ISSUE 05

2024

Cyber Guardian

Publication for your online safety

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

இலங்கைக்கான தேசிய சைபர் பாதுகாப்பு மையம்

முக்கியமான டிஜிட்டல் உள்கட்டமைப்பை வழங்கும் அரச நிறுவனங்களின் இணையப் பாதுகாப்பை உறுதி செய்வதற்காக இணையப் பாதுகாப்பு நிலையத்தை நிறுவுவதற்கு இலங்கை செர்ட் நிறுவனம் நடவடிக்கை எடுத்து வருகிறது. இந்த மையம் நிறுவப்பட்ட பிறகு, ஒரே நேரத்தில் முக்கியமான உள்கட்டமைப்பு நிறுவனங்கள் மீதான சைபர் தாக்குதல்களைக் கண்டறிந்து பதிலளிக்க முடியும்.

இந்த மையத்திற்கு தேவையான மென்பொருள் மற்றும் ஹார்டுவேர் ஏற்கனவே வாங்கப்பட்டு இறுதி கட்டமாக Cyber Security சம்பவ கண்காணிப்பு மையம் அமைக்கப்பட்டு வருகிறது. அத்தகைய சைபர் பாதுகாப்பு மையம் (SOC) இணைய அச்சுறுத்தல்களை அடையாளம் காணவும், சம்பவங்களை நிர்வகிக்கவும், பகுப்பாய்வு செய்யவும், தொடர்பு கொள்ளவும் மற்றும் சாத்தியமான சைபர் தாக்குதல்களைக் கண்டறியவும் முடியும். இது சாத்தியமான தாக்கத்தை மதிப்பிடவும் உதவும். அடுத்த சில ஆண்டுகளில், முக்கியமான டிஜிட்டல் உள்கட்டமைப்பை வழங்கும் அரச நிறுவனங்களுக்கு இந்தச் சேவையை வழங்க இலங்கை சான்றளிப்பு அதிகாரசபை செயற்படுகிறது. வேகமாக டிஜிட்டல் மயமாக்கப்படும் இலங்கையின் எதிர்கால எதிர்பார்ப்புகளைப் பூர்த்தி செய்வ-தற்காக சைபர் பாதுகாப்புத் துறையில் அதன்தொடர்ச்சியான ஆதரவை ஸ்ரீலங்கா செர்ட் மேலும் உறுதிப்படுத்துகிறது.

நண்பர் கோரிக்கைகளாக வரும் Phishing மோசடிக்காரர்கள்

இன்டர்நெட் மூலம் பல்வேறு இணைய மோசடிகள் வந்து போவது இன்றைய காலத்தில் சர்வ சாதாரணம். தனிப்பட்ட கோரிக்கைகள், வணிகம் மற்றும் வேலைவாய்ப்பு, பரிசுகள் மற்றும் பணப் பரிசுகள் ஆகியவை இதில் அடங்கும். இந்த இணைய மோசடிகள் உங்களை எப்படிப் பெறுகின்றன என்பதைப் புரிந்துகொள்வது அவசியம்.

1. போலி சுயவிவரங்கள்: Fake Profiles

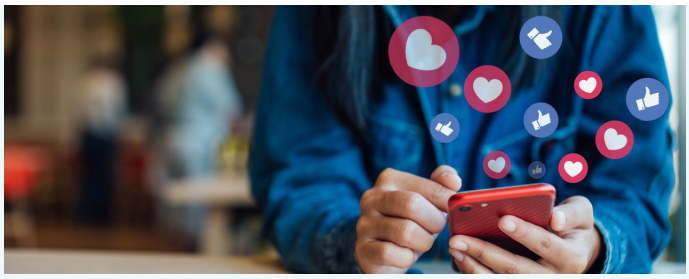
மோசடி செய்பவர்கள் பெரும்பாலும் உண்மையான நபர்களைப் போல தோற்றமளிக்கும் போலி சமூக ஊடக சுயவிவரங்களை உருவாக்குகிறார்கள், திருடப்பட்ட புகைப்படங்கள், பெயர்கள் மற்றும் பிற விவரங்களை சட்டப்பூர்வமாகத் தோன்றப் பயன்படுத்துகிறார்கள். இந்த சுயவிவரங்கள் உண்மையான நபர்கள் அல்லது நிறுவனங்களைப் போல ஆள்மாறாட்டம் செய்யலாம் அல்லது அவர்கள் நட்பு அந்நியர்களாகத் தோன்றலாம்.

2. நண்பர் கோரிக்கையை அனுப்புதல்: Friend Request

போலி சுயவிவரங்களை அமைத்த பிறகு, இந்த மோசடி செய்பவர்கள் பெரிய அளவில் பயனர்களுக்கு நண்பர் கோரிக்கைகளை அனுப்புகிறார்கள். உங்கள் தனிப்பட்ட தகவலைப் பெற்று, உங்கள் நண்பர்கள் பட்டியலை அணுக அவர்களை அனுமதிப்பதே குறிக்கோள்.

3. நம்பிக்கையைப் பெறுதல்: Gaining Trust

நண்பர் கோரிக்கையை ஏற்றுக்கொண்ட பிறகு, நம்பிக்கையை வளர்க்க மோசடி செய்பவர் உங்களுடன் தொடர்பு கொள்ளத்



தொடங்குவார். உறவை இன்னும் உண்மையானதாகக் காட்ட உங்கள் புகைப்படங்களில் கருத்துகள் போன்றவற்றைச் சேர்க்கலாம்.

4. ∴பிஷிங்கின் துவக்கம்: Phishing Attempt

நம்பிக்கையை நிறுவியவுடன், மோசடி செய்பவர் உங்களுக்கு முக்கியமான அல்லது அவசரமானதாகக் கூறி தீங்கிழைக்கும் இணைப்புடன் நேரடிச் செய்தியை அனுப்பலாம். "இந்தப் புகைப்படங்களைப் பாருங்கள்!" போன்ற ஏதாவது இருக்கலாம் அல்லது "நீங்கள் ஒரு பரிசை வென்றுள்ளீர்கள், அதைப் பெற இங்கே Click செய்யவும்!"

அந்த இணைப்பு குயஉநடிழழம போன்ற பிரபலமான சேவையின் போலி உள்நுழைவுப் பக்கமாக இருக்கலாம், அங்கு உங்கள் பயனர்பெயர் மற்றும் கடவுச்சொல்லை உள்ளிடுமாறு கேட்கப்படுவீர்கள். நீங்கள் செய்தால், மோசடி செய்பவர் உங்கள் எல்லா தகவல்களையும் கைப்பற்றுவார்.

5. மேலும் சுரண்டல்

அந்தத் தகவலின் மூலம் உங்கள் உள்நுழைவு விவரங்களைக் கொண்டு, மோசடி செய்பவர் உங்கள் கணக்கைப் பயன்படுத்தி உங்கள் கணக்கை அணுகலாம், மேலும் தகவல்களைத் திருடலாம் மற்றும் உங்கள் நண்பர்களுக்கு ∴பிஷிங் செய்திகளை அனுப்பலாம், மேலும் மோசடியை மேலும் பரப்பலாம்.

நண்பர்களிடமிருந்து வரும் ∴பிஷிங் மோசடிகளில் இருந்து உங்களை எவ்வாறு பாதுகாத்துக் கொள்வது?

1. அறியப்படாத கோரிக்கைகள் குறித்து ஜாக்கிரதை

உங்களுக்குத் தெரியாத ஒருவரிடமிருந்து நண்பர் கோரிக்கையைப் பெற்றால் கவனமாக இருங்கள், குறிப்பாக சுயவிவரம் புதியதாக இருந்தால் அல்லது இடுகைகள் மிகக் குறைவாக இருந்தால். மோசடி செய்பவர்கள் பெரும்பாலும் உண்மையான உள்ளடக்கம் இல்லாமல் போலி சுயவிவரங்களை உருவாக்குகிறார்கள்.

2. சுயவிவரத்தை சரிபார்க்கவும்

கோரிக்கை உங்களுக்குத் தெரிந்த ஒருவரைப் போல் தோன்றினால், அது முறையானதா என்பதை உறுதிப்படுத்த அவரது சுயவிவரத்தை இருமுறை சரிபார்க்கவும். மற்ற செயல்பாடுகள் இல்லை என்பதை சரிபார்க்கவும். மற்றொரு வழியில் நண்பர்களை அழைப்பதன் மூலம் உறுதிப்படுத்தவும்.

3. சந்தேகத்திற்கிடமான இணைப்புகளைக் Click செய்வதைத் தவிர்க்கவும்

உங்களுக்குத் தெரிந்த ஒருவரிடமிருந்து கோரிக்கை வந்தாலும், இணைப்புகளைக் கொண்ட எதிர்பாராத செய்திகள் குறித்து எச்சரிக்கையாக இருக்கவும், குறிப்பாக செய்தி வழக்கத்திற்கு மாறானதாக இருந்தால் அல்லது அந்த நபர் இணைப்பைப் பார்க்கவில்லை என்றால்.

4. சந்தேகத்திற்குரிய செயல்பாட்டைப் புகாரளிக்கவும்

நண்பர் கோரிக்கையானது ∴பிஷிங் மோசடியின் ஒரு பகுதியாக இருப்பதாக நீங்கள் சந்தேகித்தால், சமூக ஊடக மன்றத்தில் சுயவிவரத்தைப் புகாரளிக்கவும். இது மோசடி செய்பவர் மற்றவர்களை மேலும் குறிவைப்பதைத் தடுக்க உதவுகிறது.

உடல் பாதுகாப்பைப் போலவே இணையப் பாதுகாப்பும் முக்கியமானது

SCAM

உங்கள் இணைப்புகள் ஆரோக்கியமானவை என்பதற்கு சைபர்ஸ்பேஸ் ஆரோக்கியம் மற்றொரு உத்தரவாதமாகும். கைகளை கழுவுதல், வைட்டமின்கள் உட்கொள்வது அல்லது உடற்பயிற்சி செய்வது போன்ற முன்னெச்சரிக்கை நடவடிக்கைகளை எடுக்கும் போது கூட மக்கள் நோய்வாய்ப்படுவதைப் போலவே, நீங்கள் இணைய பாதுகாப்புச் சிறந்த நடைமுறைகளைப் பின்பற்றினாலும் உங்கள் ஆன்லைன் அமைப்புகள்தாக்கப்படலாம். சைபர் பின்னடைவு என்பது உங்களால் முடிந்த சிறந்த உத்திகளை செயல்படுத்துவதாகும்.

இன்று, சைபர் பாதுகாப்பு என்பது ஒரு முக்கியமான கருத்தாகும், இது இணைய தாக்குதல்களைத் தாங்கும் மற்றும் மீள்வதற்கும், அத்துடன் புதிய அச்சுறுத்தல்களுக்கு ஏற்ப மாற்றியமைக்கும் திறனை வலியுறுத்துகிறது. தனிநபர்கள், வணிகங்கள் மற்றும் பிற நிறுவனங்கள் தங்கள் சொந்த பின்னடைவை மதிப்பிடலாம் மற்றும் அவர்களின் இணைய பின்னடைவு உத்திகளை வலுப்படுத்தலாம்.

சைபர் பாதுகாப்பு எதிர்த்தெறிதலை புரிந்துகொள்வது

பொதுவாக, சைபர் செக்யூரிட்டி எதிர்த்தெறிதலை என்பது அவசியமான செயல்பாடுகளை பாதுகாப்பாக பராமரிக்கவும், இணைய சம்பவங்களில் இருந்து விரைவாக மீளவும் ஒரு நிறுவனத்தின் திறனின் முதுகெலும்பாகும். இதில் செயல் படிகள், சம்பவ மறுமொழி தயார்நிலை மற்றும் தற்செயல் மீட்பு உத்திகள் ஆகியவை அடங்கும்.

பயனுள்ள எதிர்த்தெறிதல், தாக்குதல்களின் தாக்கத்தைக்

குறைக்கவும், வேலையில்லா நேரத்தைக் குறைக்கவும், முக்கியமான தரவைப் பாதுகாக்கவும், வாடிக்கையாளர் நம்பிக்கையைப் பராமரிக்கவும் மற்றும் ஒழுங்குமுறைத் தேவைகளுக்கு இணங்கவும் உதவும். இது நிறுவனத்தின் நற்பெயரையும் நிதி ஸ்திரத்தன்மையையும் பாதுகாக்கிறது.

உங்கள் சொந்த சைபர் எதிர்த்தெறிதல மதிப்பிடுங்கள்

உங்களை நீங்களே கேட்டுக்கொள்ளுங்கள்:

நான் நீண்ட, சிக்கலான மற்றும் தனித்துவமான கடவுச்சொற்களைப் பயன்படுத்துகிறேனா?

ஒவ்வொரு கணக்கிற்கும் MFA பல காரணி அங்கீகாரத்தை நான் இயக்கியுள்ளேனா?

நான் மென்பொருளை தொடர்ந்து புதுப்பிக்கிறேனா?

சந்தேகத்திற்கிடமான இணைப்புகளைக் கிளிக் செய்ய மறுக்கிறேனா அல்லது தெரியாத இணைப்புகளைப் பதிவிறக்குகிறேனா?

முக்கியமான தரவை எவ்வாறு காப்புப் பிரதி எடுப்பது மற்றும் இணையச் சம்பவத்தின் போது அதை எவ்வாறு மீட்டெடுப்பது என்பது எனக்குத் தெரியுமா?

@The National Cybersecurity Alliance.

Pictuer Story

ஒரு தென் மாகாண சைபர் பாதுகாப்பு பட்டறை

தென் மாகாண அரசாங்க அதிகாரிகள் மற்றும் தகவல் தொழில்நுட்ப அதிகாரிகளுக்கான ஒரு நாள் இணைய பாதுகாப்பு விழிப்புணர்வு செயலமர்வு அண்மையில் காலி தென் மாகாண முகாமைத்துவ மற்றும் அபிவிருத்தி நிலையத்தில் இடம்பெற்றது. இலங்கை செர்ட் நிறுவனம் மற்றும் தென் மாகாண பிரதம செயலகம் இணைந்து ஏற்பாடு செய்த இந்த செயலமர்வில் சுமார் 150 பேர் கலந்து கொண்டனர்.