fairfirst INSURANCE
A FAIRFAX Company

தனிநபர்களுக்கான சைபர்பாதுகாப்பு

V 1.0 12/06/2020

COVID-19 தொற்றுப் பரவல் காரணமாக உலக நாடுகள் முடக்கப்பட்டிருந்த நிலையில், சொப்பிங், பணி, கல்வி போன்ற எமது பல தினசரிச் செயற்பாடுகள் ஒன்லைனில் மேற்கொள்ள வேண்டிய நிலை ஏற்பட்டது. இது நடைமுறைச்சாத்தியமான தெரிவாக அமைந்திருந்தாலும், இந்த புதிய வழமை என்பது பல புதிய சவால்களுடன் உதயமாகியுள்ளது.

ஒன்லைனில் மக்கள் பெருமளவான பொழுதை செலவிடும் நிலையில், சைபர்குற்றங்களில் ஈடுபடுவோரும் தமது கைவரிசையை காட்ட ஆரம்பித்துள்ளனர். இதனால், உங்கள் அந்தரங்கத்துக்கும் சாதனங்களுக்கும் பெரும் ஆபத்து நேரிடலாம். உங்கள் அலுவலக வலையமைப்பினுள் உங்கள் கணனியினூடாக பிரவேசித்து இரகசியத்தன்மை வாய்ந்த தரவுகளை ஹெக் செய்வது, ஸ்பைவெயார் ஒன்றை நிறுவுவது அல்லது உங்கள் வங்கிக் கணக்குகளை ஹெக் செய்வது போன்ற பல சைபர் குற்றங்களை உலகளாவிய ரீதியில் சைபர் குற்றவாளிகள் புரிந்த வண்ணமுள்ளனர்.

அவ்வாறான குற்றங்கள் இடம்பெறக்கூடிய வாய்ப்புகள் அதிகரித்து வரும் நிலையில், உங்கள் டிஜிட்டல் பிரசன்னத்தை பாதுகாத்துக் கொள்ள உதவும் வகையில் இந்த வழிகாட்டல் அமைந்துள்ளதுடன், உங்களையும், உங்கள் சாதனங்களையும் இவ்வாறான தாக்குதல்களிலிருந்து பாதுகாக்கும் வகையிலும் அமைந்துள்ளது.

ஒன்லைன் சொப்பிங்

ஒன்லைன் சொப்பிங்கில் ஈடுபடுவோரை எவ்வாறு தாக்குதல்களை மேற்கொள்வோர் இலக்கு வைக்கின்றனர்?

உங்களின் பிரத்தியேக தகவல்களை பாதுகாத்துக் கொள்ளவும், தவறான நபர்களின் கரங்களை சென்றடையாமல் பாதுகாக்கவும் போதியளவு முற்காப்பு நடவடிக்கைகளை மேற்கொள்வது மிகவும் முக்கியமானதாகும். ஒன்லைன் கொடுக்கல் வாங்கல்களை மேற்கொள்ளும் போது உங்கள் பாதுகாப்பை உறுதி செய்து கொள்வதற்காக சில முக்கியமான விடயங்களை நீங்கள் எப்போதும் நினைவில் வைத்திருக்க வேண்டும்.

சேவை வழங்குநர் ஒருவர் encryption முறையை பயன்படுத்தாவிடின், உங்கள் தகவல்கள் அனுப்பப்படும் போது பிரிதொரு தரப்பால் குறுக்கிட்டு பெற்றுக் கொள்ள முடியும்.

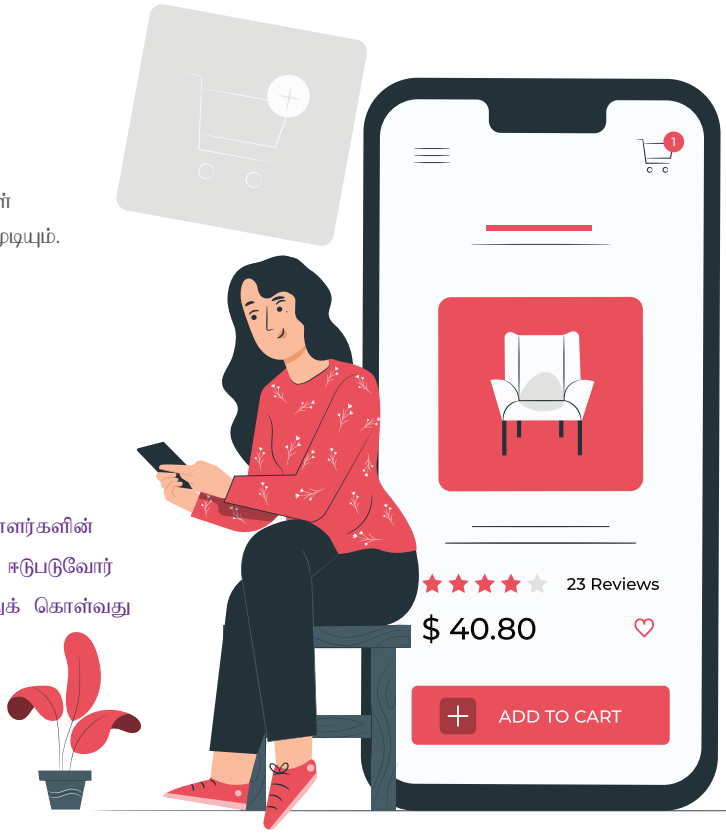
ஒன்லைன் சொப்பிங்கில் ஈடுபடுவோரில் தாக்குதல்களில் ஈடுபடுவோர் அனுகூலம் பெறக்கூடிய மூன்று பொதுவான வழிமுறைகள் காணப்படுகின்றன:

01 போலியான இணையத்தளங்கள் மற்றும் மின்னஞ்சல் தகவல்களை உருவாக்குதல்:

- நிஜ வாழ்க்கையில் சுப்பர் மார்க்கெட் ஒன்றுக்கு நீங்கள் விஜயம் செய்தால், நீங்கள் எங்குள்ளீர்கள், விற்பனையாளர் எந்தளவு உண்மையானவர் என்பதை நீங்கள் அறிவீர்கள். ஆனாலும் ஒன்லைன் சொப்பிங் சூழலில், ஒரு போலியான இணையத்தளத்தை நீங்கள் சென்றடைந்துள்ளீர்கள் என்பதை உங்களால் உணர முடியாமல் கூட இருக்கலாம்.
- தாக்குதல்களில் ஈடுபடுவோர் உண்மையானதைப் போலவே, போலியான இணையத்தளங்கள் அல்லது மின்னஞ்சல் தகவல்களை உருவாக்கி அல்லது நன்கொடை அமைப்புகள், புகழ்பெற்ற நிறுவனங்கள் போல தம்மை காண்பித்து மோசடியில் ஈடுபடக்கூடும்.
- குறிப்பாக இயற்கை அனர்த்தங்களின் பின்னர் அல்லது விடுமுறை காலப்பகுதியில், தாக்குதல்களில் ஈடுபடுவோர் போலியான இணையத்தளங்கள் மற்றும் மின்னஞ்சல்களை உருவாக்கி, உங்களை கொள்வனவு செய்ய தூண்டும் வகையில், இலவச விநியோகம் வழங்குவதாக அறிவித்து, நன்கொடை அமைப்புகளுக்கு உதவுமாறு கோரக்கூடும்.

02 பாதுகாப்பற்ற கொடுக்கல் வாங்கல்களை குறுக்கிடல்:

- விற்பனையாளர் encryption முறையை பயன்படுத்தாவிடின், உங்கள் தகவல்கள் அனுப்பப்படும் போது பிரிதொரு தரப்பால் குறுக்கிட்டு அதை பெற்றுக் கொள்ள முடியும்.



03 ஊறுபடத்தக்க கணனிகளை இலக்கு வைத்தல்:

- வைரஸ்கள் அல்லது இதர செயலிழக்கச் செய்யும் குறியீடுகளிலிருந்து உங்கள் கணனி பாதுகாக்கப்படாவிடின், தாக்குதலில் ஈடுபடுபவரால் உங்கள் கணினியில் இலகுவாக பிரவேசித்து, அதிலுள்ள சகல தகவல்களையும் பெற்றுக் கொள்ள முடியும்.
- விற்பனையாளர்களுக்கு தமது கணனிகளிலுள்ள வாடிக்கையாளர்களின் தகவல்களை தாக்குதல்களில் ஈடுபடுவோர் அணுகுவதிலிருந்து பாதுகாத்துக் கொள்வது முக்கியமானதாகும்.

உங்களை எவ்வாறு பாதுகாத்துக் கொள்ள முடியும்?

- ஏதேனும் பிரத்தியேக அல்லது நிதிசார் தகவல்களை வழங்குவதற்கு முன்னதாக, நீங்கள் புகழ்பெற்ற, உறுதியான விற்பனையாளருடன் கொடுக்கல் வாங்கலில் ஈடுபடுவதை உறுதி செய்து கொள்ளவும். தாக்குதல்களில் ஈடுபடும் சிலர், உண்மையானதை போன்று போலியான தளங்களை உருவாக்கி உங்களை மாயவலையில் சிக்க வைக்க முயற்சிப்பர். எனவே, எவ்விதமான தகவல்களையும் வழங்கும் முன்னர், அந்த தளங்களின் உண்மையை உறுதி செய்து கொள்ளவும்.

- உங்கள் கொடுக்கல் வாங்கல் அல்லது கட்டணப் பட்டியல் தொடர்பில் ஏதேனும் சிக்கல்கள் எழுந்தால், விற்பனையாளரின் தொலைபேசி இலக்கம் மற்றும் முகவரியை தெரிவு செய்து குறித்து வைக்கவும்.

- உங்கள் தகவல் encrypt செய்யப்பட்டிருப்பதை உறுதி செய்யவும். அத்துடன், address bar மற்றும் அதன் அருகாமையில் காணப்படும் தகவல்களை எவ்வாறு பயன்படுத்துவது என்பது பற்றி அறிந்திருங்கள். உதாரணம்: padlock, i-Information போன்றன.

இணையத்தள முகவரியின் இடது அல்லது வலது பக்கத்திலுள்ள padlock icon ஐ க்ளிக் செய்து, அதில் "View Certificate" லிங்கை க்ளிக் செய்யவும். அதன் போது The Certificate dialog box திறக்கும். SSL certificate தொடர்பான தகவல்கள் உடனடியாக வெளிப்படும்.

- தகவல்கள் கோரும் மின்னஞ்சல்கள் தொடர்பில் எச்சரிக்கையாக இருக்கவும் - தாக்குதல்களில் ஈடுபடுவோர், மின்னஞ்சல் அனுப்பி அதில் கொள்வனவை உறுதி செய்யுமாறு அல்லது கணக்கு விவரங்களை கோரக்கூடும். நேர்மையாக வியாபாரத்தில் ஈடுபடும் நிறுவனங்கள் இவ்வாறான தகவல்களை மின்னஞ்சல் வாயிலாக கோரமாட்டாது. மின்னஞ்சல் ஊடாக இவ்வாறான பிரத்தியேகத் தகவல்களை வழங்க வேண்டாம். வியாபாரமொன்றிலிருந்து இவ்வாறான தரவு கோரும் மின்னஞ்சல் ஒன்றை நீங்கள் பெற்றால், அதில் வழங்கப்பட்டுள்ள லிங்கை க்ளிக் செய்வதற்கு பதிலாக, அந்நிறுவனத்தின் இணையத்தள முகவரியை டைப் செய்து நேரடியாக பிரவேசிக்கவும்.

- சகல ஒன்லைன் கொள்வனவுகளுக்கும் கொடுப்பனவை மேற்கொள்ள ஒற்றை, குறைந்த எல்லைப் பெறுமதியைக் கொண்ட கிரெடிட் கார்டை பயன்படுத்துவதனூடாக ஏற்படக்கூடிய இழப்பை குறைத்துக் கொள்ள முடியும். டெபிட் கார்டை விட, கிரெடிட் கார்ட் எப்போதும் உங்களுக்கு அதிகளவு பாதுகாப்பை வழங்குவதாக அமைந்திருக்கும். உண்மையான இணையத்தளங்கள் பல்வேறு வகையான கிரெடிட் கார்ட்களை ஏற்றுக் கொள்ளும் என்பதுடன், சந்தேகத்திற்கிடமான தளங்கள், உறுதி செய்வதற்காக உங்களின் கிரெடிட்/டெபிட் கார்ட் இலக்கங்களை கோரும்.

- உங்கள் சொப்பிங் app settings ஐ பரிசோதித்துக் கொள்ளவும் - உங்கள் தரவுகளைக் கொண்டு என்ன செய்கின்றன எவ்வாறு பாதுகாப்பாக பேணுகின்றன என்பதை குறிக்கும் appகளை தெரிவு செய்யவும்.

- உங்கள் மாதாந்த கணக்கு அறிக்கைகளை பரிசோதிக்கவும் - உங்கள் கொள்வனவுகள் தொடர்பான பதிவுகளையும் உறுதிப்படுத்தல் பக்கங்களின் பிரதிகளையும் பேணவும், அவற்றை மாதாந்த கணக்கு அறிக்கையுடன் ஒப்பிட்டு சரிபார்த்துக் கொள்ளவும். ஏதேனும் வேறுபாடுகள் இருந்தால் உடனடியாக அறிவிக்கவும்.

தாக்குதலுக்கு இலக்காவதை தவிர்த்துக் கொள்ளல்

புதிய சூழலுடனான, இன்றைய வேலைப்பளு நிறைந்த உலகில், பெரும்பாலான செயற்பாடுகள் ஒன்லைனில் இடம்பெறுகின்றன. இதனால் சில சந்தர்ப்பங்களில் சில மின்னஞ்சல்கள் மற்றும் கோரிக்கைகள் தொடர்பில் பெருமளவு அக்கறை கொள்வதில்லை. இதனால் phishing தாக்குதலுக்கு இலக்காகி முக்கியத்துவம் வாய்ந்த தகவல்களை பறிகொடுக்க நேரிடும்.

Phishing முயற்சிகளை இனங்காணல்:

- **சந்தேகத்திற்கிடமான அனுப்புபவரின் முகவரியிலிருந்து வரும் மின்னஞ்சல்கள்**
  அனுப்புபவரின் மின்னஞ்சல் உண்மையான வியாபாரத்தை போன்று தோன்றக்கூடும். சைபர்குற்றவாளிகள் எப்போதும், புகழ்பெற்ற நிறுவனங்களின் பெயர்களுக்கு சமமான பெயர்களைக் கொண்டு, ஒரு சில எழுத்துக்களை மாற்றி உருவாக்கிய மின்னஞ்சல்களை இதற்காக பயன்படுத்துகின்றனர்.

- **பொதுவான ஆரம்ப விழிப்பு மற்றும் கையொப்பம்**
  “அன்பார்ந்த பெறுமதியான வாடிக்கையாளர்” அல்லது “ஐயா/அம்மணி” போன்ற பொதுவான ஆரம்ப விழிப்பு மற்றும் கையொப்ப பகுதியில் தொடர்பாடல் விவரங்கள் இன்மை போன்றன phishing மின்னஞ்சலுக்கான உறுதியான எடுத்துக் காட்டல்களாகும். நம்பிக்கையை வென்ற நிறுவனம் சாதாரணமாக உங்களின் பெயர் குறிப்பிட்டு அழைப்பதுடன், அவர்களின் தொடர்பு கொள்ளும் தகவல்களையும் உங்களுக்கு வழங்கும்.

- **மோசடியான hyperlinkகள் மற்றும் இணையத்தளங்கள்**
  மின்னஞ்சலில் காணப்படும் லிங்க்களுக்கு மேலாக உங்கள் cursor ஐ கொண்டு செல்லும் போது, அந்த வாக்கியங்களுடன் குறித்த லிங்க்கள் பொருந்தாவிடின், அந்த லிங்க் மோசடியானதாக அமைந்திருக்கும். போலியான இணையத்தளங்களும், உண்மையான இணையத்தளங்களை போன்று காட்சியளிக்கும், ஆனாலும், URL களில் எழுத்துப்பிழைகள் அல்லது வேறொரு domain முகவரி காணப்படக்கூடும்.

- **எழுத்துக்கள் மற்றும் வடிவமைப்பு**
  மோசமான இலக்கணம் மற்றும் வாக்கிய கட்டமைப்புகள், எழுத்துப் பிழைகள் மற்றும் தொடர்ச்சியற்ற கட்டமைப்புகள் போன்றன phishing முயற்சிக்கான சில எடுத்துக்காட்டுகளாகும். புகழ்பெற்ற நிறுவனங்கள் வாடிக்கையாளர்களின் தொடர்பாடல் ஆவணங்களை தயாரித்து, வடிவமைத்து அவற்றை ஒப்புநோக்குவதற்கான விசேட நிபுணர்களை கொண்டிருக்கும்.

- **சந்தேகத்திற்கிடமான இணைப்புகள்**
  அறிமுகமில்லாத நபர் ஒருவரிடமிருந்து பாவனையாளருக்கு அனுப்பப்படும் மின்னஞ்சலில் காணப்படும் இணைப்பை தரவிறக்கம் செய்து திறக்குமாறு தெரிவிப்பது என்பது malware ஐ பதிவு செய்யும் சாதாரணமாக முறையாகும். சைபர்குற்றவாளி இதற்காக பாவனையாளரை அவசரப்படுத்தும் வகையிலான சொற்பதங்களை பயன்படுத்தி, போதியளவு முற்காப்பு நடவடிக்கைகளை மேற்கொள்ள விடாமல் கவனத்தை திசைதிருப்பி, குறித்த தரவிறக்கம் செய்த ஆவணத்தை திறக்க செய்வார்.

சைபர்பகுதியில் சிறுவர்கள்

சிறுவர்களுக்கு புதிய விடயங்களை பயில்வதற்கான ஒரு ஊடகமாக இணையம் அமைந்துள்ளது. இணையத்தை பயன்படுத்துவதில் வேகமாக வளர்ந்து வரும் பயனர்களாக இவர்கள் காணப்படுகின்றனர். இதில் நன்மை தீமை ஆகிய இரண்டும் காணப்படுகின்றன. ஆனாலும் பெற்றோர் எனும் வகையில், உங்கள் சிறுவர்களுக்கு இணையத்தினால் ஏற்படக்கூடிய தீங்குகள் பற்றி நீங்கள் எப்போதும் அவதானமாக இருக்க வேண்டும். இந்த தொழில்நுட்பத்தினூடாக உச்ச பயனை பாதுகாப்பான முறையில் பெறுவதற்கான வழிமுறைகளை அவர்களுக்கு பயிற்றுவிப்பது முக்கியமானதாகும்.

சிறுவர்களுடன் தொடர்புடைய விசேடமான ஆபத்துக்கள்:

- பிள்ளைகள் உங்கள் கணனியை பயன்படுத்தும் போது, கட்டமைப்பினால் நிர்வகிக்கப்பட முடியாத பிரத்தியேகமான ஆபத்துக்கள் காணப்படுகின்றன.
- பிள்ளைகள் அப்பாவிகள், புதிய விடயத்துக்கு ஆர்வமானவர்கள் மற்றும் சுதந்திரமாக செயற்பட விரும்புபவர்கள் எனவே, தெரியாமல் செய்த ஏதேனும் காரியங்களுக்காக தண்டிக்கப்படுவோம் எனும் அச்சத்தைக் கொண்டவர்கள்.
- ஒன்லைன் வகுப்பொன்றுக்கு பிள்ளை பிரவேசிக்கும் போது, தகவலை தேடுவது அல்லது பரீட்சைத் தாளை செய்வது, எதிர்பாராதவிதமாக மோசடியான இணையத்தளமொன்றினுள் பிரவேசித்துவிடக்கூடும். இதன் பெறுபேறாக, உங்கள் கணனி வைரஸ் தாக்குதலுக்கு உள்ளாகலாம். தண்டனைக்கு ஆளாவோம் எனும் அச்சத்தின் காரணமாக, பிள்ளை அது பற்றி உங்களுக்கு தெரிவிக்காது.
- Phishing தாக்குதல்களை ஆரம்பிக்கும் குற்றவாளிகளின் வலையில் சிறுவர்கள் சிக்கக்கூடும். அவ்வாறான மோசடிக்காரர்களால் அனுப்பப்படும் மின்னஞ்சல்கள் அல்லது அநாமதேய தகவல்களை சிறுவர்கள் நம்பிவிடக்கூடும்.
- மற்றுமொரு அதிகரித்து வரும் பிரச்சனையாக சைபர்வெறுப்பூட்டல் அமைந்துள்ளது. மின்னஞ்சல் அல்லது உடனடி தகவல் பரிமாற்றல் appகளுக்கு, chat அறைகளுக்கு மற்றும்/அல்லது சமூக வலைத்தளங்களை பிள்ளை அணுகும் வசதியை கொண்டிருக்குமாயின் இவ்வாறான தாக்கங்களுக்கு ஆளாகக்கூடிய வாய்ப்புகள் அதிகம்.

பெற்றோரின் கடமை:

- **மென்பொருள் மெருகேற்றம் செய்யப்பட்டிருப்பதை உறுதி செய்யவும்**
  உங்கள் பிள்ளையின் கணனியில் பாதுகாப்பு பெட்ச்களின் பிந்திய மெருகேற்றங்களையும், மெருகேற்றப்பட்ட வைரஸ் காப்பான் ஒன்றையும் கொண்டிருப்பதை உறுதி செய்யவும்.
- **தமது பிள்ளைகளுடன் பெற்றோர் ஈடுபாட்டை பேண வேண்டும்**
  கணனியில் விடயமொன்றை பிள்ளைகள் தேடும் போது, கேம்ஸ் விளையாடும் போது அல்லது பாடசாலை வேலையை செய்யும் போது, பெற்றோர் அருகிலிருந்து அவர்களின் செயற்பாடுகளில் நட்பான வகையில் ஈடுபட வேண்டும். இதனூடாக, சிறுவர்களின் ஒன்லைன் செயற்பாடுகளை கண்காணிக்க பெற்றோருக்கு முடிவதுடன், சிறந்த கணனி பண்புகளை தமது பிள்ளைகளுக்கு போதிக்கக்கூடியதாக அமைந்திருக்கும்.
- **திறந்த பகுதியில் கணனியை வைக்கவும்**
  பிள்ளைகள் என்ன செய்கின்றனர் என்பதை பெற்றோரால் இலகுவாக கண்காணிக்கக்கூடியதாக இருக்க வேண்டும். வழமைக்கு மாறாக, செய்யக்கூடாத ஏதேனும் விடயங்களை பிள்ளை செய்கின்றதாயின், பெற்றோர் தலையிட்டு, அவற்றால் எழக்கூடிய பாதிப்புகளை தவிர்த்துக் கொள்ள முடியும்.

விதிமுறைகளை நிர்ணயித்து ஆபத்துக்கள் பற்றி எச்சரிக்கவும்

கணனியில் பிள்ளைகளுக்கு என்ன விடயங்கள் செய்ய அனுமதியளிக்கப்பட்டுள்ளனர் என்பதை அவர்களுக்கு தெளிவுபடுத்தவும். இந்த எல்லைகள், சிறுவர்களின் வயது, அறிவு மற்றும் முதிர்ச்சித்தன்மைக்கு பொருத்தமானதாக இருக்க வேண்டும். கணனியை எவ்வளவு நேரம் பயன்படுத்த அவர்கள் அனுமதிக்கப்படுவார்கள் என்பது பற்றிய விதிமுறையையும் கொண்டிருக்கவும். பார்வையிடக்கூடிய இணையத்தளங்கள், பயன்படுத்தக்கூடிய மென்பொருட்கள் மற்றும் அவர்கள் செய்யக்கூடிய செயற்பாடுகள் பற்றியும் தெளிவுபடுத்தவும். இணையத்தில் காணப்படும் ஆபத்துகள் பற்றி பிள்ளைகளுடன் பேசுவதுடன், அதனூடாக அவர்களால் ஏதேனும் சந்தேகத்திற்கிடமான செயற்பாடுகளை இனங்காண பழக்கலாம்.

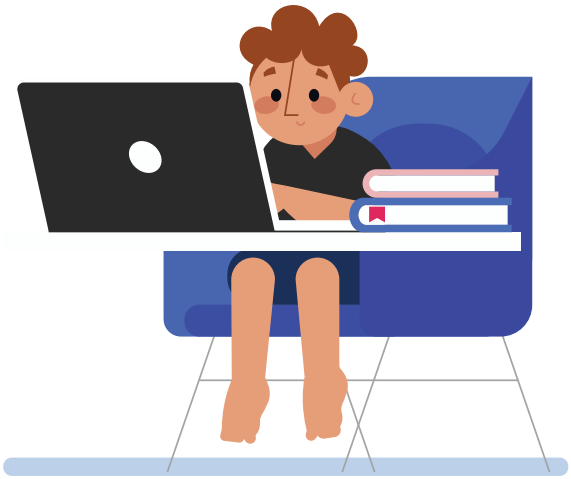
- **கணனி செயற்பாட்டை கண்காணிக்கவும்**
  எந்த இணையத்தளங்களை பார்வையிடுகின்றனர் என்பது அடங்கலாக, உங்கள் பிள்ளை கணனியில் என்ன செய்கின்றது என்பது பற்றி அறிந்திருக்கவும். மின்னஞ்சல், உடனடி தகவல் பரிமாறல் அல்லது chat roomகளை பயன்படுத்துவார்களாயின், அவர்களுடன் தொடர்பிலுள்ளவர்கள் பற்றிய தகவல்களை அறிந்து வைத்திருக்கவும். தமக்கு பரீட்சியமானவர்களுடனான இவர்கள் தொடர்பை கொண்டுள்ளனர் என்பதை உறுதி செய்யவும்.

- **உங்கள் பிள்ளைகளுடன் உங்களால் இலகுவாக உரையாட முடியும் என்பதை அவர்களுக்கு தெரிவியுங்கள்**
  கணனியில் தாம் ஏதேனும் பிரச்சினைகள் அல்லது வழமைக்கு மாறான செயற்பாடுகளுக்கு முகங்கொடுத்தால் அது பற்றி உங்களுடன் இலகுவாக பேசி தீர்வு காண முடியும் என்பதை பிள்ளைகளுக்குச் சொல்லி வையுங்கள்.

- **உங்கள் பிள்ளைகளுக்கு பிரிதான கணக்கொன்றை வைத்திருக்கவும்**
  பெருமளவான operating systemகளில் ஒவ்வொரு பாவனையாளருக்கு ஒவ்வொரு கணக்கை பயன்படுத்தக்கூடிய வசதி காணப்படுகின்றது. உங்கள் கோப்புகளை பிள்ளை தவறுதலாக மாற்றி அல்லது அழித்துவிடக்கூடும் என நீங்கள் அஞ்சினால், அவர்களுக்கென பிரிதொரு கணக்கை தயாரித்து, வரையறைகளை உள்ளடக்கி வழங்க முடியும்.

- **பெற்றோர் கட்டுப்பாடுகளை (parental controls) நடைமுறைப்படுத்தவும்**
  உங்கள் பிரவுசரில் சில parental controls கட்டுப்பாடுகளை விதிக்கவும். உதாரணமாக, Internet Explorerஇல் சில இணையப்பக்கங்களை மாத்திரம் பார்வையிட அல்லது தவிர்க்க அனுமதி காணப்படுகின்றது. இதனால் இந்த வசதியினூடாக கடவுச்சொல்லை நிறுவி அவசியமற்ற இணையத்தளங்களை பிள்ளை அணுகுவதை தவிர்க்க முடியும். இந்த தெரிவுகளை பார்வையிட, உங்கள் menu bar இல் Tools ஐ க்ளிக் செய்து, Internet Options ஐ தெரிவு செய்யவும். அதில் Content ஐ தெரிவு செய்து, Content Advisorஇல் காணப்படும் Enable பொத்தானை அழுத்தவும்.

- **உங்கள் இணைய சேவை வழங்குநரிடமிருந்து கிடைக்கும் உதவிச் சேவைகளை பயன்படுத்தவும்**
  சில இணைய சேவை வழங்குநர்களால் சிறுவர்களை ஒன்லைனில் பாதுகாக்கும் சேவைகள் வழங்கப்படுகின்றன. உங்கள் இணைய சேவை வழங்குநருடன் தொடர்பு கொண்டு, அவர்களிடம் இவ்வாறான ஏதேனும் சேவைகள் காணப்படுகின்றனவா என்பதை பரிசோதித்துக் கொள்ளவும்.



மறுதலிப்பு: இந்த ஆவணத்தில் வழங்கப்பட்டுள்ள வழிகாட்டல்கள் உங்களையும், உங்கள் அன்புக்குரியவர்களையும் சைபர் தாக்குதல்களிலிருந்து பாதுகாக்கும் வகையில் அமைந்துள்ளன. இந்த ஆவணத்தின் ஏதேனும் பிரிவுகள் தொடர்பில் மேலதிக தெளிவுபடுத்தல்கள் தேவைப்பட்டால் அல்லது இந்த ஆவணத்தின் பிரகாரம் எவ்வாறு செயலாற்ற வேண்டும் என்பது பற்றி தெரிந்து கொள்ள வேண்டுமாயின் நிபுணத்துவ ஆலோசனையைப் பெறவும்.

ஐக்கிய நாடுகள் உள்ளக பாதுகாப்பு திணைக்களத்தினால் பிரசுரிக்கப்பட்ட தகவல்களைக் கொண்டு, ஃபெயர்ஃபஸ்ட் இன்சூரன்சின் தகவல் தொழில்நுட்ப திணைக்களத்தின் ஆலோசனையின் பிரகாரம் இந்த ஆவணம் தயாரிக்கப்பட்டுள்ளது.