ISSUE 06

2024

Cyber Guardian

Publication for your online safety

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

IBM அறிக்கையின்படி, தரவு மீறல்களின் செலவுகளையும் வாடிக்கையாளர்கள் ஏற்கின்றனர்.

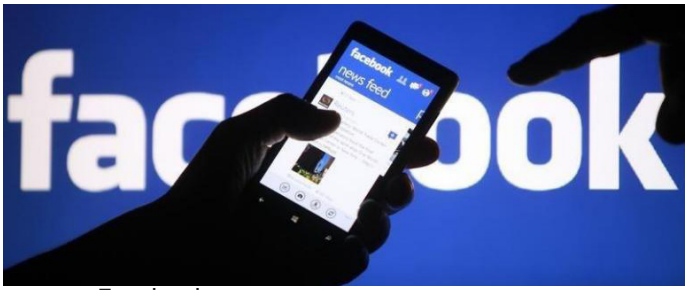
ஜூலை மாதம் வெளியிடப்பட்ட IBM இன் 2024 தரவு மீறல் அறிக்கையின்படி, தரவு மீறலின் சராசரி செலவு $4.88 மில்லியனாக உயர்ந்துள்ளது - இது முந்தைய ஆண்டை விட 10% அதிகரிப்பு. ஆய்வு, Ponemon நிறுவனத்தால் நடத்தப்பட்டது மற்றும் IBM ஆல் பகுப்பாய்வு செய்யப்பட்டது, 604 உலகளாவிய நிறுவனங்களின் தரவு மீறல்கள் பற்றிய ஆழமான பார்வையை வழங்குகிறது. இந்த சம்பவங்களை அனுபவித்த 3,500க்கும் மேற்பட்ட பாதுகாப்பு மற்றும் வணிக நிபுணர்களிடமிருந்து நுண்ணறிவு சேகரிக்கப்பட்டது.

அறிக்கையின் முக்கிய கண்டுபிடிப்பு என்னவென்றால், வணிகங்கள் தரவு மீறல்களின் செலவுகளை தங்கள் பொருட்கள் மற்றும் சேவைகளுக்கு மாற்றுவதால், நுகர்வோர் நிதிச் சுமையின் ஒரு பகுதியைச் சுமக்கிறார்கள். இந்த ஆண்டு, 63% வணிகங்கள் தரவு மீறல்களால் ஏற்படும் இழப்புகளை ஈடுகட்ட விலைகளை உயர்த்த வேண்டும் என்று தெரிவித்தன, இது கடந்த ஆண்டு 57% ஆக இருந்தது. இந்த விலை உயர்வுகள் அதிக உற்பத்தி செலவுகள், சிஸ்டம் வேலையில்லா நேரம் மற்றும் வாடிக்கையாளர்கள் போட்டியாளர்களுக்கு மாறுவதால் வாடிக்கையாளர் குழப்பம் ஆகியவற்றிலிருந்து உருவாகிறது.

சமூகப் பாதுகாப்பு எண்கள், மின்னஞ்சல்கள், தொலைபேசி எண்கள் மற்றும் வீட்டு முகவரிகள் உட்பட வாடிக்கையாளர்களின் தனிப்பட்ட தகவல்களை கிட்டத்தட்ட 46% மீறல்கள் உள்ளடக்கியது. கூடுதலாக, 43% மீறல்கள் அறிவுசார் சொத்து மற்றும் வர்த்தக ரகசியங்கள் போன்ற முக்கியமான கார்ப்பரேட் தரவுகளை உள்ளடக்கியது.

இந்த மீறல்களுக்கு முதன்மையான காரணங்களில் ஒன்று திறமையான இணைய பாதுகாப்பு பணியாளர்களின் பற்றாக்குறை ஆகும். கணக்கெடுக்கப்பட்ட நிறுவனங்களில் பாதிக்கும் மேற்பட்டவை தங்கள் பாதுகாப்புக் குழுக்களில் கடுமையான பணியாளர் பற்றாக்குறையுடன் போராடி வருவதாகக் குறிப்பிட்டுள்ளன. பாதுகாப்பை நிர்வகிப்பதற்கு பலர் புதிய AI தொழில்நுட்பங்களை பின்பற்றினாலும், இந்த குழுக்கள் ஏற்கனவே குறிப்பிடத்தக்க அழுத்தத்தில் உள்ளன. @ The National Cybersecurity Alliance

பேஸ்புக் ஹேக் செய்யப்பட்டால் என்ன செய்வது?



உங்கள் Facebook கணக்கு ஹேக் செய்யப்பட்டால், விரைவாக உங்கள் கணக்கைப் பாதுகாப்பதோடு, உங்கள் தனிப்பட்ட தகவல்களையும் பாதுகாக்க வேண்டும்.
நீங்கள் செய்ய வேண்டியது கீழ்வருமாறு:

1. உங்களால் இன்னும் உங்கள் கணக்கை அணுக முடியுமா என்று பார்க்கவும்

உங்களின் வழக்கமான சான்றுகளுடன் உள்நுழைய முயற்சிக்கவும் வெற்றியடைந்தால், உடனடியாக உங்கள் கடவுச்சொல்லை மாற்றி உங்கள் கணக்கு அமைப்புகளை மதிப்பாய்வு செய்யவும்.
கடவுச்சொல் மீட்டமைப்பு: உங்களால் உள்நுழைய முடியாவிட்டால உங்கள் மின்னஞ்சல் அல்லது தொலைபேசி எண் வழியாக உங்கள் கடவுச்சொல்லை மீட்டமைக்க Facebook உள்நுழைவு பக்கத்தில் “கடவுச்சொல்லை மறந்துவிட்டீர்கள்” என்பதை பயன்படுத்தவும்.

2. உங்கள் கடவுச்சொல்லை மாற்றவும்

புதிய கடவுச்சொல்: உங்கள் கணக்கை அணுக முடிந்தால், உங்கள் கடவுச்சொல்லை வலுவான மற்றும் தனித்துவமானதாக மாற்றவும். பொதுவான கடவுச்சொற்கள் அல்லது நீங்கள் மற்ற தளங்களில் பயன்படுத்தியதை முற்றாக தவிர்க்கவும்.
இரு-காரணி அங்கீகாரத்தை இயக்குங்கள்: கூடுதல் பாதுகாப்பு அடுக்கு சேர்க்க இரு காரணி அங்கீகாரத்தை (2FA) அமைக்கவும். இது ஒவ்வொரு முறையும் நீங்கள் ஒரு புதிய சாதனத்திலிருந்து உள்நுழையும்போது உங்கள் தொலைபேசி அல்லது மின்னஞ்சலுக்கு ஒரு குறியீட்டை அனுப்பும்.

3. உங்கள் மின்னஞ்சல் கணக்கைச் சரிபார்த்து பாதுகாக்கவும்

மின்னஞ்சல் அணுகல்: Facebook உடன் தொடர்புடைய உங்கள் மின்னஞ்சல் கணக்கு பாதுகாப்பானது என்பதை உறுதிப்படுத்தவும். ஹேக்கர்கள் உங்கள் மின்னஞ்சலை அணுகினால், அவர்களால் உங்கள் Facebook கணக்கைக் கட்டுப்படுத்த முடியும்.

மின்னஞ்சல் கடவுச்சொல்லை மாற்றவும்: தேவைப்பட்டால், உங்கள் மின்னஞ்சலை மாற்றவும் கடவுச்சொல் மற்றும் அங்கு இரண்டு காரணி அங்கீகாரத்தை இயக்கவும்.

4. Hack ஐ Facebook இல் புகாரளிக்கவும்

Facebook இன் உதவி மையம் மூலம் புகாரளிக்கவும்:
Facebook இன் உதவிக்குச் செல்லவும் “ஹேக் செய்யப்பட்ட கணக்கு” என்பதை மையப்படுத்தி தேடவும். உங்கள் கணக்கு திருடப்பட்டதாக புகாரளிக்க, வழிமுறைகளைப் பின்பற்றவும்.

Facebook ஆதரவு: உங்களால் உங்கள் கணக்கை அணுக முடியவில்லை என்றால், ஹேக் செய்யப்பட்ட கணக்குகளுக்கு

Facebook இன் ஆதரவு விருப்பங்களைப் பயன்படுத்தவும். ID ஐ சமர்ப்பிப்பதன் மூலம் உங்கள் அடையாளத்தைச் சரிபார்க்கும்படி அவர்கள் கேட்கலாம்.

5. கணக்கு செயல்பாட்டை மதிப்பாய்வு செய்யவும்

சமீபத்திய செயல்பாட்டைச் சரிபார்க்கவும்: சமீபத்திய உள்நுழைவு இடங்கள் மற்றும் சாதனங்களைப் பார்க்கவும். நீங்கள் ஏதேனும் சந்தேகத்திற்கிடமான செயல்பாட்டைக் கண்டால், மற்ற எல்லா அமர்வுகளிலிருந்தும் வெளியேறவும் (Security மற்றும் Login settings வழியாக இதைச் செய்யலாம்).
இணைக்கப்பட்ட Apps களை மதிப்பாய்வு செய்யவும்: உங்களுடன் இணைக்கப்பட்டுள்ள அறியப்படாத Apps கள் அல்லது சேவைகளை சரிபார்க்கவும் பேஸ்புக் கணக்கை நீக்கவும்.

6. உங்கள் தொடர்புகளுக்குத் தெரிவிக்கவும்

நண்பர்கள் மற்றும் குடும்பத்தினரை எச்சரிக்கவும்: கணக்கு Hack செய்யப்பட்டது உங்கள் தொடர்புகளுக்குத் தெரியப்படுத்துங்கள். இது ஹேக்கரின் எந்த செய்திகளுக்கும் அல்லது இடுகைகளுக்கும் பலியாகாமல் தடுக்கிறது.

7. சந்தேகத்திற்கிடமான செயலை கண்காணிக்கவும்

Phishing முயற்சிகளைக் கவனியுங்கள்: தனிப்பட்ட தகவல்களைக் கேட்கும் மின்னஞ்சல்கள் அல்லது செய்திகள் Facebook இல் இருந்து வந்ததாகத் தோன்றினாலும், எச்சரிக்கையாக இருங்கள்.
கணக்கை தவறாமல் மதிப்பாய்வு செய்யவும்: ஏதேனும் வழக்கத்திற்கு மாறான செயல்பாடு இருந்தால் உங்கள் கணக்கைத் தொடர்ந்து கண்காணிக்கவும்.

8. கூடுதல் பாதுகாப்பு நடவடிக்கைகளைக் கவனியுங்கள்

அடையாளத் திருட்டுப் பாதுகாப்பு: முக்கியமான தகவல் அம்பலப்படுத்தப்பட்டால், அடையாளத் திருட்டுப் பாதுகாப்புச் சேவைகளைப் பயன்படுத்துவதைக் கவனியுங்கள்.

பாதுகாப்பு அமைப்புகளை தவறாமல் புதுப்பிக்கவும்: உங்கள் கணக்கைப் பாதுகாப்பாக வைத்திருக்க, உங்கள் பாதுகாப்பு அமைப்புகளை அவ்வப்போது மதிப்பாய்வு செய்து புதுப்பிக்கவும்.

9. எதிர்கால ஹேக்குகளைத் தடுக்கவும்

வலுவான, தனித்துவமான கடவுச்சொற்களைப் பயன்படுத்தவும்: பல தளங்களில் ஒரே கடவுச்சொல்லைப் பயன்படுத்துவதைத் தவிர்க்கவும்.

சந்தேகத்திற்கிடமான இணைப்புகளைப் பற்றி எச்சரிக்கையாக இருங்கள்: மின்னஞ்சல்களில் உள்ள இணைப்புகள் அல்லது செய்திகள் சட்டபூர்வமானவை என்று நீங்கள் உறுதி செய்யாத வரை Click செய்யாதீர்கள்.

சைபர் கிரைமினல்கள் Phishing செய்ய விரும்புகிறார்கள், ஆனால் நீங்கள் பலியாக வேண்டியதில்லை.

Phishing முயற்சியை அடையாளம் கண்டுகொண்டால், அதில் விழுவதைத் தவிர்க்கலாம். இணைப்புகளைக் கிளிக் செய்வதற்கு முன் அல்லது இணைப்புகளைப் பதிவிறக்குவதற்கு முன், சில வினாடிகள் (உதாரணமாக 4 வினாடிகள்) மற்றும் மின்னஞ்சல் முறையானதாக இருப்பதை உறுதிப்படுத்தவும். Phishing மின்னஞ்சலை எவ்வாறு தெளிவாகக் கண்டறிவது என்பதற்கான சில விரைவான உதவிக்குறிப்புகள் இங்கே:

உண்மையாக இருக்க முடியாத அளவுக்கு நல்ல சலுகை இதில் உள்ளதா?

அவசரமான, ஆபத்தான அல்லது அச்சுறுத்தும் மொழி இதில் உள்ளதா?

எழுத்துப்பிழைகள் மற்றும் தவறான இலக்கணங்களால் சிக்கலாக எழுதப்பட்ட எழுத்தா?

வாழ்த்து தெளிவற்றதா அல்லது மிகவும் பொதுவானதா?

தனிப்பட்ட தகவலை அனுப்புவதற்கான கோரிக்கைகள் இதில் உள்ளதா?

அறிமுகமில்லாத ஒன்றைக் Click செய்வது அவசரத்தை வலியுறுத்துகிறதா?

இது ஒரு விசித்திரமான அல்லது திடீர் வணிகக் கோரிக்கையா?

அனுப்புநரின் மின்னஞ்சல் முகவரி அது வரும் நிறுவனத்துடன் பொருந்துகிறதா? pavpal.com அல்லது anazon.com போன்ற சிறிய எழுத்துப்பிழைகளைத் தேடுங்கள்.

ஓ! நான் ஒரு Phishing மின்னஞ்சலைப் பார்க்கிறேன். நான் என்ன செய்வது?

கவலைப்பட வேண்டாம், நீங்கள் ஏற்கனவே கடினமான பகுதியை செய்துள்ளீர்கள், அதாவது ஒரு மின்னஞ்சல் போலியானது மற்றும் ஒரு குற்றவாளியின் Phishing பயணத்தின் ஒரு பகுதி என்பதை அங்கீகரிப்பது.

நீங்கள் அலுவலகத்தில் இருந்தால், உங்கள் பணி மின்னஞ்சல் முகவரிக்கு மின்னஞ்சல் வந்திருந்தால், அதை உங்கள் IT மேலாளர் அல்லது பாதுகாப்பு அதிகாரியிடம் விரைவில் புகாரளிக்கவும்.

உங்கள் தனிப்பட்ட மின்னஞ்சல் முகவரிக்கு மின்னஞ்சல் வந்திருந்தால், அது சொல்வதைச் செய்ய வேண்டாம். எந்த இணைப்புகளையும் Click செய்யாதீர்கள் - குழுவிலகும் இணைப்பைக் கூட - அல்லது மின்னஞ்சலுக்குப் பதிலளிக்கவும். அந்த நீக்கு பொத்தானை மட்டும் பயன்படுத்தவும். நினைவில் கொள்ளுங்கள், இணைப்புகளில் கிளிக் செய்ய வேண்டாம், நீக்கவும்.

உங்கள் பாதுகாப்பை ஒரு படி மேலே கொண்டு சென்று உங்கள் மின்னஞ்சல் திட்டத்தில் இருந்து அனுப்பும் முகவரியைத் தடுக்கலாம். (Outlook. Gmail. Mac Mail. Yahoo! Mail)

Picture Story

கம்பஹாவில் இணைய பாதுகாப்பு அமைப்புகளில் திறன் வளர்ப்பு திட்டம்

கம்பஹா மாவட்டச் செயலாளர் மாவட்ட ஆளுநர் திரு.லலிந்த கமகே தலைமையில், கம்பஹா மாவட்டச் செயலக கேட்போர் கூடத்தில், அரச நிறுவனங்களுக்கான இணையப் பாதுகாப்பு முறைமைகள் தொடர்பான திறன் மேம்பாட்டு நிகழ்ச்சி அண்மையில் நடைபெற்றது

இலங்கை கணினி அவசரநிலைப் பதிலளிப்புக் குழு (Sri Lanka CERT) மற்றும் உள்நாட்டலுவல்கள் அமைச்சின் ஒத்துழைப்புடன் இந்த நிகழ்ச்சி நடத்தப்பட்டது. இதில் கம்பஹா மாவட்டத்தை சேர்ந்த பிரதேச செயலாளர்கள் உட்பட தகவல் தொழிநுட்பம் தொடர்பான அதிகாரிகள் கலந்துகொண்டனர்.