வீட்டிலிருந்து வேலை செய்வதற்கான தகவல் பாதுகாப்பு வழிகாட்டுதல்கள்

ජනාධිපති කාර්යාලය
சனாதிபதி அலுவலகம்
Presidential Secretariat

SRI LANKA CERT|CC

வீட்டிலிருந்து வேலை செய்வதற்கான மாற்றத்துடன், தகவல் பாதுகாப்பு தொடர்பான அச்சுறுத்தல்களும் அதிகரித்துள்ளன. வீட்டிலிருந்து பாதுகாப்பாக வேலை செய்வதற்கு பின்வரும் செய்ய வேண்டிய மற்றும் செய்ய தகாதவைகளை தயவு செய்து எந்நேரமும் பின்பற்றவும்.

Issued: 10th November, 2020

கோப்புகள்(files) மற்றும் தகவல்கள்

- இரகசிய தன்மை வாய்ந்த ஆவணங்களை அழிக்கும் போது அங்கீகரிக்கப்படாத நபர்கள் மூலம் கையாளப்படாதவாறு துண்டாக்கல்(shredding) அல்லது அவற்றை சிறிய துண்டுகளாக கிழித்தல் முறைகளை பயன்படுத்தவும்.
- அலுவலக ஆவணங்களை பயன்படுத்தாதவிடத்து கடவுச்சொல் இட்டு பூட்டி வைக்கவும்.
- முக்கியமான கோப்புகளை தொடர்ந்து காப்பு பிரதியிடல்(backup) மூலம் பாதுகாப்பான முறையில் சேமிக்கவும்.
- அனைத்து அலுவலக தரவுகள், தகவல்கள் மற்றும் கோப்புகளை அலுவலக நோக்கத்திற்காக மட்டும் பயன்படுத்தவும்.
- பிறர் தன் கடமையை நிறைவேற்ற அவசியமான தரவுகள், தகவல்கள் மற்றும் கோப்புக்களை "தெரிந்து கொள்ள வேண்டும்" என்ற அடிப்படையில் மாத்திரமே பகிரவும்.
- பொதுவலைத்தளங்களில் மற்றும் சேமிப்பு தளங்களில் அலுவலகத்திற்கு உரித்தான தனித்துவமான தகவல்களை பகிர்தல் மற்றும் பதிவேற்றம் செய்வதனை தவிர்க்கவும்.

மின்னஞ்சல்கள், குறுந்தகவல்கள் மற்றும் வலைத்தள உலாவல்.

- இனம் தெரியாத அனுப்புனரிடம் இருந்து வரும் குறுந்தகவல்களிலோ மின்னஞ்சல்களிலோ உள்ள இணைப்புகளை அல்லது தொடுப்புக்களை அழுத்துவதனை மற்றும் பதிவிறக்கம் செய்வதனை தவிர்க்கவும்.
- சட்டவிரோதமான மூன்றாம் தரப்பின் அங்கீகரிக்கப்படாத மென்பொருள்கள், பயன்பாட்டு மென்பொருள்கள் மற்றும் கணினி விளையாட்டுக்களை பதிவிறக்கம் செய்வதை தவிர்க்கவும்.
- பாதுகாப்பற்ற வலைத்தளங்களில் உலாவுவதை தவிர்க்கவும். (உ-ம்: கணினி விளையாட்டுக்கள், கிசுகிசுப்பு இணையத்தளங்கள், சூதாட்ட தளங்கள், ஆபாச இணைய-தளங்கள்)
- உமக்கு அலுவலக உபயோகத்திற்காக தனிப்பட்ட மின்னஞ்சல் முகவரி வழங்கப்பட்டிருப்பின், அதை அலுவலக உபயோகத்திற்கு மாத்திரம் பயன்படுத்தவும்.
- கொரோனா அல்லது இலவச தரவுகள் தொடர்பான மின்னஞ்சல்களை பெறுமிடத்து அதிகவனம் செலுத்தவும். அவை பிஷ்ஷிங்(phishing) அல்லது சூழ்ச்சி(scam) தாக்குதல்களாக இருக்கலாம்.

கணினிகள், கையடக்க தொலைபேசிகள் அல்லது மடிக்கணினிகள்(tabs)

- உங்களது கணினியில் ஒரு தரமான நன்கு அறியப்பட்ட வழங்குநரிடமிருந்து உரிமம் பெற்ற / சட்டபூர்வமான நச்சுநிரல் எதிர்ப்பானை(antivirus) நிறுவப்பட்டு அதனை எப்போதும் புதுப்பித்து வைத்தல் வேண்டும்.
- எப்பொழுதும் தெரியாத வெளிக்கருவிகளை(pendrive) பயன்படுத்துவதை தவிர்க்கவும். ஒரு வேளை பயன்படுத்தவேண்டி ஏற்படின் அதனை உங்கள் கணினியில் உரிமம் பெற்ற / சட்டபூர்வமான நச்சு நிரல் எதிர்பானின்(antivirus) ஊடாக பரிசோதித்து பயன்படுத்தவும்.
- இலத்திரனியல் சாதனங்களை பயன்படுத்தாத சந்தர்ப்பங்களில் கடவுச்சொல் இட்டு தாழிடவும்(lock) மற்றும் கணினிகளை பயன்படுத்தாவிடத்து நிறுத்திவைக்கவும். உமக்கு அரசாங்கத்தால் வழங்கப்பட்ட கருவிகளை பாதுகாப்பது உங்களது பொறுப்பாகும்.
- உமது அலுவலக தகவல்களை மறையாக்க(encrypt) முறையில் பதிவு செய்து அதனை வன்தட்டில்(harddrive) சேமிப்பதன் ஊடாக குறித்த சாதனமானது தொலைந்துவிட்டால் அல்லது திருடப்பட்டால், முக்கியமான ரகசிய தகவல்கள் வெளிதரப்பினருக்கு வெளிப்படுத்தப்படாது என்பதனை இதன் மூலம் உறுதி செய்யலாம்.
- அலுவலக தகவல்களை உள்ளடக்கிய ஏதேனும் இலத்திரனியல் கருவிகள் தொலையுமிடத்து உடனடியாக உரிய அதிகாரிகளுக்கு அறிவிக்கவும்.
- சமீபத்திய திட்டுகளால் (latest patches) எப்போதும் புதுப்பித்த நிலையில் (updates) உள்ள மென்பொருள்களை பயன்படுத்தவும். உ-ம்: இயக்க முறைமை(Operating System), வைரஸ் தடுப்பு(antivirus), உலாவிகள்(browsers), துணை நிரல்கள்(add-ons) போன்றவை.
- அலுவலக வேலைகளுக்காக பொது இணைய இணைப்புகளை பயன்படுத்துவதை தவிர்க்கவும்.
- அன்றாட கணினி வேலைகளுக்கு நிர்வாக உரிமை அற்ற பயனர் கணக்குகளை பயன்படுத்தவும்.
- உங்களுக்கு மெய்நிகர் தனியார் பிணையம் (VPN) போன்ற அதிகாரப்பூர்வ பாதுகாப்பான இணைப்பு வசதி வழங்கப்பட்டிருந்தால், அதனை மட்டுமே பணி அமைப்பு-களுடன் இணைவதற்கு பயன்படுத்தவும்.

கடவுச்சொற்கள் மற்றும் இணைய ஆதாரச்சான்றுகள்(credentials)

- உங்கள் எல்லா கருவிகளுக்கும் / பயன்பாடுகளுக்கும் கடவுச்சொற்களை பயன்படுத்தவும். கருவிகளை பயன்படுத்தாத போது கடவுச்சொல் இட்டு பூட்டி வைக்கவும்.
- நினைவில் கொள்ளத்தக்க மற்றும் இலகுவில் யூகிக்க முடியாத கடவுச்சொற்களை செயல்படுத்தவும மேலும் எளிய கடவுச்சொற்களைப் பயன்படுத்துவதைத் தவிர்க்கவும்.
- கூடுதல் பாதுகாப்பிற்காக இயலுமானவரை இருகாரணி உறுதிபடுத்தல் முறைமையை(two factor authentication) செயற்படுத்தவும்.
- காகிதங்கள் மற்றும் குறிப்புப்புத்தகங்களில் கடவுச்சொற்களை எழுதி வைப்பதை தவிர்க்கவும்.
- கடவுச்சொற்களை அடிக்கடி மாற்றவும்.
- கடவுச்சொற்களை மீள்பயன்படுத்தலை தவிர்க்கவும் மற்றும் ஒரே கடவுச்சொல்லை வெவ்வேறு பயனர் கணக்குகளுக்கு பயன்படுத்துவதை தவிர்க்கவும்.
- கடவுச்சொற்களை மற்றவர்களுடன் பகிர்வதை முற்றிலும் தவிர்க்கவும். உங்கள் இணைய ஆதாரச்சான்றுகளை(credentials) பயன்படுத்தி செய்யப்படும் பரிமா-ற்றங்களுக்கு நீங்கள் மட்டுமே பொறுப்பாவீர்கள்.
- உங்கள் தனிப்பட்ட தகவல்களை மின்னஞ்சல், இணையத்தளங்கள், சமூக ஊடகத்தளங்கள் மற்றும் தொலைபேசி அழைப்புகள் மூலம் பகிர்வதை தவிர்க்கவும்.
- உறுதியான கடவுச்சொல்லை பயன்படுத்தி உங்கள் Wi-Fi இணைப்புக்களை பாதுகாக்கவும்.

புகாரளித்தல் மற்றும் உதவி

- உங்கள் நிறுவனத்தின் தகவல் பாதுகாப்பு கொள்கைகளை படித்து, புரிந்துகொண்டு கண்டிப்பாக அவற்றை பின்பற்றவும். சந்தேகம் இருந்தால் உங்கள் மேற்பார்வையாளர் அல்லது துறை சார் மேலதிகாரியை அணுகவும்.
- உங்கள் இலத்திரனியல் சாதனத்தில் சந்தேகத்திற்கிடமான ஏதேனும் இடம்பெறின் உடனே தகவல் தொழிநுட்ப பிரிவிற்கு / அத்துறைசார் மேல் அதிகாரிக்கு தெரியப்படுத்தவும்.
- ஏதேனும் பாதுகாப்பு தொடர்பான பிரச்சினைகளை உடனடியாக உங்கள் மேல் அதிகாரிக்கும் மற்றும் incidents@cert.gov.lk என்ற மின்னஞ்சல் முகவரிக்கும் தெரியப்படுத்தவும்.