ISSUE NO 04

NOVEMBER 2023

Cyber Guardian

A Publication on Online Safety

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Readiness Team
Coordination Centre

SECURITY

இணைய வழி பொருள் கொள்வனவுக்கு (online ஷெ ாப்பிங் செய்யும்) முன் இதைப் பற்றி யோசியுங்கள்

நமது நாட்டில் இன்று பெரும்பாலான இளம் சமூகத்தினர் மத்தியில் ழுடெநெ ஷெ ாப்பிங் முறையில் பொருட்களை கொள்வனவு செய்வது பிரபலயமடைந்துள்ளது. தற்போதைய பண்டிகைக்காலப்பகுதியில் பல்வேறு விலைக்கழிவு என்ற மூலோபாய செயற்பாடு அதிகரிப்பினால் சைபர் குற்றவாளிகள் பெரும்பாலும் ழுடெநெ ஷொப்பிங்கை ளுாழீபை இலக்காகக்கொண்டு பணம் அல்லது தகவல் திருட்டுகளும் அதிகரிக்கலாம்.

போலியான சில்லறை விற்பனையாளர் வலைத்தளங்களை அமைப்பது, இல்லாத பொருட்களை விற்பனை செய்தல், அவர்களுக்குத் தேவையற்ற தனிப்பட்ட கட்டணத் தகவல்களைக் கேட்பது மற்றும் தீங்கிழைக்கும் மென்பொருளை நிறுவுதல் (“Malawar”) உட்பட பல்வேறு முறைகள் மூலம் அவர்கள் இதனை மேற்கொள்ளுகின்றனர்.
இணைய வழி மூலம் பொருட்களை கொள்முதல் (ஆன்லைனில் ஷாப்பிங்) செய்யும்போது எச்சரிக்கையாகவும் பாதுகாப்பாகவும் செயல்படுவது முக்கியம். ஒரு சைபர் குற்றவாளி உங்கள் நிதி விவரங்களையும் பணத்தையும் பெற்றவுடன் உங்கள் பணத்தை நீங்கள் திரும்பப் பெற வாய்ப்பில்லை.

உங்கள் பொருட்கள் வராததால் நீங்கள் ஏமாற்றமடைவது மட்டுமல்லாமல், நீங்கள் பொருட்களுக்கு செலுத்திய பணத்தையும் இழக்க நேரிடும். ஆன்லைன் ஷெ ாப்பிங்கிற்கு தனிப்பட்ட சாதனங்களை Smartphones, Tablets, Computers and laptops (ஸ்மார்ட்போன்கள், டேப்லெட்டுகள், கணினிகள் மற்றும் மடிக்கணினிகள்) பயன்படுத்தும் போது சிந்திக்க வேண்டிய பல விடயங்கள் உள்ளன. உங்களின் இணைய வழி பொருள் கொள்வனவு (ஆன்லைன் ஷொப்பிங்) அனுபவம் பாதுகாப்பானதா என்பதை உறுதிசெய்ய, எங்கள் பாதுகாப்பு உதவிக்குறிப்புகளைப் பின்பற்றவும்.

பாதுகாப்பான சாதனங்களைப் பயன்படுத்தி பொருட்களை கொள்வனவு செய்யுங்கள். ஆன்லைன் ஷொப்பிங்கிற்காக நீங்கள் பயன்படுத்தும் சாதனங்களில் சமீபத்திய புதுப்பிப்புகள் நிறுவப்பட்டிருப்பதையும் நம்பகமான வலைப்பின்னலு (நெட்வொர்க்கு) டன் இணைக்கப்பட்டுள்ளதையும் உறுதிப்படுத்திக் கொள்ளுங்கள். உதாரணமாக, பொது வை.ஃபைக்குப் (Wi-Fi) பதிலாக உங்கள் வீட்டு Wi-Fi அல்லது (4G/5G) செல்லுலரைப் பயன்படுத்தவும். உங்கள் கட்டணத் தகவல் மற்றும் கணக்குகளைப் பாதுகாக்கவும். Online லைன் ஷொப்பிங் கணக்கில் பணம் செலுத்தும் தகவலைச் சேமிப்பதில் கவனமாக இருங்கள். நீங்கள் ஒரு கணக்கில் பணம் செலுத்தும் தகவலைச் சேமித்தால், அதைப் பாதுகாக்க பல காரணி அங்கீகாரத்தை (MFA)

செயல்படுத்த வேண்டும். இது சாத்தியமில்லாத பட்சத்தில், இணையக் குற்றவாளிகளை தவிர்த்துக்கொள்ள உதவும் நீண்ட, சிக்கலான மற்றும் தனித்துவமான கடவுச்சொற்றொடரை கணக்கின் கடவுச்சொல்லாக அமைத்துக்கொள்ள வேண்டும். உங்களுக்கான கடவுச்சொற்களை உருவாக்கவும் சேமிக்கவும் கடவுச்சொல் நிர்வாக முகாமைத்துவத்தையும் பயன்படுத்தலாம். பொருட்களை நீங்கள் கொள்வனவு செய்தற்கு முன் நம்பகமான விற்பனையாளர்களைப் பயன்படுத்துவதுடன், ஷொப்பிங் இணையதளங்களை ஆராய்வதும் முக்கியமானது.

மிகக் குறைந்த விலைகள், நேரடி வங்கி வைப்பீடு மூலம் பணம் செலுத்துதல் , விநியோகப் பொருட்களை திரும்பப் பெறுதல் மற்றும் தனியுரிமைக் கொள்கைகள் பற்றிய குறைந்த தகவலைக் கொண்ட இணைய தள களஞ்சியசாலைகள் போன்ற எச்சரிக்கை அறிகுறிகளை அறிந்து கொள்ளுவதும் முக்கியமாகும். பொருள் கொள்வனவுக்காக நேரடி வங்கி வைப்பீடுகளின் மூலம் ஒருபோதும் செலுத்தாத பாதுகாப்பான கட்டண முறைகளைப் பயன்படுத்த வேண்டும்.

பணப் பரிமாற்றம் அல்லது டிஜிட்டல் நாணயங்கள் எண்ணிம நாணயம் (Bitcoin) போன்ற வழியில் அனுப்பப்பட்ட பணத்தை மீட்டெடுப்பது அரிது. நீங்கள் பேபால் PayPal (மின் வணிக நிறுவனம்) அல்லது உங்கள் கடன் அட்டை (Credit Card) மூலம் பணம் செலுத்த வேண்டும். குறைந்த கடன் வரம்புடன் கூடிய இரண்டாவது கடன் அட்டையை பயன்படுத்த நீங்கள் விரும்பலாம். அத்தோடு அதை குறிப்பாக ழுநெடநெ ஷாப்பிங்கிற்காக பயன்படுத்துவதற்காக வைத்திருக்கலாம்.
சந்தேகத்திற்குரிய தொடர்பை தவிர்ப்பதுடன் அது குறித்து முறையிடவும். பொருட்கள் தொடர்பான உத்தரவு ழுசனநசள பற்றி நீங்கள் பெறும் விசித்திரமான தொலைபேசி அழைப்புகள், செய்திகள் அல்லது மின்னஞ்சல்கள் குறித்து எச்சரிக்கையாக இருக்க வேண்டும். உங்களுக்கு நினைவில் இல்லாத ழுசனநச பற்றி யாராவது உங்களைத் தொடர்பு கொண்டால், அது மோசடியாக இருக்கலாம். இவ்வாறான தொடர்பை நிறுத்திவிட்டுஅ அவர்களின் அதிகாரப்பூர்வ இணையதளத்தில் உள்ள விவரங்களைப் பயன்படுத்தி இந்த கடையுடன் தொடர்புகொண்டு சரிபார்க்க வேண்டும்.

Services

போலி விநியோக மோசடிகளைக் கவனியுங்கள்

போலி விநியோக மோசடிகளைக் கவனியுங்கள் உங்கள் பொருட்கள் கொண்டுவரப்படும் வரை நீங்கள் காத்திருக்கும்போது உங்கள் பாதுகாப்பைக் குறைத்துக்கொள்ள வேண்டாம். சைபர் குற்றவாளிகள் உங்களை ஏமாற்றக்கூடிய இணைப்புகளுடன் போலியான பொதிகள் குறித்த அறிவிப்புகளை அனுப்பலாம். உங்களின் தனிப்பட்ட விவரங்களைக் பெற்றுக்கொள்வதற்காக உங்களை ஏமாற்றலாம்.அத்தகைய செய்தியை நீங்கள் பெற்றால், அது தொடர்பான இணைப்பைக் கிளிக் செய்யாதீர்கள். செய்தியை உடனடியாக நீக்கிவிட வேண்டும்.
நீதி மன்ற நடவடிக்கைகளின் போது தேவையான எண்ணியல் சாட்சியங்களை உறுதி செய்துக்கொள்வதற்கும் பகுப்பாய்வுகளை மேற்கொள்ளுவதற்கும் ஒத்துழைப்பு வழங்குவது இலங்கை CERT நிறுவனம் கொண்டுள்ள மற்றுமொரு பொறுப்பாகும். இதற்காக விசேட அறிவாற்றலுடன் கூடியவர்களைக்கொண்டு நவீன நடைமுறைகளுக்கு அமைவாக பகுப்பாய்வு சேவைகளை வழங்க தயாராகவுள்ளது. சிக்கலான இணைய பாதுகாப்பு சம்பவங்கள், தரவு மீறல்கள் மற்றும் அங்கீகரிக்கப்படாத அணுகல் சம்பந்தப்பட்ட சம்பவங்களைத் தீர்ப்பதில் இலங்கை ஊநுசுவு தனிநபர்களுக்கும் நிறுவனங்களுக்கும் உதவுகிறது.
எமது தடயவியல் நிபுணர்கள் பல்வேறு ஆதாரங்களில் இருந்து டிஜிட்டல் தரவைப் பெற்றுக்கொள்வதற்கும், பாதுகாக்கவும் பகுப்பாய்வு செய்ய அதிநவீன கருவிகள் மற்றும் வழிமுறைகளைப் பயன்படுத்துகின்றனர். சைபர் தாக்குதலின் ஆதாரத்தை கண்டறிவது, நீக்கப்பட்ட கோப்புகளை மீட்டெடுப்பது அல்லது சட்ட நடவடிக்கைகளில் நிபுணர் சாட்சியங்களை வழங்குவது என எதுவாக இருந்தாலும், நாங்கள் நம்பகமான மற்றும் திறமையான தீர்வுகளை வழங்குகிறோம். எங்கள் டிஜிட்டல் தடயவியல் சேவைகள் மூலம், டிஜிட்டல் சம்பவங்கள் தொடர்பில் முக்கியமான நுண்ணறிவுகளை நீங்கள் பெற்றுக்கொள்ள முடியும்.
சம்பவங்கள் தொடர்பிலும் தகுந்த நடவடிக்கைகளை மேற்கொள்ளமுடிவதுடன் தகுந்த நடவடிக்கைகளை எடுத்து, உங்கள் ஒட்டுமொத்த இணையப் பாதுகாப்பு நிலைப்பாட்டை மேம்படுத்தவும் முடியும்.
போலியான கட்டணச் சாதனங்கள் மீதான விசாரணைகள் (கட்டணச் சாதன மோசடி சட்டத்தின்படி) தீங்குநிரல் சம்பவங்கள் ,மின்னஞ்சல் தொடர்பான டிஜிட்டல் தடயவியல் விசாரணைகள் CCTV வீடியோ காட்சி மேம்பாடுகள் தரவு மீட்பு, தரவுகளை இல்லாது செய்தல் முதலானவையும் மேற்கொள்ளப்படுகிறது.

Hot Line -101
report@cert.gov.lk
www.cert.gov.lk
www.onlinesafety.lk

இணையத்தில் கவனம் சிதறாமல் போலி செய்திகளிலிருந்து உங்களைப் பாதுகாத்துக் கொள்ளுங்கள்.

செய்தி முறையானது அல்ல என்று நீங்கள் நினைத்தால், அத்தகைய இணைப்புகளைக் கிளிக் செய்ய வேண்டாம். பெரும்பாலும், மோசடி செய்பவர்கள் நீங்கள் நம்பும் ஒரு நபர் அல்லது நிறுவனமாக தம்மை முன்நிலைப்படுத்திக் கொள்கிறார்கள். கோப்புறை நீட்டிப்புக்கான இணைப்பு Link to Folder நீங்கள் எதிர்பார்த்ததை விட வேறுபட்டால் கோப்பு Applications களைப் பதிவிறக்க வேண்டாம். (உதாரணமாக, ஒருகோப்பு PDF அல்லது படத்தை எதிர்பார்க்கும் போது .exe அல்லது .msi இல் முடிவடையும் கோப்பு)
நம்பத்தகாத ஆதாரங்களில் இருந்து வரும் உங்கள் மின்னஞ்சல்களில் பட மாதிரிக்காட்சிகளை அனுமதிக்காதீர்கள். இவை வைரஸ்கள் படங்களுடன் உங்களை இணைத்துக் கொள்வதுமாத்திரமின்றி நீங்கள் பயன்படுத்தும் நிரலின் அமைப்புகளில் அல்லது விருப்பங்களில் முடக்கப்படலாம்.
மூன்றாம் தரப்பு பதிவிறக்க தளங்களில் இருந்து பயன்பாடுகளைப் பதிவிறக்க வேண்டாம். அவை சட்டப்பூர்வமானவை என்று அதிகம் அறியப்படவில்லை. அதற்குப் பதிலாக உங்கள் சாதனத்திற்கான அதிகாரப்பூர்வ ளவழசந ஐ பயன்படுத்தவும். உதாரணமாக Apple App Store, Google Play Store அல்லது Microsoft Store ஆகியவற்றை குறிப்பிடலாம்
பயன்பாடுகளைப் பதிவிறக்க Download apps, இணைய விளம்பரங்களைக் கிளிக் செய்யக்கூடாது. அத்தோடு விளம்பரத் தடுப்பு மென்பொருளைப் பயன்படுத்தவும்.
ீநநச-வழிநநச வலைப் பின்னல்களிலிருந்து பயன்பாடுகளைப் பதிவிறக்கி நிறுவக்கூடாது ஏனெனில் இந்த கோப்புகளை யார் மாற்றினார்கள் என்பதை நீங்கள் அறிந்திருக்க முடியாது அல்லவா.
மின்னஞ்சல்கள் அல்லது உடனடிச் செய்திகளில் உள்ள இணைப்புகளைக் கிளிக் செய்யக்கூடாது அல்லது இணைப்புகளைச் செயல்படுத்தாதீர்கள். கோப்புகளை Applications யார் மாற்றினார்கள் என்பதை நீங்கள் அறிந்திருக்க முடியாது என்பதால் இதற்கு அனுமதிக்கூடாது.
தீங்கிழைக்கும் செய்திகளிலிருந்து உங்களைப் பாதுகாக்க ஞியஅ குடைவநச (மின்னஞ்சலைச் செயலாக்கும் மென்பொருள்) வடிப்பானைப் பயன்படுத்தவும்.
நீங்கள் ஒரு சேவை அல்லது கணக்கில் உள்நுழைய டழப ழை வேண்டும் என்றால், சட்டத்திற்குப் புறம்பான இணைப்பைக் கிளிக் செய்வதற்குப் பதிலாக நேரடியாக அவர்களின் இணையதளத்தைப் பார்வையிடவும்.

தனிப்பட்ட தரவு என்றால் என்ன?

இன்று பலர் தனிப்பட்ட தரவு பாதுகாப்பு பற்றி பேசுகிறார்கள், இதைப் பற்றி உங்களுக்கு உண்மையிலேயே தெரியுமா? பேச்சு வழக்கில் இன்னும் இதனை எளிமையாக கூறமுடியும்.

யாராவது ஒரு நபரை அடையாளங்காணக்கூடிய எத்தைய விடயங்களும் தரவுகளாவதுடன், அதில் அவரது பெயர், அடையாளங்காணக்கூடிய எண், இருப்பிடத் தரவு என்பன உள்ளடங்குவதுடன் உடல் சார்ந்த மரபணு, உளவியல், பொருளாதாரம், கலாச்சாரம் அல்லது சமூக அடையாளம், நேரடியாகவோ அல்லது வேறுவிதமாகவோ குறிப்பிட்ட காரணிகளை உள்ளடக்கியதாகும். ரூசூ39. தரவுப் பாதுகாப்பு என்பது ஒரு தனிநபரின் தனிப்பட்ட தரவு அவருக்குத் தெரியாமல் பயன்படுத்தப்படவோ, பகிரப்படவோ அல்லது பராமரிக்கப்படவோ கூடாது என்ற உரிமை தனி நபர் பாதுகாப்புச் சட்டத்தில் 2022 எண் 09 பிரிவில் உறுதி செய்யப்பட்டுள்ளது.

VPN என்றால் என்ன?

நம்பத்தகாத வலைப்பின்னல் இணையத்துடன் தொடர்புபடும்போது உணர்ச்சியைத் தூண்டக்கூடிய தகவல்களைப் பாதுகாப்பதற்காக VPN (Virtual Private Network மெய்நிகர் தனியார் வலைப்பின்னல்) என்ற இணைப்பு குறியாக்கவியக்கல் பயன்படுத்துகின்றன.
இங்கு ஊடுருவும் தரவுகளின் தனியுரிமை மற்றும் தரவு ரகசியத்தன்மையை உறுதிப்படுத்தவும், ஹேக்கர்களிடமிருந்து மட்டுமல்ல,உங்கள் இணைய சேவை வழங்குநரிடமிருந்து பாதுகாக்க, மறைகுறியாக்கத்தைப் பயன்படுத்தி உங்கள் தகவலை VPN பாதுகாக்கிறது.
இந்தப் படி முறைகள் மற்றவர்கள் கண்காணிப்பதை கடினமாக்குவுதுடன் நீங்கள் எதனுடன் தொடர்பை ஏற்படுத்துகின்றீர்கள் என்பது பற்றிய தகவல்களை சேகரிக்கவும் நீங்கள் இணைய தளத்தில் என்ன செய்கிறீர்கள் என்பதையும் பொது வலைப்பின்னலை பயன்படுத்தும் போதும் பாதுகாப்பை அதிகரிக்கவும் வழிவகை செய்கிறது.
VPN (Virtual Private Network - மெய்நிகர் தனியார் வலைப்பின்னல்) ஒரு சிறந்த வலுவாகப் பரிந்துரைக்கப்பட்டாலும், நீங்கள் அனைத்து பாதுகாப்பு இணைப்புகளையும் பெறுவதை உறுதிப்படுத்துவதற்கு நீங்கள் அதனை இற்றைப்படுத்தி நிறுவ வுவது அவசியமாகும்.
சேவைகள் மூலம், டிஜிட்டல் சம்பவங்கள் தொடர்பில் முக்கியமான நுண்ணறிவுகளை நீங்கள் பெற்றுக்கொள்ள முடியும்.
சம்பவங்கள் தொடர்பிலும் தகுந்த நடவடிக்கைகளை மேற்கொள்ளமுடிவதுடன் தகுந்த நடவடிக்கைகளை எடுத்து, உங்கள் ஒட்டுமொத்த இணையப் பாதுகாப்பு நிலைப்பாட்டை மேம்படுத்தவும் முடியும். போலியான கட்டணச் சாதனங்கள் மீதான விசாரணைகள் (கட்டணச் சாதன மோசடி சட்டத்தின்படி) தீங்குநிரல் சம்பவங்கள் ,மின்னஞ்சல் தொடர்பான டிஜிட்டல் தடயவியல் விசாரணைகள் CCTV வீடியோ காட்சி மேம்பாடுகள் தரவு மீட்பு, தரவுகளை இல்லாது செய்தல் முதலானவையும் மேற்கொள்ளப்படுகிறது.