ISSUE NO 02

செப்டம்பர் 2023

Cyber Guardian

Publication for your online safety

Warning கணினி Hackers ஊடுருவியாளர்களின் இலக்கு கையடக்க தொடலைபேசி

சமீபத்திய அறிக்கைகளின்படி, கையால் எடுத்துச்செல்லக்கூடிய கையடக்க தொலைபேசி டெப் (Tap) - தத்தல் தனிப்பயன் கணினி போன்ற சாதனங்களையே கணினி ஊடுருவியாளர்களின் இலக்காக இருப்பதாக சமீபத்திய அறிக்கைகள் சுட்டிக்காட்டியுள்ளன.

கையடக்க தொலைபேசிகளின் அதிகரிப்பு மற்றும் அவை பெரும்பாலும் தனிப்பட்ட தரவு கடவுச்சொற்கள், கூட்டு வணிக நிறுவனங்களை சார்ந்திருப்பதால் சைபர் குற்றவாளிகளுக்கு கடவுச்சொற்களைத் திருடுவதற்கும் பின்னர் நிறுவன வலைப்பின்னல் அணுகலைப் பெறுவதற்கும் வசதியான எளிதான அணுகுமுறையாக மாறியுள்ளது என்பதை இந்த அறிக்கைகளில் சுட்டிக்காட்டப்பட்டுள்ளன.

பெரும்பாலான நிறுவன ஊழியர்கள் தங்கள் நிறுவன வலைப்பின்னல்களை அணுக தங்கள் கையடக்க தொலைபேசி சாதனங்களைப் பயன்படுத்துகிறார்கள்.

கையடக்க தொலை பேசி தொடர்பான இணைய வழி புள்ளிவிவர அறிக்கையின் Finance Online Statistics Report படி, இத்தொகை 39% வரையிலான அதிகரிப்பை எட்டியுள்ளது. ஒரு கருவியை (Device) ஹேக்கிங் செய்வதன் மூலம், சைபர் குற்றச்செயல்களில் ஈடுபடுவோருக்கு நிறுவனத்தின் தரவை அணுகுவதை எளிதாக அனுமதிக்கும்.

கையடக்க தொலைபேசிகளில் உள்ள தரவுகளி அதிகம் என்பதினால் அவை ஹேக் செய்யப்பட்டால், கடன் அட்டை (கிரெடிட் கார்ட்) தகவல்கள், சமூக ஊடக கணக்குகள் உள்ளிட்ட முக்கிய தகவல்களுக்கான அணுகலைப் பெறவும், அவற்றில் உள்ள கேமரா மற்றும் ஒலிவாங்கி (மைக்ரோ/போன்) யை கட்டுப்படுத்துவதன் மூலம் ரகசிய உரையாடல்களைக் கூட "ஒட்டுகேட்க" முடியும்.

கையடக்க சாதனங்களை பயன்படுத்துபவர்களில் பெரும்பாலானவர்கள் குறிப்பிடத்தக்க அளவுக்கும் அதிகமானோர் பாதுகாப்பற்ற வலைப்பின்னல் நெட்வொர்க்குகள் மற்றும் வணிக வலைப்பின்னல்களுக்கு அப்பால், பாதுகாப்பற்ற இடங்கள் ஊடாக (உதாரணமாக FreeWiFi) இணைய தளத்தை அணுகுகின்றனர். ∴போர்ப்ஸ் Forbes Magazine என்ற சஞ்சிகை இவ்வாறான செயற்பாட்டை 80% எனக் குறிப்பிட்டுள்ளது. இணைய வழி மோசடிகளில் கிட்டத்தட்ட 70% கையடக்க தொலைபேசி தளங்கள் மூலம் இடம்பெறுவதாக இவர்கள் கூறுகின்றனர். பல நிலையங்களின் நிறுவன செயற்பாடுகளுக்கான Bring-your-own-device (BOYD) கொள்கையை தெரிவு செய்கின்றன. கணினி ஊடுருவியாளர்களுக்கு அவற்றின் ஊடாக நிறுவனங்களின் வலைப்பின்னல் அணுகலை பெறுவதற்கான வசதி உண்டு.

Ransomware (பணயத் தீநிரல்) பணம் பறிப்பவர்களிடம் எச்சரிக்கையாக இருங்கள்

Security

Ransomware என்பது தீங்கிழைக்கும் மென்பொருளாகும். இது மீட்கும் தொகை செலுத்தப்படும் வரை ஒரு தனிநபர் அல்லது நிறுவனத்தின் தரவுகளை பணயக்கைதியை போன்று வைத்திருக்கக்கூடியது. இந்த சைபர் குற்றத்தில், கணினி வலைப்பின்னல் Computer networks, நடமாடும் mobile சாதனங்களில் தகவல்களை அணுகக்கூடியது. இவ்வாறு முடக்கி வைக்கப்படும் தரவுகளை மீளப்பெறுவதற்கு அதாவது வழமைபோன்ற எமது செயல்பாட்டு இயக்கத்திற்காக இதற்கான கொடுப்பனவை Bitcoin எண்ணிம நாணயக் குறியீடு: BTC மூலம்பெற முயற்சிப்பார்கள். அதேவேளை இந்த Cryptocurrencies – மிந்நாணயம்/ மென்நாணயத்திற்கு யார் உரிமையாளர் என்பதை எளிதில் கண்டறிய முடியாது.

Ransomware என்ற இந்த வைரசு போன்ற தொற்றிலிருந்து உங்கள் சாதனங்களை எப்படிப் பாதுகாக்கலாம்?

Spam Email மின்னஞ்சல் செய்திகளிலோ அல்லது அறியப்படாத இணையதளங்களிலோ உள்ள இணைப்புகளைக் கிளிக் (clicking) அழுத்துவதை தவிர்த்துக்கொள்ளுங்கள். தீங்கிழைக்கும் இணைப்புகளை நீங்கள் கிளிக் செய்தால், ஒரு தானியங்கி பதிவிறக்கம் தொடங்கப்படலாம் மற்றும் உங்கள் கணினி பாதிக்கப்படலாம்.

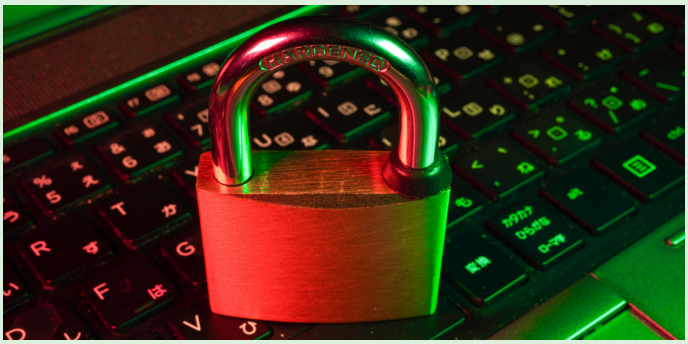
தனிப்பட்ட தகவல்களை வெளியிடுவதைத் தவிர்க்கவும்: தனிப்பட்ட தகவலைக் கேட்டு நம்பத்தகாத மூலத்திலிருந்து Untrustworthy source அழைப்பு, குறுஞ்செய்தி அல்லது மின்னஞ்சலைப் பெற்றால்,அவற்றுக்கு பதிலளிக்கக்கூடாது. சந்தேகத்திற்கிடமான மின்னஞ்சல் இணைப்புகளைத் திறக்க (Avoid opening) வேண்டாம். இதேபோன்று சந்தேகத்திற்கிடமானதாகத் தோன்றும் இணைப்புகளையும் தவிர்க்க வேண்டும். யூ.எஸ்.பி (USP) அல்லது நம்பத்தகாத (Other storage media) முறையில் நீங்கள் பெற்ற மற்ற சேமிப்பு சாதனங்களை உங்கள் கணினியுடன் இணைக்க வேண்டாம்.

நம்பிக்கைக்குரிய இணைப்புகளை மட்டும் திறக்கவும் அத்தோடு பதிவிறக்கம் செய்ய சரிபார்க்கப்பட்ட மற்றும் நம்பகமான இணையதளங்களை மாத்திரம் நம்பியிருப்பதை கவனத்திற்கொள்ள வேண்டும். எல்லா முக்கியமான தகவல்களையும் காப்புப் பிரதி எடுக்கவும். அவைகள் தவறாமல் முறையாக தொழில்படுகின்றதா என்பதை சரிபார்த்துக்கொள்ள வேண்டும். சமீபத்திய இணைப்புகளுடன் உங்கள் இயக்க முறைமை மற்றும் மென்பொருளை புதுப்பித்த நிலையில் வைத்திருங்கள். புதுப்பித்த வைரஸ் எதிர்ப்பு மென்பொருளைப் பராமரித்து (Up-to-date Anti-virus) இணையத்திலிருந்து பதிவிறக்கம் செய்யப்பட்ட அனைத்து மென்பொருட்களையும் (Software) செயல்படுத்துவதற்கு முன் ஸ்கேன் வருடு (Scan) செய்துகொள்வது முக்கியமானது. மின்னஞ்சல் இணைப்புகளிலிருந்து Macros ஆணைத்தொகுப்புகளை இயக்குவதைத் தவிர்க்கவும்.

இணைய பாதுகாப்பு விழிப்புணர்வு பயிற்சியில் ஊழியர்களை பங்குகொள்வதற்கும் இந்த விடயங்களை தெளிவுபடுத்தி அவர்களை ஊக்குவிக்க வேண்டும்.

Confidential

கடவுச்சொல் (Password) தனிப்பட்ட மற்றும் அந்தரங்கமானது



சமூகத்தின் ஒவ்வொரு பிரஜையும் டிஜிட்டல் சமூகத்தின் உறுப்பினர்கள் என்ற ரீதியில், இணைய பயனாளர்களை பாதுகாக்கும் தொழில்நுட்பமான (Cyber Security) இணைய பாதுகாப்பில் கடைபிடிக்கப்பட வேண்டிய அடிப்படை விடயங்கள் தொடர்பில் இணையப் பாதுகாப்பு மாதத்தில் பல நாடுகள் கவனம் செலுத்திவருகின்றன. வலுவான கடவுச்சொல்லைப் பயன்படுத்துவது முக்கியமான விடயமாகும். கடவுச்சொற்களை அவ்வப்போது மாற்றுவதும் முக்கியமானது. ஒரே கடவுச்சொல்லை பல இணை தள இயங்குதளங்கள் அல்லது கணக்குகளுக்கு பயன்படுத்தக் கூடாது. ஒரு கடவுச்சொல் பெரிய எழுத்துகள் சிற்றெழுத்துகள் (letters, lowercase letters), இலக்கங்கள், உட்பட குறைந்தது பத்து எழுத்துகளைக் கொண்டிருக்க வேண்டும். அத்துடன் அவை வலிமைக்கான சிறப்பு எழுத்துக்களாகவும் இருப்பது அவசியம். இரண்டு காரணி Two-factor Authentication அங்கீகாரத்தை செயல்படுத்தப்படுவது உறுதிப்படுத்தப்படுவது முக்கியமானதாகும். இதேபோன்று , உங்கள் மென்பொருளை அவ்வப்போது புதுப்பித்துக்கொள்ளுவதுடன் (Regular Software Updates) தன்னியக்க புதுப்பிப்புகளை செயல்படுத்துவதில், உங்களை தயார்படுத்திக்கொள்வதும் பாதுகாப்பான இணையதளங்களை Secure Web Browsing மட்டுமே பயன்படுவதிலும் கவனம் செலுத்த வேண்டும். பாதுகாப்பான இணையதளங்களை மட்டுமே பயன்படுத்துவதும் Firewalls மற்றும் Network Security பாதுகாப்புகளை கொண்டிருப்பதும், பாதுகாப்பான இணைய உலாவலுக்கு HTTPS ஐப் பயன்படுத்துதல் சந்தேகத்திற்குரிய கோப்பு இணைப்புகளைத் திறப்பதைத் தவிர்ப்பதும் முக்கியமானது.

இதேவேளை மின்னஞ்சல்களைப் பயன்படுத்தும் போது சந்தேகத்திற்கிடமான இணைப்புகளை Attachment திறப்பதை தவிர்ப்பதும், வழக்கமான பாதுகாப்புக்கான சேமிப்புக்கான காப்புப்பிரதிகளை வைத்திருப்பது போன்றவை பொது மக்களின் இணைய (cyber security பாதுகாப்புக்கு அத்தியாவசியமானவை.

Risk

சமூக ஊடகங்கள் - உங்கள் ஒழுக்கம் தொடர்பிலான சான்றிதழ்

தற்போது மிகவும் பிரபலமாக விளங்கும் ∴பேஸ்புக் Facebook, போன்ற சமூக ஊடகங்களைப் பயன்படுத்தும் போது முக்கியமாக கவனிக்க வேண்டிய சில விடயங்களில் கவனம் செலுத்தவது அவசியமாகும்.

மின்னஞ்சல் முகவரி, தொலைபேசி எண், புகைப்படங்கள் மற்றும் உங்கள் சுயவிவரத் தகவல்களை யார் பார்க்கலாம் என்பதைத் நீங்கள் தீர்மானிக்க வேண்டியது மிக அவசியம்.இது நண்பர்களுக்காக மட்டுமே அமைக்கப்பட்டது என்பது முக்கியமாகும்.

விசேடமாக நீங்கள் பொதுவில் பகிர விரும்பாத புகைப்படங்கள் அல்லது பிற உள்ளடக்க விடயங்களில் கூடுதல் கவனம் செலுத்த வேண்டும். சமூக ஊடகங்களில் நீங்கள் பகிரும் தகவல்களின் அடிப்படையில் நீங்கள் எப்படிப்பட்டவர் என்பதை சமூகம் தீர்மானிக்கும். இது உங்களுக்கான சொந்த எழுத்து மூலமான சான்றிதழ் என்பதை புரிந்துகொள்ள வேண்டும். இதுவரையிலான உங்கள் தகவல் அறிக்கைகள் உங்கள் பிம்பத்தைக் காட்டும் கண்ணாடியாக இருப்பதால், அவை எதிர்காலத்தில் உங்களுக்கு எதிராகப் பயன்படுத்தப்படலாம் என்பதைக் கவனத்தில் கொள்ள வேண்டும். ஒரு புதிய தொழிலை நீங்கள் தேடும் போது, உங்களது வருங்கால முதலாளி உங்களைப் பற்றிய தகவலைக் கண்டறியும் முதல் இடம் இது என்பதை நீங்கள் நினைவில் கொள்ள வேண்டும்.

இந்தப் விடயங்கள் தொடர்பில் மிகுந்த விழிப்புணர்வுடன் செயல்படுவதன் மூலம், நாட்டின் டிஜிட்டல் வளர்ச்சி மிகவும் பாதுகாப்பாக முன்னெடுக்கப்படும் திறனைத் தீர்மானிக்கும் என்பதிலும் கவனம் செலுத்துவது சிறப்பானதாகும்.

Beware

பெண்களுக்கு மட்டும்

விசேடமாக, நீங்கள் ஒரு பெண்ணாக இணையத்திற்குள் பிரவேசிக்கும் போது ஆணுக்கு ஏற்படாத பாதுகாப்புச் சிக்கல்கள் மற்றும் தடைகளை நீங்கள் எதிர்கொள்ள நேரிடும். பாலியல் துன்புறுத்தல், அச்சுறுத்தல்கள், தனிப்பட்ட புகைப்படங்கள் மற்றும் வீடியோக்களை அங்கீகரிக்கப்படாது பகிர்தல் போன்றவை பெண்கள் எதிர்கொள்ளும் பல பிரச்சனைகளாக இன்று இணைய உலகில் அமைந்துள்ளன. இவை இணைய உலகில் பெண் மற்றும் ஆணின் உறவை அடிப்படையாகக் கொண்ட பாலியல் துஷ்பிரயோகங்கள்.

நீங்கள் ஒரு புத்திசாலிப் பெண் என்ற ரீதியில் இணைய வெளியில் ஏற்படும் ஆபத்துகள் குறித்து நீங்கள் எப்போதும் தெளிவுடன் விழிப்புடன் இருப்பதுடன், பாலின அடிப்படையிலான இணைய துஷ்பிரயோகத்திலிருந்து உங்களைப் பாதுகாத்துக் கொள்ள அவை தொடர்பான உங்கள் திறமைகளை வளர்த்துக் கொள்ள வேண்டும். ஒரு பெண்ணாக நீங்கள் எதிர்கொள்ளக்கூடிய சில இணைய அச்சுறுத்தல்கள் பின்வருமாறு:

Cyber bullying இணைய உலக அடாவடித்தனங்கள்

Cyber bullying சைபர் புல்லிங், என்பது ஒரு நபரை சங்கடப்படுத்த, அவமானப்படுத்த, அச்சுறுத்த அல்லது வாய் திறக்காது அமைதிப்படுத்த சமூக ஊடகங்கள், மின்னஞ்சல் அல்லது மொபைல் போன் கையடக்க தொலைபேசி களைப் பயன்படுத்தும் செயற்பாடாகும். Facebook, WhatsApp, Viber, Instagram மற்றும் பிற சமூக ஊடகங்கள் மூலம் பின்வரும் பிரச்சனைகள் ஏற்படக்கூடும்.

Doxing டொக்சிங்

Doxing என்பது உங்கள் அனுமதியின்றி உங்கள் வீட்டு முகவரி தொலைபேசி எண், மின்னஞ்சல் முகவரி அல்லது பணியிடம் போன்ற உங்களின் தனிப்பட்ட தகவல்களைப் பகிரும் இணைச் செயற்பாடு. இதுபோன்ற தனிப்பட்ட உங்களது தகவல்களை ஒரு குற்றவாளி உங்களை மிரட்ட அல்லது உங்களைப் போன்று ஆள்மாறாட்டம் செய்ய பயன்படுத்த முடியும்.

Cyber-stalking சைபர்-ஸ்டாக்கிங்

Cyber-stalking சைபர்ஸ்டாக்கிங் என்பது உங்களைத் துன்புறுத்துவதற்காக அல்லது உங்களைத் தொடர்புகொள்வதற்காக இணையத்தில் உள்ள உங்கள் தனிப்பட்ட தரவை (உங்கள் நிதி விவகாரங்கள், சமூக தொடர்புத் தகவல், தனிப்பட்ட மற்றும் தொழில் வாழ்க்கைத் தரவு, உங்கள் பயணங்கள் பற்றிய தகவல்கள் போன்றவை) சேகரிப்பதாகும்.

Revenge Porn பழிவாங்கு வதற்காக ஆபாச காட்சிகளை பயன்படுத்தல்

Revenge Porn என்பது இணைய தளங்கள் ஊடாக ஒரு பெண்ணின் நிர்வாண அல்லது பாலியல் படங்களை விநியோகிக்கும் நடவடிக்கையாகும் . பெரும்பாலும் இதுபோன்ற சம்பவங்கள் முன்னாள் காதலர்களால் பழிவாங்கும் நோக்கத்துடன் அல்லது துஷ்பிரயோகம் செய்யும் நோக்கத்துடன் செய்யப்படுவதாக தெரிவிக்கப்படுகிறது. இதுபோன்ற அச்சுறுத்தல்களை நீங்கள் எதிர்கொண்டால், அவை இணைய மிரட்டலாக அடையாளப்படுத்தப்படுகிறது. அந்தச் சிக்கல்களைத் தடுப்பதற்கும், தொடர்புடைய சமூக ஊடகங்களில் புகார் செய்வதற்கும், மேலும் அடுத்த நடவடிக்கைகளுக்கும் நீங்கள் சட்டத்தின் உதவியை நாட முடியும்.