற்று வருகின்றது! ஹெக் செய்பவர்களுக்கு உங்களின் கடவுச்சொல் மிக மிக அவசியமாகும். அப்பொழுது தான் உங்களை பற்றிய தகவல்களை அவர்களால் பெற முடியும். எப்படி அவர்கள் இந்த செயலில் வெற்றிப் பெறுகின்றனர்? நாம் பயன்படுத்தும் கடவுச்சொற்கள் இலகுவாக கண்டுபிடிக்கப்படக் கூடியவை. இதனால் கணினிகளிலிருந்து களவாடப்பட்டு சைபர் குற்றவாளிகளினால் தாராளமாகப் பயன்படுத்தப்படுகின்றது.

p@ssword என்ற சொல் ஆங்கிலத்தில் பொதுவாக அனைவராலும் பயன்படுத்தப்படும் கடவுச்சொல் என்பது உங்களுக்குத் தெரியுமா?

கருத்திற்கொள்ளுங்கள்:

- இலகுவில் ஊகிக்க முடியாத கடினமான கடவுச்சொல்லை உருவாக்கிப் பயன்படுத்துவது ஹெக் செய்பவர்களிடமிருந்து பாதுகாப்பு பெறுவதற்கான முதலாவது சிறந்த வழிமுறையாகும். அதனால் புத்திசாலித்தனமாக சிந்தித்து கடவுச்சொல்லைத் தெரிவு செய்யுங்கள்.
- உங்களின் அனைத்து கடவுச்சொற்களையும் நினைவில் வைத்துக் கொள்வதற்கு password manager ஐ முயற்சியுங்கள் உங்களுக்காக அது உங்களின் அனைத்து கடவுச்சொற்களையும் நினைவில் வைத்திருக்கும். நீங்கள் அனைத்தையும் நினைவில் வைத்திருக்க வேண்டிய அவசியமில்லை.

அதிரா வினவுகின்றார்

கடினமானதொரு கடவுச்சொல்லை எப்படி என்னால் உருவாக்க முடியும்?

உங்களின் ஒன்லைன் கணக்குகளை ஹெக்கர்களிடமிருந்து பாதுகாப்பதற்காக நீங்கள் முன்னெடுக்கின்ற ஒரு சிறிய முயற்சி உங்களுக்கு மிகப் பெரிய உதவியினைப் புரிகின்றது. தற்போது சாதாரண கடவுச்சொற்கள் போதுமானதல்ல என்ற விழிப்புணர்வு அதிகரித்து வருகின்றது. ஏனெனில் அவை இலகுவானவையாகவும், சுருக்கமாகவும் இருப்பதனால் கணினிக்குள் அத்துமீறி பிரவேசிக்க இலகுவாக இருக்கின்றது. அதனால் passphrase னை முயற்சித்துப் பாருங்கள். சொற்கள் சில இணைந்த தொகுதிகளாக உள்ள இந்த passphrase ஐ ஒன்றாக இணைக்கும் போது அதனை உருவாக்கியவருக்கு கணக்குகளை இயக்குவது இலகுவாக இருக்கும். passphrase ஐ இலகுவாக நினைவிற் கொள்ளவும் முடியும். ஆனால் அத்துமீறி பிரவேசிப்பது இலகுவாக இருக்க மாட்டாது. குறிப்பாக அதிக தொழினுட்ப முன்னேற்றம் கொண்ட கணினிகளிலும் இது சாத்தியமில்லை.

அதிராவின் முகநூல் கணக்கின் கடவுச்சொல் august2013!, என்றவாறு அமைந்துள்ளது. அவரது இளைய சகோதரியின் பிறந்த மாதமும் ஆண்டும் இதில் உள்ளடங்கியுள்ளன. இதனை ஊகிப்பது வெகு இலகுவான செயலாகும். கடினமான passphrase கடவுச்சொல்லை உருவாக்க அவர் அதனை EyeLIkeMyFrIends&Family! ஆக மாற்றினார். (இந்த சொல் 'I like my friends and family' என்றவாறு வருகின்றது).

கருத்திற்கொள்ளுங்கள்:

- நீளமான கடவுச்சொல்லே நல்லது உங்களது கடவுச்சொல்லை 15 சொற்கள் உள்ளடங்குமாறு உருவாக்கிக் கொள்ளுங்கள். அதில் அடையாளங்கள், இலக்கங்கள் என்பனவற்றுடன் ஆங்கில கெப்பிட்டல் எழுத்துக்களையும் இயலுமாயின் சேர்த்துக் கொள்ளுங்கள்.
- எனினும் சிறப்பான passphrase ம் எப்பொழுதும் போதுமானதல்ல. உங்களது முக்கியத்துவம் வாய்ந்த கணக்குகளுக்கு அதிக பாதுகாப்பு தேவைப்படுமாயின், Two- Factor Authentication (2FA) யை இயக்கி விடுங்கள். பெரும்பாலான பிரசித்திப் பெற்ற இணையத்தளங்கள் (முகநூல், ஜிமெயில், டுவிட்டர், இன்ஸ்ட்டகிராம்) 2FA ஐ கணக்குகளுக்குள் பிரவேசிக்க மிகவும் பாதுகாப்பானவையாக சலுகை அடிப்படையில் வழங்குகின்றன. அது பற்றி பரிசீலித்துப் பாருங்கள்.
- எதனைப் பயன்படுத்துவது என்பது பற்றி நீங்கள் தீர்மானித்தாலும், கடவுச்சொற்களையும், பாஸ்பிரேசசையும் ஒரு கணக்குக்கு மேல் பயன்படுத்தாதீர்கள். ஏனெனில் கடவுச்சொற்களையும், பாஸ்பிரேசசையும் எவராவது அறிந்துகொண்டால் அனைத்து கணக்குகளிலும் அத்துமீறி பிரவேசிக்க அவர்களுக்கு இலகுவாக இருக்கும்.

அதிரா வினவுகின்றார்

சமூக ஊடகங்களில் நான் எவ்வாறான விடயங்களைப் பதிவேற்ற வேண்டும்?

நீங்களும் மற்றவர்களைப் போன்று பொதுவாக சிந்தித்து செயற்படும் ஒருவராயின் நண்பர்களுடனும், குடும்பத்தினருடனும் தொடர்புகளைப் பேணவும், சமூகத்துடன் ஊடாடவும் சமூக ஊடகங்கள் உங்களுக்கு இலகுவான வழிமுறையாக உள்ளன. பல தகவல்களையும், படங்களையும் சமூக ஊடகங்களில் மக்கள் பதிவிடுகின்றனர். ஆனால் அவர்களின் படங்களையும், கருத்துக்களையும் அறிமுகம் இல்லாதவர்களும் பார்க்கக் கூடியதாக உள்ளது என்பதனை பின்பே அவர்கள் அறிந்து கொள்கின்றனர். உங்களது முகநூல் கணக்கினைப் பார்த்து விட்டு உங்களைப் பற்றிய பல விடயங்களை அறிமுகமற்றவர்கள் அறிந்து கொள்கின்றனர்.

ஒன்லைனில் பதிவிடும் தகவல்கள், வீடியோக்கள் மற்றும் படங்களை புத்திசாலித்தனமாக சிந்தித்துப் பார்த்து பதிவேற்றுங்கள். எந்த படத்தினை தெரிவு செய்கின்றீர்கள், உங்கள் தொடர்பான எந்த தகவல்களை அனுப்புகின்றீர்கள் என்பது தொடர்பில் எப்பொழுதும் விழிப்புடன் இருங்கள்.

ஒன்லைனில் எதுவும் உண்மையில் முற்று முழுதாக அகன்று விடாது என்பதனை எப்பொழுதும் நினைவில் வைத்திருங்கள்.

கருத்திற்கொள்ளுங்கள்:

- உங்களது பெயரை கூகுள் தேடல் செய்து பார்த்து அதில் மற்றவர்களுக்கு தெரியக் கூடியளவு எவ்வாறான தகவல்கள் உள்ளன என்பது பற்றி ஆராய்ந்து பாருங்கள்.
- உங்களது தந்தையார் உங்களின் சமூக ஊடக கணக்கினுள் சென்று பார்த்தால் அவர் உங்களைப் பற்றி எவ்வாறான தனிப்பட்ட தகவல்களை கண்டறிவார்? அந்த தகவல்கள் பகிரங்கமாக இருப்பது தொடர்பில் உங்களுக்கு சௌகரியமாக உள்ளதா? இல்லையெனின், உங்கள் கணக்கின் பிரைவசி செட்டிங்ஸை மாற்றிக் கொள்ளுங்கள்.

அதிரா வினவுகின்றார்

கடவுச்சொல் இல்லாமல் எனது கணக்கினுள் எவராலும் அத்துமீறி பிரவேசிக்க முடியுமா?

உங்களுக்கு அறிமுகம் இல்லாதவர்களிடமிருந்து அடிக்கடி லின்க்குகளைப் பெறுகின்றீர்களா? அல்லது நீங்கள் பரிசு ஒன்றைப் பெற்றுள்ளீர்கள் என்று வாழ்த்துக் கூறி மெசேஜ்கள் வருகின்றனவா? அல்லது உங்கள் கணினியில் வைரஸ் உள்ளதாகவும் அதனை நீக்குவதற்கு உடனடியாக டவுன்லோட் செய்து அப்டேட் பண்ணுமாறு மெசெஜ் வருகின்றதா?

உங்களது கடவுச்சொல்லை அறியவுள்ள மற்றுமொரு வழிமுறையாகவும் உங்கள் கணக்கினுள் அத்துமீறி பிரவேசிப்பதற்காகவும் இவ்வாறு வைரஸ் (இதனை malware என்றும் கூறுவர்) அனுப்பப்படுகின்றது. இந்த ரைவஸ்கள் கணினி புரோகிராம்களில் நுழைந்து ஆபத்தினை விளைவிக்கக் கூடியவை. அத்துடன் உங்கள் கணினியிலிருந்து உங்களை பற்றிய தகவல்களையும், வங்கிக் கணக்குகள் தொடர்பான விபரங்களையும் களவாடக் கூடியவை. லின்க்கை கிளிக் செய்தவுடன் அல்லது தெரியாத பைல்களை டவுன்லோட் செய்தவுடன் அவை இயங்க ஆரம்பித்து விடுகின்றன.

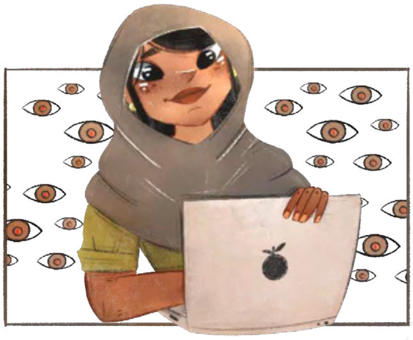
கருத்திற்கொள்ளுங்கள்:

- எப்பொழுதும் சந்தேகப் பார்வையைக் கொண்டிருங்கள். அறிமுகம் இல்லாத நபர்களினால் அனுப்பப்படும் ஈமெயில் இணைப்புகள் மற்றும் லின்க்குகள் தொடர்பில் அவதானமாக இருங்கள். அனுப்புநரின் விபரங்களை நன்கு அவதானித்துப் பாருங்கள். அதில் ஏதும் சந்தேகங்கள் இருந்தால் கிளிக் செய்யாதீர்கள்.
- உங்களது கைத்தொலைபேசி அல்லது கணினியில் வைரஸ் இருக்கின்றது. அதனால் டவுன்லோட் செய்து அப்டேட் செய்யுங்கள் என்று குறுஞ்செய்திகள் வந்தால் கவனமாக இருங்கள். ஏனெனில் அது உண்மையான தகவலாக இருக்க மாட்டாது. வெகு உன்னிப்பாக அவதானித்துப் பாருங்கள். உண்மையானதாக இருக்கின்றதா? உங்களால் முடிவுக்கு வர முடியாதிருப்பின் கூகுளுக்கு அலர்ட் மெசேஜ்ஜை டைப் செய்யுங்கள். அத்துடன் வேறு யாராவது முறைப்பாடு செய்துள்ளார்களா? என்றும் தேடிப் பாருங்கள்.
- சொப்ட்வெயார் அப்டேட் தொடர்பாக வரும் தகவல்களை புறக்கணிக்காதீர்கள். ஏனெனில் வைரஸ்களிலிருந்து உங்களது கணினியை பாதுகாக்கும் புதிய அம்சங்கள் மற்றும் பாதுகாப்பு அப்டேட்ஸ்கள் அதில் இருக்கும். நீங்கள் இவ்விடயத்தில் அக்கறையுள்ளவராயின், நேரடியாக சொப்ட்வெயார் இணையத்தளங்களுக்கு சென்று அவற்றிலிருந்து டவுன்லோட் செய்யுங்கள்.

அதிரா வினவுகின்றார்

யாராவது என்னை ஒன்லைனில் கண்காணித்துக் கொண்டிருப்பது போல் தோன்றினால் என்ன செய்ய வேண்டும்?

ஒன்லைனில் உங்களை யாராவது எப்பொழுதும் கண்காணித்துக் கொண்டே இருக்கின்றார்கள் என்பது பொதுவான ஓர் உள்ளுணர்வாகும். அதற்காக உங்களை கெமராவில் யாரோ பார்த்துக்கொண்டே இருக்கின்றார்கள் என்பது அர்த்தமல்ல. பெரும்பாலான நேரங்களில் இணையத்தளப் பாவனையின் போது நீங்கள் பிரவேசித்த டிஜிட்டல் சுவடுகளையும், அல்லது கைத்தொலைபேசியில் பெறப்பட்ட தகவல்களையும் லொக்கேஷன்களையும், பார்வையிட்ட இணையத்தளங்களையும், பயன்படுத்திய செயலிகளையும் அதாவது அப்ஸ்களையும் அவ்வாறே விட்டு விடுகின்றீர்கள். எங்களுக்குப் பிடித்த விடயங்கள் (அல்லது பிடிக்காத விடயங்கள்), நண்பர்களின் குடும்பத்தினரின் பெயர்கள், நீங்கள் சென்ற பாடசாலை, எமது அரசியல் பார்வைகள், மற்றும் கடந்த வாரம் இரவு என்ன சாப்பாடு சாப்பிட்டீர்கள் என்ற விடயங்களும் அதில் அடங்கியிருக்கக் கூடும்.



நாம் நாளாந்தம் பயன்படுத்துகின்ற பெருமளவான இணையத்தளங்கள் வர்த்தக நோக்கத்தினைக் கொண்டவையாக இருப்பதுடன், அவை எமது தகவல்களை சேகரித்து விளம்பர நிறுவனங்களுக்கு விற்கக் கூடும். இந்த நிறுவனங்களினால் உங்களது டிஜிட்டல் சுவடுகள் தற்போது சேகரிக்கப்படுவதற்கான சாத்தியக்கூறுகள் அதிகம் உள்ளன. ஆனால் உங்களது பிரைவசியினை மேம்படுத்திக் கொள்வதனூடாக குறைவான தகவல்கள் ஒன்லைனில் விடப்படுகின்றன.

கருத்திற்கொள்ளுங்கள்:

- ஒரு செயலி அதாவது அப் இலவசமாக வழங்கப்படுகின்றதாயின் அதனை உருவாக்கியவரினால் எப்படி பணம் சம்பாதிக்க முடியும்? பெரும்பாலும் உங்கள் தகவல்கள் யாவும் சேகரிக்கப்பட்டு விளம்பதாரர்களுக்கு விற்கப்படுகின்றன என்பதே உண்மையாகும்.
- சமூக ஊடகங்களுக்கான பிரைவசி பொலிசியினை எப்பொழுதும் பரிசீலனை செய்து கொண்டே இருங்கள். ஏனெனில் அவை அடிக்கடி மாற்றப்படுகின்றன.
- உங்களது கைத்தொலைபேசியில் உள்ள அப் எனப்படும் செயலி அனுமதி விபரங்களுக்குள் (அப் பேர்மிஷன்ஸ்) சென்று அந்த அப் மூலம் எந்தெந்த வசதிகளை அணுக முடியும் என்று பாருங்கள். கொன்டக்ட் லிஸ்ட், உங்களது மைக்ரோபோன், அல்லது லொக்கேஷன் என்பனவற்றை அவதானியுங்கள். தேவையெனில் அவற்றை மாற்றிக் கொள்ளுங்கள்.

அதிரா வினவுகின்றார்

எனது டிவைஸ்களை மற்றவர்களுடன் நான் பகிர்ந்துகொள்கின்றேன் எனின் என்ன செய்ய வேண்டும்?

நீங்கள் பணியாற்றும் இடத்திலோ, வீட்டிலோ அல்லது சைபர் நிலையத்திலோ கணினியைப் பகிர்ந்து பயன்படுத்துகின்றீர்களாயின் நீங்கள் கணினியில் பார்த்த விடயங்களை அதாவது நீங்கள் பிரவேசித்த இணையத்தளங்களைப் பார்வையிடவும், உங்களது தனிப்பட்ட ஈமெயில்கள் மற்றும் மெசேஜ்களை வாசிக்கவும், உங்களது படங்களைப் பார்க்கவும், அது மட்டுமன்றி வீடியோக்களையும், மெசேஜ்களையும் உங்களது கணக்குகளிலிருந்து பதிவேற்றிக்கொள்ளவும் பிறரால் இயலும்.

உங்களது கணினியில் பிறர் அத்துமீறி பிரவேசிக்காமல் இருப்பதற்கு மிகச் சரியான வழிமுறையாக கணினியிலிருந்து வெளியேறும் போது நீங்கள் சென்ற இணையத்தளங்களின் வரலாறுகளை அதாவது அவற்றின் ஹிஸ்ட்ரியை டிலிட் செய்து விடுங்கள். கணக்குகளிலிருந்து (ஈமெயில், சமூக ஊடகங்கள் போன்றவை) சைன் அவுட் செய்து வெளியேறி விடுங்கள். அத்துடன் கணினியிலிருந்து லொக்அவுட் செய்து விடுங்கள் (இயலுமாயின்). உங்களின் தனிப்பட்ட ஆவணங்களையும், படங்களையும் பிறர் பார்க்கின்றார்கள் என்று அஞ்சுகின்றீர்களாயின் அவற்றை கணினியில் டவுன்லொட் செய்யாதீர்கள். அதற்கு பதிலாக அவற்றை கிளவுட்டில் (கூகுள் டிரைவ், அல்லது ட்ரொப் பொக்ஸ்) சேமித்து வையுங்கள். ஆனால் நீங்கள் கணினியிலிருந்து வெளியேறும் போது சைன் அவுட் செய்ய மறவாதீர்கள்.

உங்களது கணினி அல்லது தொலைபேசி உங்களின் குடும்ப உறுப்பினர்களுடன் பகிரப்படுகின்றதாயின் கடவுச்சொல் அதாவது பாஸ்வேட் அல்லது நம்பர் லொக் ஐ (சில வேளைகளில் PIN கோட் எனப்படும்) அவர்களுடன் பகிர்ந்துகொள்வது அவசியமாகும். இதனால் உங்களின் டிவைஸ் ஏதாவது களவாடப்படுமாயின் உங்களுக்குரிய உணர்வுபூர்வமான தகவல்களும், படங்களும் திருடர்களினால் அணுகப்பட முடியாது போய்விடும்.

கருத்திற்கொள்ளுங்கள்:

- நம்பிக்கையில்லாதவர்களுடன் கணிணி பகிரப்படுகின்றதாயின் அவர்கள் சில சொவ்ட்வெயார்களை அதனுள் புகுத்தி உங்களைக் கண்காணிக்கக் கூடும். இந்த சொவ்ட்வெயார் spyware என்று அழைக்கப்படுகின்றது. ஸ்பைவெயார் உள்ள கணினியை நீங்கள் பயன்படுத்துகின்றீர்கள் என்று உங்களுக்கு சந்தேகம் ஏதும் ஏற்பட்டால் அதில் வேலை செய்வது தொடர்பில் மிகவும் அவதானமாக இருங்கள்.
- நீங்கள் நன்கு அறிந்த ஒருவர் உங்கள் கைத்தொலைபேசியில் உள்ள தனிப்பட்ட மெசேஜ்களை வாசிக்க விரும்புகின்றாராயின் உங்களுக்கு ஆபத்தினை ஏற்படுத்தக் கூடிய பிரச்சினைக்குரிய தனிப்பட்ட தொடர்பாடல்களை அழித்து விடுங்கள்.

அதிராவின் சரிப்பார்ப்பு பட்டியல்

அதிரா தற்போது தனது டிஜிட்டல் பாதுகாப்பு முன்னேற்றம் தொடர்பில் மாற்றங்களை செய்வதில் ஆர்வமாக உள்ளார். அவர் தனது சரிப்பார்ப்பு பட்டியலில் எவ்வாறான விடயங்களை உள்ளடக்கியுள்ளார் என்பதனை நோக்குவோம்.

01 சிறந்த பாஸ்வேர்ட்களை உருவாக்குதல்

பாஸ்பிரேசஸ் மூலம் கடினமான கடவுச்சொல்லை உருவாக்கும் வேலையை மகிழ்வுடன் செய்தல். அதாவது எனது விருப்பத்திற்குரிய பாடலின் வரிகளுடன் கெப்பிட்டல் எழுத்துக்களையும், இலக்கங்களையும், அடையாளங்களையும் சேர்த்து கடவுச்சொல்லை உருவாக்குதல். கணக்குகள் பலவற்றுக்கு ஒரே கடவுச்சொல்லைப் பயன்படுத்தாமல் இருத்தல்.

02 கிளிக் செய்ய முன்பு சிந்தித்தல்

சந்தேகத்திற்குரிய லின்க்குகள், அட்டாச்மென்ட்களை கிளிக் செய்யாமல் இருத்தலை இப்பொழுது முதல் ஆரம்பித்தல். அறிமுகம் இல்லாதவர்களிடம் இருந்து வரும் புதிய ஈமெயில்கள் தொடர்பில் அவதானமாக இருத்தல். அனுப்புநர் விபரங்கள், ஈமெயிலின் உள்ளடக்கங்கள் தொடர்பில் கவனம் செலுத்துதல்.

03 எப்பொழுதும் லொக்ஒவ்

தொலைபேசியிலும் கணினியிலும் உள்ள செக்யூரிட்டி செட்டிங்ஸ்ஸை மீள்பரிசீலனை செய்தல். டிவைஸ்களுக்குள் செல்ல கடவுச்சொல் ஒன்றை இடுதல். பகிர்ந்து வேலை செய்யப்படும் கணினி மற்றும் தொலைபேசியிலிருந்து வேலைகளை முடித்து வெளியேறும் போது கணக்கிலிருந்து சைன் அவுட் செய்தல்.

04 ஒன்லைனில் பதிவேற்றும் விடயங்கள் தொடர்பில் கவனமாக இருத்தல்

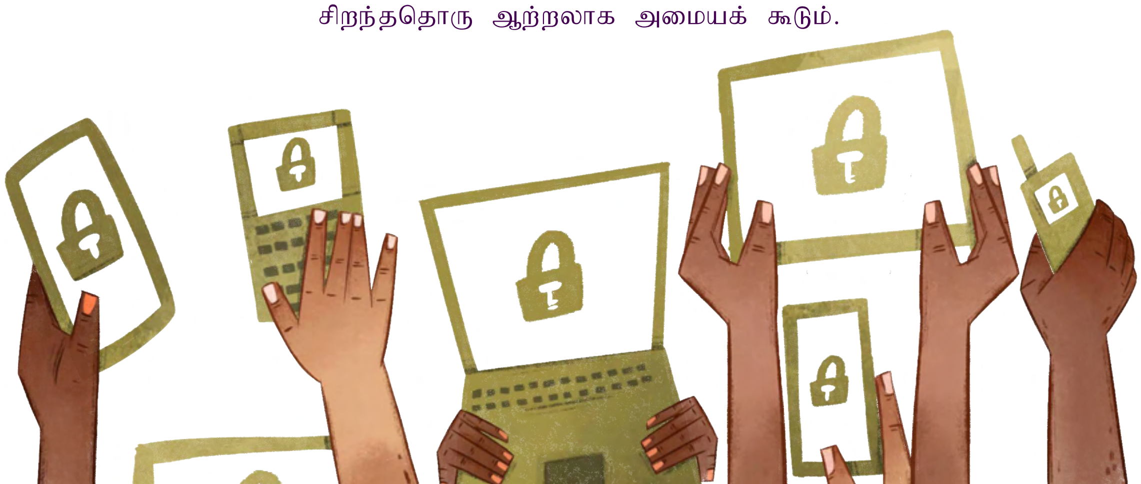
இணையத்தில் பதிவிடும் விடயங்களையும், படங்களையும் முற்றாக அகற்றுவது என்பது பெரும்பாலும் இயலாத விடயமாகும். அதனால் சமூக ஊடகங்களில் பகிரப்படும் விடயங்கள் தொடர்பில் கவனமாக சிந்தித்து செயற்பட வேண்டும். சமூக ஊடக அப்ஸ்களின் பக்கங்களின் பிரைவசி செட்டிங்ஸ்ஸை நன்கு அவதானித்துப் பார்க்க வேண்டும். அத்துடன் அனுமதிகளை மட்டுப்படுத்துதல் (லொக்கேஷன், மைக்ரோபோன், கொன்டக்ட் லிஸ்ட்) மற்றும் யார் தகவல்களைப் பார்க்கின்றார்கள் என்ற விடயங்கள் குறித்து அவதானம் செலுத்துதல்.

05 உங்களது சகோதரியின் பாதுகாவலராகுங்கள்

ஒன்லைனில் அனுமதியின்றி படங்கள் வெளியாவது பெருமளவான பெண்களைப் பாதிக்கும் ஓர் விடயமாகும். உங்களின் சக சகோதரிகளை பாருங்கள். பொருத்தமற்ற விடயங்களை இணையத்தில் பகிராதீர்கள். துன்புறுத்தல்களுக்கும், பெண்களுக்கு எதிரான வன்முறைகளுக்கும் ஒன்லைனில் தனது கணக்குகளை ஒரு தளமாகப் பயன்படுத்தும் நபர்களைப் பற்றி முறையிடுதல் மற்றும் அவர்களின் தொடர்புகளை டிலிட் செய்தல்.

நினைவிற்கொள்ளுங்கள்: உங்களால் செய்ய முடியும்!

ஒன்லைனில் பாதுகாப்பாக செயற்படுவது என்பது தொடர்பில் கற்றுக் கொள்வதற்காக நேரத்தினை அர்ப்பணியுங்கள். இணையத்தினைப் பயன்படுத்தும் போது அவதானமாக செயற்படுவது எப்படி என்பது தொடர்பாக பயிற்சியில் ஈடுபடுங்கள். விசித்திரமான விடயங்களை அவதானிப்பதும், பிரச்சினைகள் மற்றவர்கள் மத்தியில் ஊடுருவி பரவுவதற்கு முன்னர் அவற்றை இனம் காண்பதும் உங்களுக்குள்ள சிறந்ததொரு ஆற்றலாக அமையக் கூடும்.



35C, Torrington Avenue, Colombo 07

LK-Info@internews.org

www.facebook.com/internewslk

@Internews_LK

ISBN 978-624-5789-02-3