பொது வை-ஃபை இணைப்பைப் பாதுகாப்பாகப் பயன்படுத்துவதற்கான உதவிக்குறிப்புகள்

இணையத்தில் மோசடிப் பேர்வழிகள் உங்களை அவர்களுக்கு சாதகமாகப் பயன்படுத்திக்கொள்ள முடியும். உங்களுக்கு பொது வை-ஃபை இணைப்பைப் பயன்படுத்த வேண்டியிருந்தால், அதற்கான சில உதவிக்குறிப்புகளை கீழே காணலாம்.

கொரோனாவின் தீவிர நோய்ப்பரவல் காரணமாகவும் வணிகங்களும் நூலகங்களும் மூடப்பட்டிருப்பதாலும் நம்மில் பலர் இணையத்தில் அதிக நேரம் செலவிடுகிறோம். இதன் விளைவாக, இணையத்தில் இணைய நாம் பொது வை-ஃபையைப் பயன்படுத்த வேண்டியிருக்கலாம். நீங்கள் பொது வை-ஃபை பயன்படுத்த வேண்டியிருந்தால், உங்கள் தரவுகளைப் பாதுகாக்க உதவும் மாகாண தலைமை தனியுரிமை அதிகாரியின் பின்வரும் பரிந்துரைகளை தயவுசெய்து கவனத்தில் கொள்ளவும்:

1. உங்களுக்கு சரியான வலைத்தொடர்பு இருப்பதை உறுதிப்படுத்துங்கள்.

சரியான வலைத்தொடர்பில் நீங்கள் இணைப்பதை உறுதிப்படுத்துங்கள். பெயரைப் பார்த்தால் தீங்கற்றதாகத் தோன்றும் வலைத்தொடர்பை மோசடிப்பேர்வழிகள் உருவாக்கலாம். ஆனால் உண்மையில் உங்களது இணைய உலாவலை கண்காணிக்கும்படி அமைக்கப்பட்ட ஒரு வலைத்தொடர்பாக அது இருக்கக்கூடும். இதன் அர்த்தம், நீங்கள் நுழைவுச்சான்றுகள் அல்லது கடவுச்சொற்களை இணையதளங்களில் உள்ளிடும்போது, தகவல் திருடர்கள் உங்கள் தகவல்களைத் திருடமுடியும்.

இதிலிருந்து காத்துக்கொள்ள வலைத்தொடர்புப் பெயரை கவனமாகப் படிக்கவும். முடிந்தால், ஒரு பணியாளரிடம் கேட்கலாம் அல்லது வலைத்தொடர்பு சட்டபூர்வமானது என்பதை உறுதிப்படுத்த அதன் அடையாளத்தை சரிபார்க்கவும்.

பிரபல காபி சங்கிலித்தொடர்கள் போன்ற நன்கு அறியப்பட்ட வலைத்தொடர்புகள் குறைவான சந்தேகத்துக்குரியவை. காரணம் அத்தகு நிறுவனங்கள் அவர்களது வணிகத்தோடு இணைந்த ஒரு சேவையாக வலைத்தொடர்பை இயக்குகின்றன. அறிந்த வலைத்தொடர்புகள் பொதுவாக உங்கள் அலைபேசியில் காண்பிக்கப்படும் ஏதோவொரு இலவச வை-ஃபை இணைப்புகளைக் காட்டிலும் பாதுகாப்பானவை.

2. தானாக இணைப்பு ஏற்படுத்தும் செயலம்சத்தை அணையுங்கள்.

பல சாதனங்களில் (பல்திறன்பேசிகள், மடிக்கணினிகள் மற்றும் டேப்லட்கள்) தானாக இணைப்பு ஏற்படுத்தும் அமைப்புகள் உள்ளது. இந்த அமைப்பு அருகிலுள்ள வலைத்தொடர்புடன் வசதிப்படி இணைத்துக்கொள்ள அனுமதிக்கிறது. நம்பகமான வலைத்தொடர்புகளுக்கு இது சரிதான். ஆனால் இதனால் பாதுகாப்பற்ற வலைத்தொடர்புடனும் இணைப்பு பெற வாய்ப்புள்ளது. இந்த அம்சத்தை உங்கள் சாதனத்தின் அமைப்புகளுக்குள் சென்று முடக்கலாம். குறிப்பாக பழக்கமில்லாத இடங்களுக்கு நீங்கள் பயணிக்கும்போது இத்தகு அமைப்புகளை அணைத்து வைத்திருக்கவும். கூடுதல் முன்னெச்சரிக்கையாக, பொது வை-ஃபையை பயன்படுத்தியபின், “forget network”ஐ தேர்வுசெய்யுங்கள்.

பொது இடங்களில் இருக்கையில் உங்கள் Bluetoothஐயும் நீங்கள் கண்காணிக்க வேண்டும். Bluetooth இணைப்பு பல்வேறு சாதனங்கள் ஒன்றுக்கொன்று தொடர்புகொள்ள அனுமதிக்கிறது. தகவல் திருடர்கள் திறந்துள்ள Bluetooth சமிக்ஞைகளைக் கண்டு உங்கள் சாதனங்களை அணுகமுடியும். பழக்கமில்லாத இடங்களில் நீங்கள் இருக்கும்போது இந்தச் செயலமைப்பை உங்கள் செல்பேசியிலும் பிற சாதனங்களிலும் அணைத்து வைத்திருக்கவும்.

3. கோப்பு பகிர்வை அணைக்கவும்.

பொது வை-ஃபை இணைப்பில் இருக்கும்போது கோப்பு பகிர்வு செயலமைப்பு அணைத்து வைத்திருப்பதை உறுதிசெய்யவும். உங்கள் இயங்குதளத்தைப் பொறுத்து அமைப்பு விருப்புரிமைகள் அல்லது கட்டுப்பாட்டுப் பலகை மூலம் கோப்பு பகிர்வை அணைக்கலாம். நீங்கள் அணைக்க விரும்பும் கோப்பு பகிர்வு அம்சத்திற்கு AirDrop ஓர் உதாரணமாகும். Windows (விண்டோஸ்)/பிசி போன்ற சில

இயங்குதளங்களில், முதல்தடவை புதிதாக பொது வலைத்தொடர்பில் இணைக்கும்போது “பொது" விருப்புரிமையை நீங்கள் தேர்ந்தெடுக்கையில் கோப்பு பகிர்வு அணைக்கப்படும்.

கோப்பு பகிர்வை அணைக்கும் வழிமுறை

ஒரு கணினியில்:

1. நெட்வொர்க் அண்ட் ஷேரிங் சென்டர் செல்க.
2. பின் அட்வான்ஸ்ட் ஷேரிங் அமைப்புகளை மாற்றவும்.
3. கோப்பு மற்றும் அச்சு இயந்திரப் பகிர்வை அணைக்கவும்.

Macs கணினியில்:

1. System Preferences (அமைப்பு முன்னுரிமைகள்) செல்க.
2. ஷேரிங்கை தேர்வுசெய்க.
3. அனைத்தையும் தேர்வு நீக்கம் செய்க.
4. அடுத்ததாக, தேடுவானில் AirDrop மீது சொடுக்கி Allow me to be discovered by: No One (பிறரால் பார்க்க அனுமதி: யாருமில்லை) தேர்வுசெய்க.

iOSல், கட்டுப்பாட்டு மையத்தில் AirDropஐ கண்டறிந்து அணைக்கவும்.

4. ஒரு VPNஐ பயன்படுத்தவும்.

உங்கள் சாதனத்தில் ஒரு VPN (மெய்நிகர் தனிப்பட்ட வலைத்தொடர்பு) நிறுவுவது குறித்து யோசியுங்கள். பொது வலைத்தொடர்பில் மின்னணுசார் தனியுரிமைக்கு ஒரு VPN மிக பாதுகாப்பான தேர்வாகும். அது உங்கள் சாதனத்திலிருந்து செல்லும் மற்றும் உள்வரும் தரவுகளை குறியாக்கம் செய்து பாதுகாப்புச் ”சுரங்கமாக” செயல்படுகிறது. இதனால் ஒரு வலைத்தொடர்பில் உங்கள் தரவுகள் செல்வது வெளியில் தெரியாது.

5. குறியாக்கம் செய்யப்பட்ட வலைத்தளங்கள் - HTTPS. குறித்து FBI எச்சரிக்கைகள்.

“https.” எனத் தொடங்கும் இணையதள முகவரிகள் குறித்து FBI எச்சரித்துள்ளது. “https” இருப்பதும் பூட்டு அடையாளப்படமும் இணைய போக்குவர்த்து குறியாக்கம் செய்யப்பட்டதையும் வருகைதருவோர் தரவுகளை பாதுகாப்பாகப் பகிரமுடியும் என்பதையும் குறிக்கிறது. எனினும், சைபர் குற்றவாளிகள் இப்போது httpsஐ இணைத்து பாதுகாப்பான தோற்றத்தைத் தந்து மக்களைக் கவர்வதன் மூலம் அவர்களது நம்பிக்கையைப் பெற்று வருகிறார்கள்.

FBIயின் பரிந்துரைகள்:

- ஒரு மின்னஞ்சலில் வரும் பெயரை எளிதாக நம்பிவிடாதீர்கள்: மின்னஞ்சலில் கூறப்பட்டவற்றின் நோக்கத்தைக் கேள்விக்குட்படுத்துங்கள்.
- ஒரு தெரிந்த நபரிடமிருந்து ஓர் இணைப்புடன் கூடிய சந்தேகத்துக்குரிய ஒரு மின்னஞ்சலை நீங்கள் பெறும்போது அந்த நபருக்கு அழைத்தோ அல்லது மின்னஞ்சல் செய்தோ அந்தச் செய்தி உண்மையானதா என்பதை உறுதிசெய்யுங்கள். ஒரு சந்தேகத்துக்குரிய மின்னஞ்சலுக்கு நேரடியாக பதில் அனுப்பாதீர்கள்.
- ஓர் இணைப்பில் உள்ள எழுத்துப்பிழைகள் அல்லது தவறான தளப்பெயர் (உதாரணமாக, ஒரு முகவரி ".com" என முடிவதற்குப் பதில் ".gov" என முடிவது) ஆகியவற்றை சோதியுங்கள்.
- உலாவியின் முகவரிப் பட்டையில் "https" என இருப்பதாலோ அல்லது பூட்டு அடையாளப்படம் இருப்பதனாலோ ஒரு இணையதளத்தை நம்பிவிடாதீர்கள்.

6. அதிமுக்கிய தகவல்களை அணுகுவதை தவிர்க்கவும்.

உங்களிடம் ஒரு VPN இருந்தாலும் தனிப்பட்ட வங்கிக் கணக்குகள் அல்லது அதுபோன்ற சமூக பாதுகாப்பு எண்கள் ஆகிய அதிமுக்கிய தனிப்பட்ட தரவுகளை பாதுகாப்பற்ற பொது வலைத்தொடர்பில் அணுகுவதை தவிர்க்கவும். பொதுவில் உள்ள பாதுகாக்கப்பட்ட வலைத்தொடர்பும் அபாயகரமானதாக இருக்கக்கூடும். பொது வை-ஃபையில் இந்தக் கணக்குகளை நீங்கள் அணுகவேண்டியிருந்தால் சிந்தித்துச் செயல்படுங்கள். மாறாக, நிதி பரிவர்த்தனைகளுக்கு உங்கள் பல்திறன்பேசியின் ஹாட்ஸ்பாட் செயல்பாட்டைப் பயன்படுத்துவது நல்லது.

7. பாதுகாப்பானதும் பாதுகாப்பற்றதும்.

அடிப்படையில் இருவிதமான பொது வை-ஃபை இணையத்தொடர்புகள் உள்ளன: பாதுகாப்பானது மற்றும் பாதுகாப்பற்றது.

முடிந்தபோதெல்லாம் பாதுகாப்பான பொது இணையத்தொடர்பைப் பயன்படுத்துங்கள். எந்தவகையான கடவுச்சொல்லோ அல்லது உள்நுழைவு போன்ற பாதுகாப்பு அம்சம் தேவைப்படாதபோது பாதுகாப்பில்லாத வலைத்தொடர்பில் இணைக்கலாம். ஒரு பாதுகாப்பான வலைத்தொடர்புக்கு வலைத்தொடர்பில் இணைவதற்குமுன் பொதுவாக விதிமுறைகள் மற்றும் நிபந்தனைகளுக்கு ஒரு பயனரின் ஒப்புதல், ஒரு கணக்கை பதிவுசெய்தல் அல்லது ஒரு கடவுச்சொல்லை தட்டச்சிடுதல் போன்றவை தேவைப்படும்.

8. உங்கள் ஃபயர்வாலை செயல்பாட்டில் வைத்திருங்கள்.

நீங்கள் ஒரு மடிக்கணினியைப் பயன்படுத்துவதாயிருந்தால், பொது வை-ஃபை உபயோகிக்கும்போது உங்கள் ஃபயர்வாலை செயலில் வைத்திருங்கள். ஒரு ஃபயர்வால் உங்கள் சாதனத்தை தீம்பொருள் அச்சுறுத்தல்களுக்கு தடை ஏற்படுத்தி காக்கிறது. பாப்-அப்கள் மற்றும் அறிவிப்புகளின் காரணமாக பயனர்கள் Windows ஃபயர்வாலை முடக்கிவிட்டு பின்னர் அப்படியே மறந்துபோயிருக்கக் கூடும். ஒரு கணினியில் அதை மீண்டும் தொடங்குவதற்கு, கட்டுப்பாட்டு பலகைக்குச் சென்று “பாதுகாப்பு மற்றும் தனியுரிமை"க்குள் போய் “Windows ஃபயர்வால்” தேர்வுசெய்யவும். நீங்கள் ஒரு Mac கணினி பயன்படுத்துபவர் எனில், இந்த அம்சத்தை இயக்க “கணினி விருப்பத்தேர்வுகள்” சென்று, “பாதுகாப்பு மற்றும் தனியுரிமை”க்குள் “ஃபயர்வால்” தாவலுக்குச் செல்லவும்.

9. நச்சுநிரல் தடுப்பானைப் பயன்படுத்துதல்.

மேலும் உங்கள் மடிக்கணினியில் நச்சு நிரல் தடுப்பானின் சமீபத்திய பதிப்பைப் பயன்படுத்துவதை உறுதிசெய்யுங்கள். நச்சு நிரல் எதிர்ப்பான்கள் நீங்கள் பகிரத்தக்க பொது வை-ஃபை பயன்படுத்தும்போது உங்கள் கணினிக்குள் நுழையக்கூடிய தீம்பொருட்களைக் கண்டறிந்து பாதுகாக்க உதவும். அறியப்பட்ட நச்சு நிரல்கள் உங்கள் சாதனத்தில் சேரும்போது அல்லது ஏதேனும் சந்தேகத்துக்குரிய நடவடிக்கை, தாக்குதல் அல்லது உங்கள் கணினியில் தீம்பொருள் நுழைந்துவிட்டால் எச்சரிக்கை அறிவிப்பு மூலம் உங்களுக்கு தெரியப்படுத்தப்படும்.

10. இரு காரணி அல்லது பல காரணி உறுதிப்பாட்டைப் பயன்படுத்தவும்.

உங்கள் தனிப்பட்ட தகவல்களோடு இணையதளங்களில் நுழையும்போது பலகாரணி உறுதிப்பாட்டை (MFA) பயன்படுத்தவும். இதன் அர்த்தம் உங்களுக்கு மேலும் பாதுகாப்பளிக்கக்கூடிய இரண்டாவது சரிபார்ப்பு குறியீட்டை (உங்கள் செல்பேசிக்கு செய்தி அனுப்பப்படுதல் அல்லது ஒரு செயலிமூலம் வழங்கப்படுதல் அல்லது ஸ்தூலமான சாவி) கொண்டிருப்பதாகும். ஒரு தகவல் திருடர் உங்கள் பயனர்பெயரையும் கடவுச்சொல்லையும் பயன்படுத்தினாலும் அவர்களால் உங்கள் கணக்குகளை உறுதிப்படுத்தும் குறியீடு இல்லாமல் அணுக இயலாது.

11. உங்கள் தனிப்பட்ட சாதனங்கள்மீது கவனம்.

உங்கள் மடிக்கணினி, டேப்லட் அல்லது பல்திறன்பேசியை ஒரு பொது இடத்தில் அல்லது வாகனத்தில் கவனிக்காமல் விடாதீர்கள். ஒரு வை-ஃபை இணையத்தொடர்பில் நீங்கள் முன்னெச்சரிக்கைகளை மேற்கொண்டாலும் அது ஒருவரை உங்கள் உடைமையை எடுப்பதையோ அல்லது உங்கள் தகவல்களை ஒளிந்திருந்து பார்ப்பதையோ தடுப்பதில்லை. உங்கள் சுற்றுப்புறத்தில் கவனமும் உங்களைச் சுற்றியிருப்பவர்களிடம் கவனமும் கொள்ளுங்கள்.

12. பிற இணைய பாதுகாப்பு உதவிக்குறிப்புகள்.

இணையத்தில் குறிப்பாக ஒரு பொது வை-ஃபை இணைப்பை நீங்கள் உபயோகிக்கும்போது பாதுகாப்பாக இருக்க இதோ சில உதவிக்குறிப்புகள்:

- வலுவான கடவுச்சொல்லை பயன்படுத்துங்கள்.
- உங்கள் சாதனங்களை குறியாக்கம் செய்யவும்.
- ஏமாற்று மின்னஞ்சல்களிடம் எச்சரிக்கையாக இருங்கள்.
- சமூக ஊடகத்தில் நீங்கள் என்ன பதிவிடுகிறீர்கள் என்பதில் கவனம் கொள்ளுங்கள். பல தனிப்பட்ட விபரங்கள் தகவல் திருடர்களுக்கு கடவுச்சொற்களை ஊகிக்க உதவக்கூடும்.
- இனி தேவையிராத பழைய தகவல்களை அழித்துவிடுங்கள்.
- ஒரு இணையத்தொடர்பு ஏதேனும் கூடுதல் மென்பொருளை அல்லது உலாவி நீட்டிப்புகளை நிறுவச்சொன்னால் அதில் இணைக்கவேண்டாம்.
- தெரிந்த சிக்கல்களிலிருந்து உங்கள் சாதனங்களைக் காக்க சமீபத்திய ஒட்டுக்களும் புதுப்பித்தல்களும் நிறுவப்பட்டிருப்பதை உறுதிசெய்யுங்கள்.