MODULE 3

டிஜிட்டல் பாதுகாப்பினை மேம்படுத்தல்

பதிப்பு

முதற் பதிப்பு மார்ச் 2020

பிரசுரித்தவர்கள்:
இலங்கை தேசிய கிறிஸ்தவ சுவிசேஷக ஐக்கியத்துவின் **(NCEASL)**
மைனர்மட்டர்ஸினால் **(MinorMatters)** பிரசுரிக்கப்பட்டது.

வலையமைப்பு: **www.minormatters.org**

நூலாசிரியர்: நாலக்க குணவர்தன

செயல் திட்ட ஒருங்கிணைப்பு:

யாமினி ரவீந்திரன், சட்ட மற்றும் ஆலோசனை இயக்குனர்
ஷலோமி டானியல், சட்ட மற்றும் ஆலோசனை ஒருங்கிணைப்பாளர், சமய சுதந்திரம் மற்றும் சமூகநீதி ஆணைக்குழு
அக்னா பலிகவதன, ஊடக தந்திரோபாய அலுவலகர், சமய சுதந்திரம் மற்றும் சமூகநீதி ஆணைக்குழு

முகப்புத்தக வடிவமைப்பு: சஞ்சயன் அய்யாதுரை

பக்க ஒழுங்கமைப்பு மற்றும் வடிவமைப்பு: சேனல் ஜேசுடியன்

பொறுப்புத் துறப்பு:
இப் பிரசுரங்களில் வெளிப்படுத்தப்பட்டிருக்கும் ஆராய்ச்சி மற்றும் கருத்து என்பவை பங்களிப்பாளர்கள் மற்றும் நூலாசிரியரால் வெளிப்படுத்தபட்டவை.அது இலங்கை தேசிய கிறிஸ்தவ மறு பிரவேச கூட்டணியினுடையதாக இருக்க வேண்டிய அவசியமில்லை. அதற்கு இவ்வமைப்பு பொறுப்புக்கூறாது.

டிஜிட்டல் பாதுகாப்பினை மேம்படுத்தல்

வலைத்தளம் எனப்படுவது உலகில் காணப்படும் கணனிகளை ஒன்றிணைத்து தகவல் பரிமாற்றங்களுக்காக உருவாக்கப்பட்ட இலத்திரனியல் வலைப்பின்னல் ஆகும்.

இந்த நிஜ உலகின் ஒத்த தன்மையின் பயன்பாட்டிற்காக இணையதளமானது ஒரு சாதாரண தபால் சேவையைப் போன்று பயன்படுத்தப்படுகிறது ஆனாலும் இவை மிக வேகமானவை. தபால் சேவையைப் போன்றே தபாலுறை ஒன்றிற்கும் கடிதத்தை வைத்து தங்களது தகவல்களை ஒருவர் மற்றொருவருக்கு அனுப்பி வைக்கிறார். இணையதளமானது கணனிகள் சிறியதொரு பொதிகள் போன்றதொரு அமைப்புக்குள் டிஜிட்டல் தகவல்கனை அனுப்பி செய்தி பரிமாற்றத்தை மேற்கொள்ள உதவுகிறது.

பூகோள வலையமைப்புடன் பில்லியன் கணக்கான சாதனங்கள் ஒன்றிணைக்கப்பட்டுள்ளன. அவைகளாவன மேம்படுத்தப்பட்ட கணனிகள், தனிப்பட்ட கணனிகள (desktops, laptops or tablets), ஸ்மார்ட் கையடக்க தொலைபேசிகள் மற்றும் ஆயிரக்கணக்கான தயாரிப்பாளர்களினால் தயாரித்து சந்தையில் விடப்பட்ட விசேட சாதனங்கள் என்பவற்றைக் குறிப்பிடலாம்.

"பொதுவான மொழி" ஒன்றினை பயன்படுத்தியே இந்த சாதனங்களை இயக்கி தரவுகள் பரிமாற்றம் செய்யப்படுகின்றன. இந்த மொழியானது பரிமாற்றல் தடுப்பு நெறிமுறை அல்லது இணையதள நெறிமுறை (Transmission Control Protocol/Internet Protocol) என்று அழைக்கப்படும். இணையதளத்தில் இணைக்கப்பட்ட ஒவ்வொரு சாதனங்களும் பரிமாற்றல் தடுப்பு நெறிமுறை அல்லது இணையதள நெறிமுறை ஒன்றுடன் இணைந்து காணப்படும்.

சாதாரணமாக நீங்கள் தபாலில் கடிதமொன்றை அனுப்பும் போது அவை தபாலகத்தினாலேயே கையாளப்படுகிறது. இவை எவ்வாறு சேகரிக்கப்படுகிறது, எவ்வாறு பிரிக்கப்படுகிறது, எவ்வாறு அனுப்பப்படுகிறது மற்றும் விநியோகிக்கப்படுகிறது போன்ற விடயங்கள் பற்றி நீங்கள் கவலைப்படத் தேவையில்லை. இதே போன்றுதான் இணையதள தரவுகளும் பல்தரப்பட்ட கம்பிகள், திசைவிகள் மற்றும் கணனிகளினூடாக அது சென்றடைய வேண்டிய இடத்தைச் சென்றடைகிறது.

2018 ஆம் ஆண்டின் இறுதிக் காலகட்டத்தில் மேற்கொள்ளப்பட்ட கணக்கெடுப்பின்படி உலகில் சுமார் 3.9 பில்லியன் இணையதள பாவனையாளர்கள் மில்லியன் கணக்கான அரச, தனியார், தொண்டு நிறுவனங்களில் பாவிக்கப்பட்டிருந்ததாகக் கணிக்கப்பட்டுள்ளது. அநேகமான பகுதிகளில் இணையதள தேடல் அநுபவங்கள் பாதுகாப்பானதாகவும் திருப்திகரமானதாகவும் காணப்பட்டதாகத் தெரிவிக்கப்பட்டுள்ளது. ஆனாலும் பல்வேறுபட்ட சாதனங்கள் ஒன்றுடனொன்று இணையும்போது சில நேரம் இவைகள் தவறான திசைகளில் செல்வதற்கும் வாய்ப்புகள் காணப்படுகின்றன. இதன் காரணமாகவே இணைய பாதுகாப்பு அல்லது கணனிசார் பாதுகாப்பு மிக முக்கியமானதாக காணப்படுகிறது.

கணனி பாதுகாப்பு எனப்படுவது விடயங்களையும் முறைமைகளையும் உள்ளடக்கியவை: மேலும் அவை பாவிக்கும் மக்களைப் பற்றியவை. இந்தப் பாடப்பரப்பில் நாம் கணனி பாதுகாப்பு பற்றிய அடிப்படை விடயங்களை அறிந்து கொள்வோம். அடுத்த பாடப்பரப்பில் காணப்படும் கணனி பாதுகாப்பு பகுதியில் டிஜிட்டல் சேவைகளைப் பயன்படுத்தும் போது அவற்றை பெற்றுக்கொள்ளுபவர்களின் பாதுகாப்பு பற்றிய விடயங்களை அறிந்து கொள்வோம்.

முக்கிய சொற்கள்

டிஜிட்டல் பாதுகாப்பு (தகவல் தொழில்நுட்ப பாதுகாப்பு என்றும் அழைக்கலாம்) எனப்படுவது டிஜிட்டல் முறையில் பதிவேற்றப்பட்ட தகவல்களுக்கான பாதுகாப்பு நடைமுறைகளை குறிக்கும். இதற்காக பயன்படுத்தப்படும் சாதனங்கள் இணைய வலையமைப்புடன் இணைக்கப்பட்டோ அல்லது இணைக்கப்படாமலோ காணப்படலாம். கணனி பாதுகாப்பு வரையறைக்குள் பௌதீக மற்றும் இணைய பாதுகாப்பு ஆகிய இரண்டையும் நாம் உள்ளடக்கலாம்.
கணனி பாதுகாப்பு: இணையதளங்களில் கணனிகள் இணைக்கப்பட்டு இருக்கையில் அவற்றைப் பாதுகாப்பதற்காக மேற்கொள்ள வேண்டிய முன்னெச்சரிக்கைகள். விசேடமாக இவை உரிமைகளற்ற முறையில் தரவுகள், தகவல்களை பெற்றுக்கொள்வதை (கணனிகளை தாக்கப்படுவதை) தடுப்பதற்கு உதவியளிக்கிறது.

மேக கணனி முறை **(Cloud computing)** என்றால் கணனியிலுள்ள வன்தட்டில் தகவல், நிகழ்ச்சிகளை சேகரிக்காமல் இணையதளங்களில் சேமித்துக் கொள்ளும் முறை ஆகும். மேக முறை இணையதளத்துக்கான ஒரு உருவகம **(metaphor)** ஆகும்.

Source: https://searchsecurity.techtarget.com/definition/cybersecurity

டிஜிட்டல் பாதுகாப்பு மற்றும் கணனி பாதுகாப்பு ஆகியவற்றின் அடிப்படை அம்சங்கள்

நாம் டிஜிட்டல் சாதனங்களை பாவிக்கும்போது எமது தனிப்பட்ட, இரகசியமான, நாம் பணிபுரியும் இடங்களிலுள்ள அலுவலக ரீதியான, ஆக்கத்திறனான மற்றும் ஏனைய பல வகையான தரவுகளை வழங்குகிறோம். இணையதள வலையமைப்பொன்றுடன் இணைக்கப்பட்டுள்ள கணனியொன்றுடன் நாம் இணைக்கும் போது – எமது நிறுவனத்துக்கு உள்ளேயோ அல்லது உலகளாவிய இணைய வலையமைப்புடனோ – நாம் மற்றவர்களது தரவுகளுடன் சம்மந்தப்படுகிறோம்.

எங்களது சாதனங்களையும் தரவுகளையும் பாதுகாப்பது மிக முக்கியமானதாகும், அதே போன்று மற்றவர்களது தரவு பாதுகாப்புக்கு மரியாதை கொடுப்பதும் மிக முக்கியமான ஒன்றாகும். இணையதளம் போன்ற ஒன்றுடனொன்று இணைந்து காணப்படும் வலையமைப்புகளில் நாம் அனைவரும் விழிப்புடனும் அவதானமானவும் இருப்பது மிக முக்கியமாகும். இவற்றில் ஒருவர் அவதானமிழந்து இருப்பினும் மற்றவர்கள் அனைவரையும் பாதிப்புக்குள்ளாக்கவும் வழியமைக்கும்.

டிஜிட்டல் பாதுகாப்பு அல்லது கணனி பாதுகாப்பு எனப்படுவது அதிகாரமளிக்கப்படாதவர்களின் ஊடுருவல்கள் மட்டுமே என்று எண்ணிவிடக்கூடாது. எங்களது அறியாமை அல்லது அவதானக் குறைவின் காரணமாகவும் சேமிக்கப்பட்டிருக்கும் தரவு, தகவல்களை இழந்துவிடக்கூடிய சந்தர்ப்பங்களும் அதிகமாகக் காணப்படுகிறது. இதன் விளைவாக எமது தரவுகள் பாதிக்கப்படுவது மட்டுமல்லாமல் அவற்றை இழந்துவிடவும் வாய்ப்புகள் உண்டு. வெள்ள அனர்த்தம், தீப்பரவல் மற்றும் மின்சாரப் பாதிப்பு போன்ற எதிர்பாராத நிகழ்வுகளினாலும் எமது தரவுகள் பாதிக்கப்பட வாய்ப்புண்டு.

கணனி பாதுகாப்பு அல்லது டிஜிட்டல் பாதுகாப்பு எனப்படுவது அதி தீவிரமான பாதுகாப்பு ஏற்படுகளை தன்னகத்தே ஏற்படுத்திக் கொள்வது மட்டுமே என்று பொருள்கொண்டு விடக்கூடாது. சில நேரம் நாங்கள் மிகப்பொருத்தமான தீர்வு என்று எண்ணிக்கொள்ளும் ஒரு விடயம் சாத்தியமற்றதாகி விடலாம். எனவே காலத்துக்குக் காலம் அவை பற்றி வெளிவரும் புதிய அம்சங்கள் பற்றி தெளிவைப் பெற்றிருப்பதோடு எமது பாதுகாப்பு முறைமைகளையும் மீள்பரிசீலனை செய்து கொள்ள வேண்டும், குறிப்பாக இணையதள பாவனையாளர்கள் இவற்றைக் கவனத்தில் எடுத்துக்கொள்ள வேண்டும்.

தயவு செய்து ஞாபகத்தில் வைத்துக்கொள்ளுங்கள்: நல்ல ஆரோக்கியமான கணனி பாதுகாப்பு மற்றும் டிஜிட்டல் பாதுகாப்பு அம்சங்களுக்கு பாவனையாளர்களின் ஈடுபாடு, கடப்பாடுகள் மற்றும் அவை பற்றிய சரியான தெளிவுகள் போன்றன மிக இன்றியமையாதது ஆகும். நாம் எமது சில தேவைகளான மென்பொருள், வன்பொருள் விடயங்களுக்காக வெளியிலுள்ள ஒருவரை தகவல் தொழில்நுட்ப சேவை வழங்க கேட்டுக்கொள்வது போன்றதொரு விடயமல்ல.

டிஜிட்டல் பாதுகாப்பு அல்லது கணனி பாதுகாப்பு முறைமையில் கடைப்பிடிக்க வேண்டிய ஒவ்வொரு விடயங்களையும் இங்கே பட்டியலிடுவதென்பது சாத்தியமற்றதொரு விடயம் ஆகும். இவை பற்றிய எண்ணிலடங்கா ஆலோசனைகளும் விடயங்களும் இணையதளங்களில் நீங்கள் பெற்றுக் கொள்ளலாம். கீழே வழங்கப்பட்ட சில பொதுவான விடயங்கள் இவை பற்றிய அடிப்படை விடயங்களை உங்களுக்கு வழங்குகிறது.

Source: https://wiobyrne.com/digital-hygiene/

டிஜிட்டல் ஆரோக்கியமே முக்கியமான விடயம்!

டிஜிட்டல் ஆரோக்கியம் எனப்படும் சொல்லானது ஒருவரது டிஜிட்டல் சாதனங்கள், கணக்குகள் மற்றும் தரவுகள் என்பன எவ்வாறு சுத்தமான அல்லது அசுத்தமான நிலையில் காணப்படுகிறது என்பதை சுட்டிக்காட்ட பயன்படுத்தப்படுகிறது.
நல்லதொரு டிஜிட்டல் ஆரோக்கியம் என்பது எமது இல்லங்களிலும் வேலைத்தளங்களிலும் ஒரே மாதிரியானதாகக் காணப்பட வேண்டும். தனிக்கணக்குகள் அல்லது சாதனங்கள் மற்றவர்கள் அவற்றுக்குள் நுழைவதற்கான வாய்ப்பாக அமைந்து விடலாம். அவ்வாறன்றி இவை தீங்கு விளைவிக்கும் ஒன்றால் இடம்பெற்றிருப்பின் உங்களது தகவல்கள், தரவுகள், ரகசிய இலக்கங்கள் மற்றும் கணக்குகள் போன்றவை ஆபத்தான நிலைக்குள் காணப்பட்டு உங்களது கணனி மோசமான விளைவுகளை எதிர்கொள்ள நேரிடும்.

கணனி வைரஸ் அல்லது கணனிகளுக்கு தீங்கு விளைவிக்கக்கூடிய விடயங்களிலிருந்து எவ்வாறு உங்கள் தரவுகளை பாதுகாத்துக் கொள்வது.

கணனி வைரசுக்கள் எனப்படுவது மிகச் சிறியதொரு நிகழ்ச்சி மூலம் ஒரு கணனியிலிருந்து மற்றைய கணனிகளுக்கு மின்னஞ்சல்கள், மின்னஞ்சல் இணைப்புக்கள் மற்றும் சிறிய தரவேற்றிகளின் மூலம் பரவக்கூடியது. இப்படியான வைரசுக்கள் உங்களது கணனிகளுக்குள் ஊடுருவுவதன் மூலம் அங்கு காணப்படும் தரவுகளின் சாதாரண நிலைமைகளில் மாற்றங்களை அல்லது அதன் முழு வடிவத்தையும் அழிக்கக்கூடியவை.

- கணனி வைரசுக்களை எதிர்க்கக்கூடிய வைரஸ் பாதுகாப்புக்களை பயன்படுத்துங்கள்
- உங்களது இயங்கு தளங்கள (Windows, FireFox மற்றும Chrome) போன்றன காலத்துக்கேற்ற வகையில் புதுப்பிக்கப்பட்டுள்ளவையா என்பதை உறுதிப்படுத்திக் கொள்ளுங்கள். இதன் இறுதி பதிப்பானது உங்களுக்கு சரியான பாதுகாப்பை வழங்கும்.
- மின்னஞ்சல் இணைப்புகளை பயன்படுத்தும் போது மிகவும் அவதானமாக இருங்கள்: உங்களுக்கு பரீட்சியமல்லாத, உறுதியற்ற விடயங்கள் ஏதாவது காணப்படின் அவற்றை திறப்பதிலிருந்து விலகியிருங்கள்.
- தேடல் தளங்களில் காணப்படும் கட்டுப்பாட்டு இயக்கியை (pop-up blocker) எப்போதும் இயங்கச் செய்யுங்கள்.
- உங்களது தேடல்களின் போது எப்போதும் ஒரு கட்டுப்பாட்டு இயக்கியை பயன்படுத்துங்கள். அநேகமான கட்டுப்பாட்டு இயக்கிகள் பாதிப்பான தீங்கு விளைவிக்கக்கூடிய விடயங்களை தன்னகத்தே கொண்டவை. மேலும் இவை உங்களது கணனிகளுக்கும் அவற்றுக்குள் காணப்படும் தரவுகளுக்கும் பாதிப்பு ஏற்படுத்துபவை.
- தடுப்பு சுவர (firewall) ஒன்றினை எப்போதும் பதிவிறக்கம் செயது கொள்ளுங்கள். இதுவே உங்களது கணனிகளுக்குள் வரும் விடயங்களை அவதானித்து நெரிசல்களைக் கட்டுப்படுத்துகிறது. உங்களது கணனிகளில் ஏலவே காணப்படும் வைரஸ் பாதுகாப்பு செயலியுடன் இணைந்து இவை மேலதிக பாதுகாப்பையும் வழங்குகிறது.
- நிருவாகக் கணக்குகளுக்கு எப்போதும் ரகசிய குறியீடொன்றை பாவியுங்கள்.

குறிப்பு: உங்களது சாதனங்கள் சில வேளைகளில் தாக்கங்களுக்கு உட்பட்டிருப்பினும் அவை எப்பொழுதும் அறிந்து கொள்ளக்கூடிய வகையில் இலகுவாகக் காணப்படும் என்று எண்ண வேண்டாம். எனவே தொடர்ந்து வைரஸ் அழிப்பு செயலிகளை புதிப்பித்து நுட்பமான சோதனைகளை மேற்கொள்ள வேண்டும்.

வைரஸ் தொற்றுக்கு உள்ளானதற்கான அறிகுறிகள்

தீங்கு விளைவிக்கும் வைரஸ் தாக்கங்களுக்கு உள்ளானதை அடையாளங்கண்டு கொள்வதற்கான சில இலகு வழிகள் இங்கு தரப்பட்டுள்ளன.

- நல்லதொரு காரணம் இன்றி உங்களது சாதனங்கள் மிகவும் குறைவான வேகத்தில் இயங்கும்.
- உங்களது சாதனங்கள் திடீரென மீள் ஆரம்பம் செய்து கொண்டிருக்கும் அதே வேளை வழமைக்கு மாறான விடயங்களைக் காட்டிக் கொண்டிருக்கும்.
- உங்கள் சாதனங்களில் காணப்படும் செயலிகள் நீங்கள் எதிர்பார்க்கும் அளவுக்கு செயல் திறனுள்ளதாகக் காணப்படமாட்டாது.
- அங்கு வழமைக்கு மாறான சில பிழையான தகவல்கள் திரையில் காணப்படும் (சில வேளைகளில் பிழையான முறையிலும் எழுதப்பட்டிருக்கும்)
- பாவனையாளர்களினால் உருவாக்கப்படாத சில குறுகிய செயலிகள் உருவாக்கப்பட்டிருப்பதை அவதானிக்கலாம்.
- தகவல்களை சேகரித்து வைப்பதற்கான போதிய இட வசதிகள் இல்லாமல் காணப்படும்
- உங்களது அனுமதியேதுமின்றி கோப்புகள் மற்றும் செயலிகள் அழிக்கப்பட்டு காணப்படும

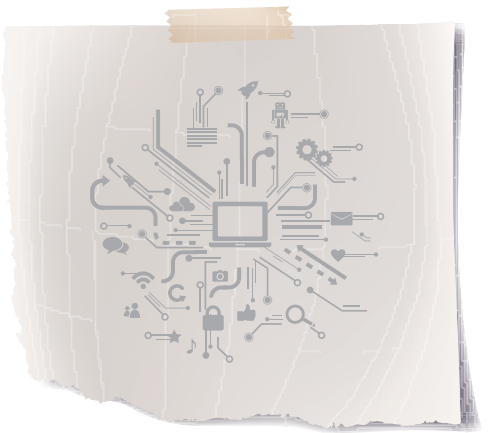
தரவுகளை மீள சேமித்துக் கொள்ளல்
(BACKING-UP DATA)

தரவு ஊழல் அல்லது இழப்பு என்பன நல்லதொரு மென்பொருள் மற்றும் வன்கொருள் காணப்படினும் இடம்பெறலாம். எனவே தரவுகளை மீள சேமித்துக் கொள்ளல் இப்படியான விடயங்களிலிருந்து தம்மைப் பாதுகாத்துக் கொள்ளும் ஒரு சிறந்த முறை என்பதோடு தங்களுக்கு தேவைப்படும் போது அவற்றை மீளப் பெற்றுக் கொள்ள வசதியையும் கொடுக்கிறது.

பொதுவான தரவு மீள் பெற்றுக்கொள்ளும் முறையானது உங்களது கணனியின் வன்தட்டு சேமிப்பகத்திலிருக்கும் (hard disk) தரவு ஊழல் அல்லது இழப்பு என்பன நல்லதொரு மென்பொருள் மற்றும் வன்கொருள் காணப்படினும் இடம்பெறலாம். எனவே தரவுகளை மீள சேமித்துக் கொள்ளல் இப்படியான விடயங்களிலிருந்து தம்மைப் பாதுகாத்துக் கொள்ளும் ஒரு சிறந்த முறை என்பதோடு தங்களுக்கு தேவைப்படும் போது அவற்றை மீளப் பெற்றுக் கொள்ள வசதியையும் கொடுக்கிறது.

பொதுவான தரவு மீள் பெற்றுக்கொள்ளும் முறையானது உங்களது கணனியின் வன்தட்டு சேமிப்பகத்திலிருக்கும் (USB) பொருளொன்றுக்குள் மாற்றம் செய்து கொள்ளும் முறை ஆகும். அதே போன்று இணையங்களை அடிப்படையாகக் கொண்ட முகில்கள (cloud) முறையைப் பயன்படுத்தியும் உங்களது தரவு, கோப்புக்களை சேமித்து வைத்துக் கொள்ள முடியும் (உதாரணமாக Google போன்ற இணைய அடிப்படையிலான சேமிப்பகம்).

மேக முறையிலான சேமிப்பு முறையானது உங்களுக்கு தேவையான இடத்திலிருந்து தேவையான வேளையில் தேவைப்படும் விடயங்களை தொலைதூர (remote) வன்பொருட்களில (hardware) சேமித்து வைக்க உதவுகிறது. இவற்றை பாவனையாளர்கள் தங்களுக்கு தேவைப்படும் வேளையில் தேவையான போது இணையதள பிரவேசத்தின் மூலம (internet) பெற்றுக் கொள்ளலாம். மேக முறைகள் உண்மையில் தரவுகளை முகாமை செய்வதற்கு மிக இலகுவான வழிவகையாகும். அநேகமான மேக முறைகள் அதிக சேமிப்பு வசதிகளை வழங்குவதுடன் தரவுகள் பாதிக்கப்படாமல் இருப்பதற்கான பாதுகாப்பு ஏற்பாட்டு வசதிகளையும் வழங்குகிறது (Google போன்ற சேவை வழங்குநர்கள் தாம் கணக்கொன்றுக்குள் நுழையும் வேளையில் இலகுவான இலவச சேமிப்பு வசதிகளை வழங்குகிறது)



தரவுகளை மறை குறியாக்குதல் (ENCRYPTING DATA)

மறைகுறியாக்கல் எனப்படுவது (தன்னியக்க மென்பொருளொன்றினால்) அதிகாரமளிக்கப்படாத ஒருவரால் உங்களது தரவுகளை பார்க்க முடியாமல் செய்யும் வழிமுறை ஆகும். இம்முறையானது உங்களது அதி ரகசிய விடயங்களான கடனட்டை ரகசிய இலக்கங்கள் போன்றவற்றை குறிகளாக்கி (encoding) அத்தகவல்களை வாசிக்க முடியாத மறைக்குறியீட்டு எழுத்தாக (cipher text) மாற்றுகிறது. அப்படியான தரவுகள் அதிகார கடவுச் சொற்களின் உதவியுடன் மட்டுமே மறைகுறியீடுகளை நீக்கி (decrypted) வாசிக்க கூடியதாக மாற்றப்படுகிறது.

தரவுகளை மறைகுறியாக்கல் என்பது அவற்றை பாதுகாப்பான இடமொன்றில் சேமித்து வைக்கும் பொறிமுறையாகும் -- அவற்றினை பற்றி ஏலவே அறிந்தவர்களினால் மட்டுமே அதை மீண்டும் வாசிக்க முடியும். மறைகுறியாக்கம் என்பது குறியாக்கவியலின (cryptography) டிஜிட்டல் வடிவம் ஆகும், மேலும் இவை கணித வழிமுறையினைப் பயன்படுத்தியே தகவல்களை துருவி வெளியில் கொண்டுவருகிறது. எனவே அதை உருவாக்கி அனுப்பியவர்களினால் மட்டுமே அவற்றினை வாசிக்க முடியும். அதிகாரமற்ற ஒருவர் அவற்றை வாசிக்க முற்படின் அவை தேவையற்ற (junk) விடயமாக தோற்றமளிக்கும்.

மறைகுறியாக்கலில் இரண்டு பிரதானமான முறைகள் காணப்படுகிறது. ஆவையாவன: சரியான அளவில் (சமச்சீரான) மறைகுறியாக்கல் - இது தனி கடவுச் சொற்களுடன் வழங்கப்பட்டிருக்கும் மற்றும் சரியான அளவிலற்ற (சமச்சீரற்ற) மறைகுறியாக்கல் - இவை தனி மற்றும் பொது குறியீடுகளைக் கொண்டு காணப்படும்.

இணைய பாவனை தொடர்பாடல்களுக்கு மறைகுறியாக்கல் மிகவும் முக்கியமானதொன்றாகும் (உதாரணமாக, மின்னஞ்சல், அரட்டைகள் மற்றும் பரிமாற்றல்கள் இடம்பெறும் பகுதிகள்). இங்கு செய்திகள் மறைகுறியாக்கப்படவில்லையாயின் தீங்கு விளைவிக்கக்கூடிய சில உங்களது செய்திகளை இடைமறிக்க வாய்ப்புகள் காணப்படும்.

முடிவிலிருந்து – முடிவுக்கு வரும் மறைகுறியாக்கி (End-to-end encryption/E2EE) எனப்படுவது தொடர்பாடல்களில் பங்குபற்றும் பாவனையாளர்கள் மட்டுமே செய்திகளை வாசிக்கக் கூடிய முறையில் உருவாக்கப்பட்ட பாதுகாப்பான செய்தி அனுப்பல் முறையாகும். மேலும் இவை வலையமைப்பு சேவை வழங்குநர்கள், இன்டர்நெட் வழங்குநர்கள், மற்றும் ஏனைய தொலைத் தொடர்பாடல் சேவைகள் வழங்குநர்கள் தொடர்பாடல்களை டிஜிட்டல் பரிமாற்ற மறைகுறியாக்க முறையினைப் பாவித்து உரையாடல்களை ஒற்றுக்கேட்பதை தடுக்கும் ஒரு சிறந்த செயல்முறையாகும்.

மறைகுறியாக்கல் முறையானது தொலைத்தொடர்பாடல்களின் நம்பிக்கையையும் ரகசியத் தன்மையையும் உயர்த்தி நிற்கிறது. உதாரணமாகக் கூறுமிடத்து WhatsApp, Signal போன்ற தளங்கள் தானாகவே முடிவிலிருந்து முடிவுக்கான மறைகுறியாக்கி (E2EE) முறையில் மூலம் உருவாக்கப்பட்டிருக்கிறது. இவற்றின் மூலம் இடம்பெறும் கலந்துரையாடலின் உயரிய தன்மையை மேம்படுத்துவதற்கு இவை உறுதுணையாக காணப்படுகிறது.

முக்கியமான தரவுகளை இல்லாது அழித்தல

நீங்கள் கோப்பு ஒன்றினை உங்களது கணனியிலிருந்து அழித்தால் அது முற்றாகவே மறைந்து விடுவதில்லை. இது உங்களது கோப்புகளை சேமித்து வைத்திருந்த தளத்திலிருந்து மாத்திரமே அழிக்கப்படுகிறது. எனவே உங்களது கோப்புக்கள் இன்னுமே வன்தட்டில் சேமிக்கப்பட்டிருக்கிறது, இன்னுமொரு கோப்பொன்று அதன்மேல் உருவாக்கப்படுமிடத்து மாத்திரமே முன்னைய கோப்புகள் அங்கிருந்து அகற்றப்படும். அவ்வாறு அதன்மேல் இன்னுமொரு கோப்பொன்று உருவாக்கப்பட்டிருப்பினும் தேவையேற்படின் முன்னைய தரவுகளை மீளப் பெற்றுக்கொள்வது சாத்தியமாகும்.

நீங்கள் ஏதாவது தரவுகளை முற்றாக அகற்ற வேண்டுமாயின் பாதுகாப்பான முறையொன்றின் மூலம் அவற்றை அகற்ற வேண்டும். அவ்வாறு இல்லாதவிடத்து அத்தரவுகள் அவ்வாறே காணப்படும் அல்லது அதன்மேல் முக்கியமான விடயங்கள் மீளெழுதப்பட வாய்ப்புகள் மிக அதிகம். இவ்வாறான முறையில் அழிக்கப்பட்டாலும் தொழில்நுட்ப வல்லுநர்களினால் அந்த தரவுகளை தேவையேற்படின் மீண்டும் பெற்றுக் கொள்ள முடியும் என்பதை ஞாபகத்தில் வைத்துக் கொள்ளுங்கள்.

"துடைத்தல்" எனும் செயன்முறையானது ஒரு தரவினை மீண்டும் மீண்டும் எழுதுவதனைக் குறிக்கும். Eraser (அழிப்பான் செயலி) எனப்படும் உயர்தர விண்டோவ் செயலியை பயன்படுத்துவதன் மூலம் வன்தட்டுக்களில் காணப்படும் தரவுகள் அதன் மேல் மேலும் மேலும் எழுதப்படுவதன் மூலம் நிரந்தரமாக அழிக்கப்படுகிறது. இது மிகவும் அவதானமாக தெரிவு செய்யப்பட்ட ஒரு முறையினால் நடைமுறைப்படுத்தப்பட வேண்டும் என்பது குறிப்பிடத்தக்கது.

Https://eraser.Heidi.Ie/

இணைய முறையில் இருக்கும் போது உங்களது தரவுகளை பாதுகாத்தல்.

Wi-Fi அல்லது wireless இணையதளம் எனப்படுவது கம்பிகளேதும் இல்லாமல் வானலை (காற்றலைகளினால்) வலையமைப்பொன்றுடன் தொடர்பு கொள்ளும் முறை ஆகும். இது பாவனையாளர்கள் எந்த இடத்துக்கு நகர்ந்து சென்றாலும் எந்தவொரு இடைஞ்சலுமில்லாமல் தமது தேவைக்கேற்றால் போல சேவைகளை பெற்றுக் கொள்ளக்கூடிய வசதிகளை வழங்குகிறது. எவ்வாறிருப்பினும் இவை மிகுந்த அவதானத்துடன் பயன்படுத்தப்பட வேண்டும் என்பது இங்கு குறிப்பிடத்தக்கதாகும்.

பொது இடங்களில் மிக மலிவாகக் காணப்படும் இலவச Wi-Fi வசதிகளைப் பயன்படுத்தும் போது நாம் மிகுந்த அவதானத்துடன் இருப்பது அவசியம், எமது தரவுகள் குறிப்பிட்ட வலையமைப்புடன் இணைந்து செயற்படுபவர்களினால் இடைமறிப்பு செய்யப்பட வாய்ப்புகள் மிக அதிகமாகக் காணப்படுகிறது. எவ்வாறாயினும் சமூக வலைத்தளங்களான Facebook அல்லது செய்தி வழங்கும் சேவைகள் போன்றனவற்றைப் பாவிப்பதற்கு மிக சிறந்தது, உங்களது தனிப்பட்ட விடயங்களான மின்னஞ்சல் மற்றும் வங்கிக் கணக்குகள் போன்றனவற்றை பொது Wifi இனைப் பயன்படுத்தி செயற்படுத்தாமல் இருப்பது மிக சிறந்தது.

இது ஏன் நிகழ்கிறது? ஏனெனில் நீங்கள் பொது Wi-Fi களைப் பயன்படுத்தும் போது அக்குறிப்பிட்ட வலையமைப்புடன் தொடர்புபட்ட யாராவது ஒருவரினால் உங்களது தரவுகள் இடைமறித்து ஒத்துக்கேட்க வாய்ப்புகள் அதிகமாகக் காணப்படுகிறது, இதற்குரிய காரணம் உங்களது வலையமைப்பு பொதுவானதாக காணப்படுவது ஆகும். உண்மையில் உங்களுக்கு பரீட்சயம் இல்லாத யாராவது ஒருவரினால் வழங்கப்படும் இலவச Wi-Fi இனைப் பயன்படுத்தாது இருப்பது மிக புத்திசாலித்தனமான செயற்பாடாகும். சில குற்றங்களை இழைப்பவர்கள் இப்படியான இலவச அல்லது முரட்டுத் தனமான Wi-Fi வசதிகளை வழங்கி தகவல்களை திருட அதிகமான வாய்ப்புகள் காணப்படுகிறது.

மற்றுமொரு பாதுகாப்பு அறிவுறுத்தல்: இணையதளங்கள் அல்லது சமூக வலைதளங்களுக்குள் நுழைகையில் அப்பகுதியினுடைய தனியுரிமை பற்றிய அறிவுறுத்தல்களைக் கட்டாயம் படித்து விளங்கிக் கொள்ளுங்கள். இவற்றினை இயங்கு தளத்தின் மேற்பகுதியில் அல்லது அடியிலுள்ள பகுதியில் கண்டு கொள்ளலாம். புதிய தளங்களுக்கு செல்கையில் ஆரம்பத்தில் கணக்கிற்கு உட்செல்லும் வாயிலில் அல்லது இருக்கும் கணக்கைக் கொண்டு உட்செல்கையில் இவற்றினை அறிந்து கொள்ள முடியும். எனவே இணைய தளங்களுக்கு நுழைவதற்கு முதலே அவற்றை பற்றி நன்கு அறிந்து கொண்ட பின்னர் உட்செல்வது எப்போதும் மிகச் சிறந்தது.

மின்னஞ்சல், சமூக வலைத்தளங்கள் போன்றவற்றுக்கு மற்றவர்களுக்கும் உபயோகிக்கும் சாதனம் ஒன்றினைப் பயன்படுத்தி நீங்கள் கணக்கொன்றுக்குள் உட்செல்வதாயின் உங்களது வேலைகள் முடிந்தவுடன் கட்டாயம் கணக்கை விட்டு வெளியேறும் (sign out) விடயத்தை மேற்கொள்வதை மறக்காதீர்கள். இதனை சரியாக மேற்கொள்ளாதவிடத்து உங்களுக்கு அடுத்தபடியாக பயன்படுத்துபவர்கள் மிக இலகுவாக உங்கள் கணக்குகளுக்குள் உட்செல்ல இது வழி வகுக்கும், அது மாத்திரமல்லாமல் கணக்குகளுக்குள் மற்றவர்களது அனுமதியில்லாமல் ஊடுருவும் நபர்கள் மிக எளிதாக உங்களது விடயங்களை திருடிவிடுவார்கள் என்பதும் இங்கு கவனிக்கத்தக்க ஒரு விடயமாகும்.

டிஜிட்டல் சொத்துக்களைப் பாதுகாத்தல

உங்களது டிஜிட்டல் சொத்துக்களை பாதுகாப்பதற்கு மிக எளிதானதும் முக்கியமானதுமான சில முன்னெச்செரிக்கைகள் அவசியமாகும்.

கடவுச் சொல் அல்லது அடையாளச் சொல் என்பது பாவனையாளர் ஒருவர் மிக இலகுவாக மனனம் செய்து கொள்ளக்கூடிய வகையில் உருவாக்கப்படும் உள் நுழைவு அனுமதி ஆகும். டிஜிட்டல் பொறிமுறையில் இக்கடவுச்சொற்கள் எழுத்துக்கள், குறிகள் மற்றும் இலக்கங்களைக் கொண்டு இணைந்து ஒழுங்கமைக்கப்பட்டதொரு முறையில் காணப்படும்.

பாதுகாப்பான முறையில் பாதுகாக்கக்கூடிய தங்களுக்கு பரீட்சயமான கடவுச் சொற்களைக் கொண்டிருப்பது உங்களது கணக்குகளுக்குள் அனுமதியில்லாமல் பிறர் அனுமதிப்பதைத் தடுக்கும் மிக முக்கியமான நடவடிக்கை ஆகும். கடவுச் சொல்லானது நீங்கள் நாளாந்த வாழ்க்கையில் பயன்படுத்தும் ஒரு உண்மையான சொல்லாக இருக்க வேண்டிய எந்தத் தேவையுமில்லை: சொல்லொன்று இல்லாமல் வித்தியாசமான ஒன்றாக காணப்படின் மற்றவர்கள் ஊகித்து உங்களது கணக்குக்குள் நுழைவதைத் தடுக்கும் சிறந்த வழிமுறையாகும். ஆகவே மற்றவர்களால் ஊகித்துக் கொள்ளமுடியாத ஒன்றைத் தெரிவு செய்து கொள்ளுங்கள்.

நல்லதொரு கடவுச்சொல்லைத் தெரிவு செய்து கொள்வதற்கான சில ஆலோசனைகள் இங்கே தரப்பட்டுள்ளன.

- உங்களது கணக்குகளை பாதுகாத்துக்கொள்ள எப்பொழுதும் மிகவும் வலிமையான கடவுச் சொல்லொன்றை தேர்வு செய்து கொள்ளுங்கள். இலக்கங்கள், குறியீடுகள், சிறிய எழுத்துக்கள் மற்றும் பெரிய எழுத்துக்கள் உள்ளடங்கலான நீண்டதொரு கடவுச்சொல்லை தெரிவு செய்து கொள்ளுங்கள்.
- உங்களுக்கு நன்கு பரீட்சயமான மிக எளிதில் நினைவில் வைத்துக் கொள்ளக்கூடிய கடவுச்சொல் ஒன்றினைத் தெரிவு செய்து கொள்ளுங்கள்.
- வெளிப்படையாக மற்றவர்களால் ஊகித்துக் கொள்ளக்கூடிய மிக இலகுவான விடயங்களான உங்களது பிறந்த தினம், வருடாந்த நினைவுகள், முகவரி, பிறந்த இடம், உயர்தர பாடசாலை, உறவினர்கள் மற்றும் செல்லப்பிராணிகள் போன்றவற்றை வழங்க வேண்டாம்.
- உங்களது ஒவ்வொரு கணக்குகளுக்கும் வெவ்வேறான கடவுச்சொற்களை வழங்குங்கள். முக்கியமான கணக்குகளுக்கு கடவுச் சொற்களை மீண்டும் மீண்டும் வழங்குவது மிக ஆபத்தானது. இப்படியான நிலையில் ஒருவர் உங்களது கடவுச் சொல்லைப் பெற்றுக்கொண்டால் உங்களது ஏனைய கணக்குகளான மின்னஞ்சல், முகவரிகள் மற்றும் வங்கிக் கணக்குகள் போன்ற எல்லாவற்றுக்கும் நுழைவதற்கு இது வாய்ப்பை ஏற்படுத்திக் கொடுக்கும்.
- உங்களது கடவுச் சொற்கள் ஏதாவது மறந்து போய்விடின் அவற்றை மீளப் பெற்றுக்கொள்ளும் வகையிலான மாற்றுக் கணக்கொன்றை அல்லது வழிமுறைகளை வழங்குங்கள்
- காலத்துக்குக் காலம் உங்களது கடவுச் சொற்களை மாற்றிக் கொள்ளுங்கள் - அடிக்கடி இவற்றில் மாற்றங்களை ஏற்படுத்துவது மிகவும் பிரயோசனமானதொரு விடயம் ஆகும்.
- நீங்கள் பாவிக்கும் இயங்கு தளங்களில் உங்கள் கடவுச் சொற்களை ஞாபகத்தில் வைத்திருக்க அனுமதிப்பது வசதியாக இருக்கலாம், ஆனாலும் இவை ஆபத்தானதொரு விடயம் ஆகும். வேறு யாராவது உங்களது சாதனங்களைப் பாவிப்பின் அவர்கள் மிகவும் இலகுவாக உங்களது கணக்குகளிலுள்ள தொடர்புகள் உட்பட அனைத்து விடயங்களையும் பெற்றுக்கொள்ள இவை வழி வகுக்கும்.

டிஜிட்டல் சொத்துக்கள் யாவை?

மிக இலகுவான மொழிநடையில் கூறுவதானால் டிஜிட்டல் சொத்து எனப்படுவது டிஜிட்டல் தொழில்நுட்பத்தின் மூலம் சேமிக்கப்பட்ட ஒரு உள்ளடக்கம் ஆகும். முகில் **(cloud)** முறையானது படங்கள், வீடியோக்கள், கோப்புக்களைக் கொண்ட எழுத்துக்கள், விரிதாள்கள் அல்லது பகுதிகளைக் கொண்டதொரு முறையாகும். இவ்வாறான டிஜிட்டல் சொத்துக்கள் உங்களது கணனியின் வன்தட்டில் அல்லது ஸ்மார்ட் கையடக்க தொலைபேசியின் நினைவகத்தில் அல்லது இணையதளத்தில் சேகரித்து வைத்துக் கொள்ள முடியும்.

டிஜிட்டல் சொத்துக்கள் எனும் போது உங்களது மின்னஞ்சல் கணக்குகள் மற்றும் சமூக வலைதளங்களுக்கான கணக்குகளும் உள்ளடங்கும்.

இரு முனை அங்கீகார முறைகளை பயன்படுத்தல்

மிக உறுதியான கடவுச்சொல் ஒன்றினை வழங்கியதன் பிற்பாடு மேற்கொள்ள வேண்டிய அடுத்த முக்கியமான நடவடிக்கையானது இரு முனை அங்கீகாரத்தை ஏற்படுத்திக் கொள்வது ஆகும் (இரு முனை உறுதிப்படத்தல் அல்லது இரு முனைகளில் அங்கீகரித்தல் என்றும் அநேகமாகக் கூறப்படும்).

அதாவது நீங்கள் உங்களது கடவுச் சொற்களை வழங்கியதற்கு மேலதிகமாக, நீங்கள் இரண்டாவது பகுதியான தகவல்களை உங்களது கணக்குகளுக்கு வழங்க வேண்டும். இது அநேகமாக உங்களது பதிவு செய்யப்பட்ட கைத்தொலைபேசிக்கு குறுந்தகவல் மூலம் அனுப்பி வைக்கப்படும் (இவை குறிப்பிட்ட சில நிமிடங்களுக்குள் செயல்படுத்தக்கூடிய ஒரு முறை மட்டுமே பயன்படுத்தக்கூடிய ஒன்றாகவே காணப்படும்). பொதுவாக தற்காலத்திலுள்ள எல்லா சமூக ஊடகங்களும் அதே போன்று கூகுள் நிறுவனமும் இந்த இரு முனை அங்கீகார முறைமைகளை தற்போது தேர்ந்தெடுத்துக் கொள்வதற்கான வாய்ப்பினை வழங்குகிறது. இணையதளங்கள் எழுத்து மற்றும் செயலி முறை போன்ற இரு முறைகளையும் அங்கீகரிக்க ஒத்தாசை வழங்குவதாயின், தயவு செய்து செயலி முறையினை மாத்திரமே தெரிவு செய்யவும். இவ்வாறு கூறுவதற்கான காரணம் குறுஞ்செய்திகள் அனுப்பப்படும் போது அவை ஒரு போதும் மறைகுறியாக்கப்படுவதில்லை, எனவே மற்றவர்கள் அதை இடை மறித்துப் பெற்றுக்கொள்ள இவை ஒரு வாய்ப்பாக அமைந்து விடலாம்.

கடவுச் சொற்கள் இரகசியமானவை!

கடவுச் சொல் என்பதன் பொருள் அவை தங்களுக்குரிய இரகசியமானதும் தனிப்பட்டதுமாகும். அவை மற்றவர்களுடன் பகிர்ந்து கொள்ளக்கூடிய ஒரு விடயம் அல்ல. மேலும் இது எந்த விதத்திலும் மற்றவர்களுக்காக காட்சிப்படுத்தக்கூடிய ஒரு பொருளும் அல்ல. இருந்தாலும் இதுவே அநேகமானவர்களால் விடப்படும் மாபெரும் தவறுகளில் ஒன்று என்பதோடு அவ்வாறு ஏதாவது அசம்பாவிதங்கள் நடந்து முடிந்த பின்னரே மனம் வருந்துவதையும் எம்மால் காண முடிகிறது. ஆகவே தயவு செய்து ஞாபகத்தில் வைத்துக்கொள்ளுங்கள்: நீங்கள் பாதுகாப்பான ரகசியமான கடவுச் சொற்களை வழங்கினால் மட்டுமே உங்களது கணக்குகளை பாதுகாத்துக் கொள்ளலாம்.

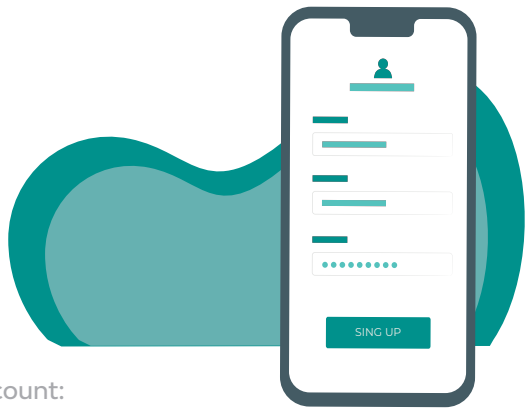
கையடக்க தொலைபேசியின் பாதுகாப்பு

ஒவ்வொரு கையடக்க தொலைபேசி, GSM ஒவ்வொரு கையடக்க தொலைபேசி, (IMEI அல்லது International Mobile Equipment Identity) எனும் தனி அடையாள இலக்கத்தைக் கொண்டு காணப்படும்.

இந்த IMEI இலக்கம் உருவாக்கப்பட்டதற்கான பிரதான காரணம் யாதெனில் கையடக்க தொலைபேசியில் பயன்படுத்தப்படும் சிம் அட்டைகள் நிரந்தரமானதொன்று இல்லை என்பதோடு அது பாவனையாளர்களின் விருப்பத்திற்கேற்ப மாற்றமடையலாம், ஆனாலும IMEI இலக்கம் உருவாக்கப்பட்டதற்கான பிரதான காரணம் யாதெனில் கையடக்க தொலைபேசியில் பயன்படுத்தப்படும் சிம் அட்டைகள் நிரந்தரமானதொன்று இல்லை என்பதோடு அது பாவனையாளர்களின் விருப்பத்திற்கேற்ப மாற்றமடையலாம், ஆனாலும IMEI இலக்கத்தின் அடிப்படையில் அக்கையடக்க தொலைபேசி பற்றி சில மேலதிக தகவல்களை உதாரணமாக கையடக்க தொலைபேசியின் வகை மற்றும் உற்பத்தி ஆண்டு போன்றவற்றை நீங்கள் அறிந்து கொள்ளலாம்.

உங்களது கையடக்க தொலைபேசியின IMEI இலக்கத்தை *#06# sequence. ஐ டயல் செய்வதன் மூலம் நீங்கள் இலகுவாகத் தெரிந்து கொள்ளலாம். அதே போன்று உங்களது கையடக்க தொலைபேசியின் உத்தரவாத காலத்தில் வழங்கப்படும் சேவைகளைப் பெற்றுக் கொள்வதாயின் அல்லது அதற்கான படிவத்தை நிரப்பும் போது இந்த IMEI அடையாள இலக்கம் உங்களுக்கு மிகவும் உறுதுணையாகக் காணப்படும். அதே போன்று உங்களது கையடக்க தொலைபேசி தொலைந்தோ அல்லது திருடப்பட்டாலோ இந்த ஐஆநுஐ இலக்கத்தைக் கொண்டு சம்பவம் இடம்பெற்ற பிரதேசத்திலுள்ள பொலிஸ் நிலையத்திலோ அல்லது வலையமைப்பு சேவை வழங்குநரிடமோ நீங்கள் முறைப்பாடொன்றினைப் பதிவு செய்து கொள்ளலாம். இதன் மூலமாக உங்களது தொலைந்த அல்லது திருடப்பட்ட தொலைபேசியின் பாவனையை உடனடியாக நிறுத்தி வைக்கவும் முடியும். இதன் பிற்பாடு வேறொரு சிம் அட்டையைக் கொண்டு உங்களது கையடக்க தொலைபேசியை பயன்படுத்த முயன்றாலும் அவற்றை இயங்கச் செய்ய முடியாமல் போகும்[1].

எனவே உங்களது தொலைபேசியின் IMEI இலக்கத்தை தெரிந்து கொள்வதுடன் அவற்றை சரியான பாதுகாப்பானதொரு இடத்தில் குறித்தும் வைத்துக் கொள்ளுங்கள்.



[1] Google has some useful advice on creating a strong password and a more secure account: https://support.google.com/accounts/answer/32040?hl=en

கீழே உங்களது கையடக்க தொலைபேசியின் பாதுகாப்பை உறுதிப்படுத்திக் கொள்வதற்கான சில பயன்தரும் குறிப்புகள் வழங்கப்பட்டுள்ளன.

- உங்களது கையடக்க தொலைபேசியைப் பாதுகாத்துக் கொள்வதற்கான தனி ரகசிய இலக்கமொன்றினை வழங்கிக் கொள்ளுங்கள். குறைந்தது 06 இலக்கங்களைக் கொண்டதொரு தனி அடையாளக் குறிப்பை வழங்குங்கள்.
- மிகவும் அண்மையில் வெளியிடப்பட்ட செயலியை தரவிறக்கம் செய்வதோடு அதனை உங்களது கையடக்க தொலைபேசியில் செயற்படுத்திக் கொள்ளுங்கள்.
- உங்களது கையடக்க தொலைபேசிக்கான வைரஸ் பாதுகாப்பு செயலியை அல்லது வேறு ஏதும் தீங்கு விளைவிக்கக்கூடிய விடயங்களிலிருந்து பாதுகாக்கக்கூடிய செயலிகளை தரவிறக்கம் செய்து செயற்படுத்திக் கொள்ளுங்கள்.
- நம்பத் தகுந்த தளங்களிலுள்ள செயலிகளை மட்டுமே தரவிறக்கம் செய்து கொள்ளுங்கள் உதாரணமாக (Google play store அல்லது Apple app store)
- உங்களது செயலிகளுக்கான தடைகளை உயர்த்திக் கொள்ளுங்கள். Android மற்றும IOS இயங்கு தளங்களில் எந்த வகையான செயலிகளை அனுமதிக்கலாம் அல்லது அனுமதிக்க முடியாது என்பதை உங்களுக்கு ஏற்ற வகையில் உயர்த்தி அல்லது தளர்த்திக் கொள்ளுங்கள். நீங்கள் இதற்கான அனுமதிகளை உயர்த்திக் கொள்வது மிகவும் ஆரோக்கியமானது, இதனால இந்த செயலிகள் உங்களது தனிப்பட்ட விடயங்களுக்கு உள்ளே செல்வது தடுக்கப்படும். Mypermissions.Com எனும் இலவச இணையதளமானது இவை பற்றிய ஆரோக்கியமான பல விடயங்களை உங்களுக்கு வழங்குகிறது. அது மட்டுமல்லாமல் இந்த தளமானது தொலைபேசிக்கே ஏற்ற பல செயற்பாடுகளைக் கொண்டதொரு செயலி என்பதோடு உங்களது கையடக்க தொலைபேசிக்குள் இயங்க விடப்பட்ட ஏதாவது செயலிகளை நிறுத்தவோ அல்லது அகற்றவோ வேண்டுமாயின் மிக இலகுவான முறையில் ஒரு முறை அழுத்துவதன் மூலம் இவற்றை செயற்படுத்திக் கொள்ளலாம்.
- வேறு இடத்திலிருந்து இயக்கக்கூடிய செயலியை செயற்படுத்திக் கொள்ளுங்கள்: இது உங்களது கைத்ததொலைபேசி தொலைந்தோ அல்லது திருடப்பட்டாலோ அது இருக்கும் இடத்தை கண்டுபிடிப்பதற்கு உதவும் ஒரு செயற்பாடாகும். அதே போன்று இந்த செயலியானது உங்களது தொலைபேசியிலுள்ள செயலிகளை வேறொரு இடத்திலிருந்து அதில் காணப்படும் இரகசிய விடயங்களை பெற்றுக்கொள்ளவும் உதவும்.
- நீங்கள் பாவிக்காத வேளையில Bluetooth இனை செயலிழக்கச் செய்யவும்: உங்களது Bluetooth இயங்கும் நிலையில் காணப்படும் போது உங்களது கையடக்க தொலைபேசி வலுவிழந்ததாகவே காணப்படும். ஆகவே பிற சாதனங்களின் தாக்கத்திலிருந்து உங்களது கையடக்க தொலைபேசியினை பாதுகாக்க வேண்டியேற்படின் Bluetooth செயலிழந்த நிலையில் இருப்பது மிக முக்கியமானதாகும். சில வேளைகளில் நீங்கள் மற்றவர்களால் காண முடியாத நிலையில் இதனை செயற்படுத்தியிருந்தாலும் இவற்றால் ஏற்படக்கூடிய தாக்கங்கள் மிகவும் அதிகமானவை.

டிஜிட்டல் அடையாள திருட்டு

ஒன்லைன் மற்றும் ஒன்லைன் அற்ற இரு முறைகளிலும் டிஜிட்டல் அடையாளத் திருட்டுக்கள் இடம்பெறலாம். அதாவது வேறு நபர்களால் உங்களது தனிப்பட்ட மற்றும் இரகசியமான விடயங்களை உங்களது கணக்குகள் அல்லது சாதனங்களுக்குள் உங்களது அனுமதியில்லாமல் உள் நுழைந்து திருடுவது ஆகும். உங்களது மிகவும் பெறுமதியான விடயங்களான வங்கிக் கணக்கு இலக்கங்கள், மின்னஞ்சல்கள், கடனட்டை இலக்கங்கள் போன்றனவற்றை திருடுவது தற்காலத்தில் அதிகமாக அவதானிக்கக் கூடியதாகவுள்ளது. இவ்வாறு இடம்பெறுமிடத்து இதனால் பல பாரதூரமான நிலைமைகள் ஏற்படலாம்.
தனியொருவரின் தனிப்பட்ட டிஜிட்டல் அடையாளங்கள் பல முறைகளில் திருடப்படலாம். ஒன்லைன் முறைகளை உபயோகிக்கும் போது இத்திருட்டு சம்பவங்கள் மிக அதிகமாக இடம்பெறுகிறது. மேலும் திருடர்களுக்கு நீங்கள் ஒன்லைன் மூலம் இருப்பது மிகவும் இலகுவாக அவர்களது திருட்டினை மேற்கொள்ள உதவுகிறது.

அடையாள திருட்டுக்களை டிஜிட்டல் முறையின்படி பின்வரும் வகைகளில் உள்ளடக்கலாம் .

- கைவிடப்பட்ட சாதனங்களான கணனி, கையடக்க தொலைபேசி மற்றும் USB போன்றவற்றிலிருக்கும் அனைத்து தகவல்களையும் வேறொரு சாதனத்துக்குள் மாற்றிக் கொள்ளல்
- Keystroke logging or spyware போன்ற செயலிகளைப் பயன்படுத்தி உங்களது தனிப்பட்ட விடயங்களை திருடிக் கொள்ளல்.
- உங்களது கணனி போன்ற சாதனங்களிலுள்ள மிகவும் பெறுமதியான கோப்புகள் மற்றும் ஏனைய விடயங்களை கடத்தல்.
- மின்னஞ்சல் மற்றும் குறுந்தகவல் போன்றவற்றினூடாக மக்களை ஏமாற்றும் செய்திகளை அனுப்பி அவர்களின் பெறுமதியான விடயங்களைப் பெற்றுக் கொள்ளல்.
- உங்களது பலமிழந்த கடவுச்சொல்லினை ஊகித்துக் கொண்டு அவற்றை உட்செலுத்தி உங்களது கணக்குகளுக்குள் நுழைந்து தனிப்பட்ட விடயங்களை பெற்றுக் கொள்ளல்.
- சமூக வலைத்தளங்கள் போன்ற செயலிகளை உருவாக்கி அவற்றுக்குள் உங்களை உள் நுழைய வைத்து நீங்கள் வழங்கும் மின்னஞ்சல் முகவரியினூடாக தாங்கள் ஊகிக்கும் கடவுச் சொல்லொன்றைக் கொண்டு உங்களது கணக்கிற்குள் நுழைதல்.
- உங்களது செயலிழந்த கணக்கொன்றை வேறொரு கணக்கிற்குள் மாற்றுவதைப் போல் உருவாக்கி அவற்றிற்கு நீங்கள் வழங்கும் விடயங்களைக் கொண்டு உங்களது தனிப்பட்ட விடயங்களை திருடுதல்.

இவ்வாறான அடையாள திருட்டுக்களின் பாதிப்பை நாம் முற்று முழுதாக ஒழித்து விட முடியாது. ஆனால் இவற்றிலிருந்து எம்மைக் காத்துக் கொள்ள எம்மையும் எம்மைச் சுற்றியுள்ளவர்களையும் அவை பற்றி விழிப்படைய செய்ய வேண்டும். அவை பற்றி கீழே சில ஆலோசனைகள் வழங்கப்பட்டுள்ளன .

- நீங்கள் வங்கிக் கணக்குகள் போன்ற பாதுகாப்பானதொரு இணையதளத்தினுள் நுழைந்திருந்தாலும் எப்பொழுதாவது வேறொரு நடுத்தர இணையதள பகுதிக்கு மாற்றப்பட்டால் அவை பற்றி விழிப்பாக இருங்கள். இணையதள பகுதிகளை (URL) அடிக்கடி பரீசீலனை செய்து கொள்ளுங்கள்.
- நீங்கள் சந்தேகத்துக்கிடமான ஏதாவதொன்றுக்காக இணையதள முறையிலான பணக்கொடுக்கல்வாங்கல்களுக்கு உங்களது கடனட்டையை பயன்படுத்தியிருப்பின் அவற்றை தொடர்ந்து அவதானித்துக் கொண்டே இருங்கள்.
- நம்பத் தகுந்த பகுதிகளில் மாத்திரமே பணக்கொடுக்கல்வாங்கல்களை மேற்கொள்ளவும். நீங்கள் ஏதாவது கட்டணங்களை இணையதளத்தின் மூலம் மேற்கொண்டிருப்பின் அப்பகுதியின் மேல் பகுதியில் (வலது பக்க) பூட்டு போன்றதொரு உருவம் தோன்ற வேண்டும். அப்படியானதொரு உருவம் தோன்றாவிடத்து உங்களது அட்டைகளது இலக்கங்களை உட்செலுத்த வேண்டாம்.
- மிகப்பிரபல்யமான நிறுவனங்களாக பல்கலைக்கழகங்கள், வங்கிகள் போன்ற நிறுவனங்களிலிருந்து அனுப்பப்படும் மின்னஞ்சல்களுக்கு ஒத்ததானவற்றில் ஏதாவது இணைப்புகளுடன் காட்சிப்படுத்தி உங்களது தனிப்பட்ட விடயங்களை வழங்கக் கேட்டால் அவைகளிலிருந்து தவிர்த்து கொள்ளவும். இதற்கு மாற்றாக அக்குறிப்பிட்ட நிதி நிறுவனத்துக்கோ அல்லது பல்கலைக்கழகத்துக்கோ அழைப்பொன்றினை மேற்கொண்டு அவை பற்றிய மேலதிக விடயங்களை கேட்டுத் தெரிந்து கொள்ளுங்கள்.
- உங்களது பொதுவான புரிந்து கொள்ளும் தன்மைக்கேற்றவாறு நடந்து கொள்ளுங்கள். ஏதாவது ஒரு வழங்கல்கள் மிகவும் உண்மையான நம்பத்தகுந்தவொன்றாக காணப்படுமிடத்து (உதாரணமாக பாரிஸுக்கு சுற்றுப்பயணமொன்றை இலவசமாக பெற்றுக்கொள்ள உங்களது கடனட்டை இலக்கத்தை வழங்கவும் போன்ற) அவற்றை கவனத்தில் எடுக்காதீர்கள்.
- பொதுவான Wi-Fi இனை உபயோகிக்குமிடத்து உங்களது வங்கிக் கணக்கு அல்லது கடனட்டை விடயங்களை வழங்காதீர்கள்.
- சில கணனிசார் நிறுவனங்களை போன்றதொரு நிறுவனங்களிலிருந்து வரும் மின்னஞ்சல்கள் பற்றி கவனமாக இருக்கவும் (உதாரணமாக Norton Anti-Virus இது அவற்றை பதிவிறக்கம் செய்யும்படி உங்களைக் கேட்டு நிற்கும்). இவை பற்றி இந்நிறுவனங்களிலிருந்து அறிந்து கொள்ளுங்கள், மாறாக மின்னஞ்சலில் எந்த பதிலும் அனுப்ப வேண்டாம்.

[2] More information at: https://www.imei.info/
[3] Source: https://www.techopedia.com/definition/13637/identity-theft

சம்பவக் கற்கைகள்

சம்பவக் கற்கைகள் 1: DATA DETOX KIT

ஆரோக்கியமான தொழில்நுட்ப அம்சங்களில் உங்களுடைய தரவுகள் செல்லும் பாதையை குறைக்க வேண்டுமாயின் அதை எங்கிருந்து ஆரம்பிப்பது என்று முடிவெடுப்பது மிக கடினமான ஒரு விடயம் ஆகும். எங்களுடைய சாதனங்கள் நமது தனிப்பட்ட வாழ்க்கையுடன் பின்னிப்பிணைந்து காணப்படுவதனால் இதுவே அவற்றில் சமநிலையை உருவாக்க உதவுகிறது.

Data Detox Kit எனப்படுவது நாம் அனைவரினாலும் அணுகக்கூடிய மிக எளிய ஒரு கருவியாகும். இது ஆரோக்கியமான இணையத்தை விரும்பி நீங்கள் எடுக்கக்கூடிய ஒவ்வொரு அடியின் மூலமும் உங்களை அந்த இடத்துக்கு எடுத்து செல்கிறது. இது உங்கள் டிஜிட்டல் வாழ்க்கையின் வெவ்வேறு வகையான அம்சங்களைக் கொண்டு உங்களது தொலைபேசியில் நீங்கள் செலவிடும் நேரத்தைக் கொண்டும், நீங்கள் பயன்படுத்தும் சேவைகளைக் கொண்டும், நீங்கள் வழங்கிய கடவுச் சீட்டைக் கொண்டும் ஒரு முழுமையான அணுகுமுறை ஒன்றை உருவாக்கும்.

இந்த Data Detox Kit ஆனது Tactical Tech எனும் சர்வதேச இலாப நோக்கற்ற நிறுவனம் ஒன்றினால் உருவாக்கப்பட்டது. இந்நிறுவனமானது சிவில் சமூகம் மற்றும் சாதாரண பிரஜைகளுக்கு தொழில்நுட்பத்தினால ஏற்படுத்தும் தாக்கங்கள் பற்றிய விடயங்களில் தனது வேலைகளை முன்னகர்த்திக் கொண்டு செல்கிறது.

இதன் பதிப்புக்கள் டச்சு, பிரெஞ்சு, ஜேர்மன், இந்தோனேசியன், நோர்வே, போலாந்து, போர்த்துக்கீஸ், ஸ்பானிஸ் மற்றும் சுவீடன் மொழிகளிலும் பிரசுரிக்கப்பட்டிருக்கின்றன. datadetox@tacticaltech.org எனும் மின்னஞ்சல் முகரியினூடாக நீங்கள் விரும்பிய மொழியில் PDF வகையான பிரதியொன்றைக் கேட்டு விண்ணப்பிக்கலாம் என்பதோடு மட்டுமல்லாமல் இவற்றை நீங்கள் எங்கே என்ன விடயத்துக்கு பாவிக்கப் போகிறீர்கள் என்ற விடயத்தையும் குறிப்பிட்டாக வேண்டும்.

[4] Source: http://www.digitalresponsibility.org/how-to-avoid-online-identity-theft

சம்பவக் கற்கை 2: டிஜிட்டல் முதலுதவிப் பெட்டி

டிஜிட்டல் முதலுதவிப் பெட்டி என்ற விடயம் வெளியில் வருவதற்குக் காரணம் யாதெனில் இத்துறையில் ஒரு போதுமில்லாத அளவிற்கு அதிக எண்ணிக்கையானவர்கள் தற்காலத்தில் ஈடுபடுகின்றனர், எனவே யாராவது ஒருவருக்கு டிஜிட்டல் துறையில் பாதிப்புகள் ஏற்பட்டு அவர்களுக்கு உதவிகள் தேவைப்படுமிடத்து உரிய வேளையில் உதவியை வழங்க வேண்டும் என்பதற்காகவே இது அறிமுகம் செய்யப்பட்டது. இவ்வாறான நிலையில் அந்த பாதிக்கப்பட்ட நபர் என்ன செய்வது? எங்கே செல்வது என்பது பற்றித் தெளிவில்லாமல் காணப்படுவார், எனவே அவ்வேளையில் இது மிகவும் உறுதுணையாக அமையும். இந்த நடைமுறையை உருவாக்குவதற்கான பின்னணியாக அமைந்தது யாதெனில் எந்த ஒருவருக்கும் அவசர நிலையொன்றிலிருந்து தம்மைப் பாதுகாத்துக் கொள்வதறதகான தேவை உள்ளது என்பதோடு மட்டுமல்லாமல் அவர்களுக்கு ஏதாவது அவசர தேவைகள் ஏற்படுமிடத்து அத்தேவைகளை பூர்த்தி செய்து கொள்ள சேவைகளையும் பெற்றுக் கொள்ள வாய்ப்பு வசதி காணப்பட வேண்டும் என்பதாகும்.

இந்த டிஜிட்டல் முதலுதவிப் பெட்டியானது யாராவது இத்துறையிலுள்ள ஒருவருக்கு ஏற்படக்கூடிய பொதுவான பிரச்சினைகளுக்கு முதற்கண்ணாக வழங்கக் கூடிய அல்லது அந்நிலையைத் தடுக்கக்கூடிய வசதிகளை ஏற்படுத்த வேண்டும் என்பது ஆகும். இவ்வுதவிப் பெட்டியானது மனித உரிமை செயற்பாட்டாளர்கள், சமூக செயற்பாட்டாளர்கள், ஊடகவியலாளர்கள், போன்றோர்களுக்கு தாம் சுயமாக தங்களுக்கு ஆபத்து விளைவிக்கக்கூடிய விடயங்களைப் பற்றி கண்டறிந்து கொள்வதற்காகவே உருவாக்கப்பட்டுள்ளதாகும். அது மாத்திரமல்லாமல் எவராவது ஒருவர் பாதிக்கப்பட்டிருப்பின் அவருக்கு உடனடியாக வழங்கப்பட வேண்டிய சேவைகளும் இதில் உள்ளடக்கபட்டுள்ளது.

இந்தத் தொகுதியானது எவ்வாறு பாதுகாப்பான தொடர்பாடலை மேற்கொள்வது என்ற விடயத்தில் ஆரம்பித்து அவற்றுக்கான உதவிகளை பெற்றுக்கொள்வது பற்றியும் குறிப்பிடுகிறது. அதன் பின்னர் இது கணக்குகளை கடத்தல், சாதனங்களை பறிமுதல் செய்தல், ஆபத்தை விளைவிக்கும் விடயங்களிலிருந்து எவ்வாறு பாதுகாப்பு பெறுவது என்பது பற்றியும் குறிப்பிடுகிறது.

இக்கேள்விகள் சுய மதிப்பீடொன்றை மேற்கொள்வதன் மூலம் உங்களை வழிப்படுத்தும் அல்லது நீங்கள் எதிர்கொள்ளும் சவால்களைப் பற்றி முதலில் பதிலளிக்க இருப்பவர்களுக்கு தெரியப்படுத்தும். இது சிக்கல்களை புரிந்து கொள்வதறகான ஆரம்ப நடவடிக்கைளாக அமைகிறது. இதில் பயன்படுத்தப்படும் நடைமுறைகள் ஒரு நிபுணரிடம் எவ்வாறு உதவிகளைப் பெற்றுக் கொள்வது என்பது பற்றியும் குறிப்பிடுகிறது.

இந்த முதலுதவியில் காணப்படும் விடயங்கள் ஒரு சிக்கலான நிலையொன்றின் போது நிலைமைகளை அறிந்து தெரிந்து கொள்வதற்கான ஆரம்பகட்ட உதவிகளை உங்களுக்கு வழங்குகிறது. இதன் மூலம் நீங்கள் ஆரம்பத்திலேயே விடயங்களை அறிந்து அதற்கேற்ற செயற்பாடுகளை மேற்கொள்ள முடியும். இதிலுள்ள ஏதாவதொரு வியடங்களுக்கு எவ்வாறு அவற்றை வெற்றி கொள்வது என்பது பற்றி உங்களுக்கு தெளிவுகள் காணப்படவில்லையாயின் உடனேயே அதில் பாண்டித்தியம் பெற்ற ஒருவரிடம் உதவியைப் பெற்றுக் கொள்ளுங்கள் அல்லது இவற்றை உருவாக்கியவர்களிடம் தெரியப்படுத்துங்கள்.

இவ்வாறு சுயமாகவே விடயங்களை கண்டறியக்கூடிய இந்த செயலிகள் ஊடகவியலாளர்கள், பிளொக் எழுதுபவர்கள், சமூக செயற்பாட்டாளர்கள் மற்றும் மனித உரிமைகள் செயற்பாட்டாளர்கள் போன்ற அனைத்து சாரார்களுக்கும் டிஜிட்டல் உலகில் இடம்பெறும் விடயங்கள் பற்றிய தெளிவையும் விளக்கங்களையும் கொடுப்பதாக அமைய வேண்டும். இதன் மூலமே டிஜிட்டல் உலகில் காணப்படும் ஆபத்து விளைவிக்கக்கூடிய விடயங்களிலிருந்து தங்களைப் பாதுகாத்து ஆபத்தற்ற ஒரு சூழலை நாம் எல்லோருக்காகவும் உருவாக்கிக் கொள்ள முடியும்.

More: https://www.digitaldefenders.org/digitalfirstaid/

கலந்துரையாடல் விடயங்கள்

இவ்விடயங்கள் பற்றிய மேலதிக விடயங்களை அறிந்து கொள்ளும் பொருட்டு கீழ்வரும் கலந்துரையாடல் விடயங்களை அவதானித்துக் கொள்ளுங்கள்.

- டிஜிட்டல் பாதுகாப்பு மற்றும் கணனி பாதுகாப்பு என்பது பாவனையாளர், பயனாளர்கள் மற்றும் தொழில்நுட்ப சேவை என்பவற்றுக்கிடையிலான பகிரப்பட்ட பொறுப்புணர்ச்சி ஆகும். நீங்கள் இதனை ஏற்றுக் கொள்கிறீர்களா? கலந்துரையாடவும்.
- நீங்கள் எப்போதாவது கணனி வைரஸ் அல்லது கணனிகளுக்கு பாதுகாப்பு விளைவிக்கக்கூடிய ஏதாவதொன்றின் மூலம் பாதிக்கப்பட்ட சம்பவங்கள் இடம்பெற்றுள்ளனவா? அவ்வாறான நிலையை வெற்றி கொள்ள எவ்வகையான உத்திகளை நீங்கள் அல்லது உங்களது நிறுவனம் மேற்கொண்டுள்ளது?
- உங்கள் டிஜிட்டல் சேவைகளில் ஏதேனும் குறியாக்கத்தை மேற்கொண்டுள்ளீர்களா? அப்படியாயின் உங்களது அநுபவத்தைப் பகிர்ந்து கொள்ளுங்கள்?
- தரவு அல்லது தனியுரிமை மீறப்பட்டால் உங்களால் என்ன வகையான விடயங்களை மேற்கொள்ள முடியும்? உங்களுக்கோ அல்லது உங்கள் நிறுவனத்துக்கோ ஏதாவது ஆபத்திலிருந்து பாதுகாத்துக்கொள்ளக்கூடிய திட்டங்கள் காணப்படுகிறதா?
- டிஜிட்டல் அடையாள திருட்டுக்கள் பற்றிய ஏதேனும் நிகழ்வுகள் உங்களுக்கு இடம்பெற்றிருக்கிறதா? அது எவ்வாறு இடம்பெற்றுள்ளது? அதை மீட்டுக்கொள்ளல் எந்த வகையில் சாத்தியமானது?
- நீங்கள் வீட்டிலிருந்தோ அல்லது அலுவலகத்திலிருந்தோ வேறு இடங்களுக்கு சென்று பொது wi fi களைப் பயன்படுத்துபவரா? அப்படியாயின் எந்த வகையான முன்னாயத்தங்களை நீங்கள் மேற்கொண்டீர்கள்?

கற்றல் பலன்கள்

இந்தப்பாடத்திட்டத்தின் இறுதியில் நீங்கள் பின்வரும் விடயங்கள் பற்றிய தெளிவினைப் பெறுவீர்கள்

- இணைய பாதுகாப்பு எனப்படுவது விடயங்கள் மற்றும் முறைமைகளை உள்ளடக்கியது. இணைய முன்பாதுகாப்பு எனப்படுவது மக்களைப் பற்றியது.
- டிஜிட்டல் பாதுகாப்பு மற்றும் இணையப் பாதுகாப்பு ஆகிய இரண்டும் பாவனையாளர்கள், சேவை வழங்குநர்கள் மற்றும் தொழில்நுட்ப சேவை ஆகியவற்றுக்கிடையிலான தொடர்புபட்ட எல்லோராலும் மேற்கொள்ள வேண்டிய கூட்டுப் பங்காண்மை ஆகும். நல்லதொரு டிஜிட்டல் பாதுகாப்பு மற்றும் இணையப் பாதுகாப்பு என்பவற்றுக்கு பாவனையாளர்களின் பங்குபற்றல், கடப்பாடு மற்றும் அவதானம் ஆகியவை மிக முக்கியமானது ஆகும்.
- உறுதியான கடவுச்சொல், இரு வழி அங்கீகாரம், தரவு மறைகுறியாக்கல் மற்றும் காலத்துக்கு காலமான தரவு மீளப் பெறல் போன்றன ஒவ்வொரு டிஜிட்டல் பாவனையாளர்களும் கட்டாயம் மேற்கொள்ள வேண்டிய ஆரோக்கியமான நடைமுறை ஆகும். மேலும் இது நல்லதொரு ஆரோக்கியமான டிஜிட்டல் முறை என்றும் அழைக்கப்படும்.
- டிஜிட்டல் பாதுகாப்பு மற்றம் கணனி பாதுகாப்பு பற்றிய அதிகளவான இலவச ஆலோசனைகளும் அறிவுறுத்தல்களும் இணையதளங்களில் பெற்றுக் கொள்ளலாம். எவ்வாறாயினும் இதிலுள்ள முக்கிய விடயம் யாதெனில் நீங்கள் - அதாவது பாவனையாளர்கள்.

மேலதிக வாசிப்புகளுக்காக

ஆரோக்கியமான டிஜிட்டல் : இணைய வழியில் பாதுகாப்பாக இருப்பதற்கான வழி முறைகள்
Book by Ed Gelbstein (2013)
http://index-of.co.uk/IT-managment/good-digital-hygiene.pdf

Norton இணைய பாதுகாப்பு அறிவுறுத்தல்கள்
https://us.norton.com/internetsecurity

கூகுள் பாதுகாப்பு நிலையம் (கூகுள் கணக்கு வைத்திருப்பவர்களுக்கு மட்டுமே)
https://support.google.com/

உள் பெட்டிக்குள் பாதுகாப்பு, சமூக செயற்பாட்டாளர்களுக்கும் மனித உரிமைகள் பாதுகாப்பாளர்களுக்குமான வழிகாட்டி
https://www.frontlinedefenders.org/en/digital-security-resources

உங்களது அண்ட்ரொய்ட் தொலைபேசியில் காணப்படும் டிஜிட்டல் ஆபத்துக்கள் இருப்பின் அதற்கான குடை
https://secfirst.org/

ஊடகவியலாளர்களுக்கான தகவல் பாதுகாப்பு கைநூல்
http://www.tcij.org/resources/handbooks/infosec

Electronic Frontier குழரனெயவழைெ'ள இனது கண்காணிப்புத் தற்காப்பு
https://ssd.eff.org/en

நல்லதொரு டிஜிட்டல் சுகாதாரம் பற்றிய உதவிக் குறிப்புக்கள்
https://wiobyrne.com/digital-hygiene/

Electronic Intifada இனது ஆர்வலர்களுக்கான டிஜிட்டல் பாதுகாப்பு
https://electronicintifada.net/content/guide-online-security-activists/17536