

இன்றுமுதல் ஒன்பது இன்றியமையாத சைபர் பாதுகாப்பு பழக்கங்களை நாம் அனைவரும் பின்பற்ற வேண்டும்



1. நீங்கள் கிளிக் செய்வதற்கு முன் இடைநிறுத்தவும்!

இணைப்புகளைக் கிளிக் செய்வதற்கு முன் அல்லது இணைப்புகளைத் திறப்பதற்கு முன், அவை உங்களுக்குத் தெரிந்த ஒருவரிடமிருந்து வந்ததாகத் தோன்றினாலும், இருமுறை யோசியுங்கள்.

- தெரியாத இணைப்புகளைக் கிளிக் செய்வதற்குப் பதிலாக அறியப்பட்ட, முறையான வழியாக எப்போதும் இணையதளங்களுக்குச் செல்லவும் (உதாரணம்: HTTPS)
- இணைப்பு எதிர்பாராததாகத் தோன்றினால், நம்பகமான முறை மூலம் அனுப்புநருடன் உறுதிப்படுத்தவும் அல்லது இணைப்புகளைக் கிளிக் செய்யாதல் இருப்பது பாதுகாப்பானது.



2. தனிப்பட்ட தகவலுக்கான கோரிக்கைகளை சரிபார்க்கவும்

தனிப்பட்ட தரவுக்கான கோரிக்கைகளை எப்போதும் உறுதிப்படுத்தவும்—அது உங்களுடையதாக இருந்தாலும் அல்லது வேறொருவருடையதாக இருந்தாலும் சரி.

- மோசடி செய்பவர்கள், நம்பகமான தொடர்புகள் என்கிற போர்வையில் ஆள்மாறாட்டம் செய்யலாம்.
- தங்களது வங்கி கணக்கு அறிக்கைகள் மற்றும் கடன் அறிக்கைகளை தவறாமல் மதிப்பாய்வு செய்யவும்.
- பல ஃபிஷிங் செய்திகளில் எழுத்துப்பிழை மற்றும் இலக்கணப் பிழைகள் இருக்கும்.
- கோரிக்கை முறையானதா என்பதைக் கவனியுங்கள். நபருக்கோ நிறுவனத்திற்கோ அந்தத் தகவல் தேவைப்படுமா என்பதையும் கவனியுங்கள்?



3. உங்கள் கடவுச்சொற்களை பாதுகாக்கவும்

வலுவான, சிக்கலான கடவுச்சொற்களை உருவாக்குதல் மற்றும் அவற்றை புத்திசாலித்தனமாக நிர்வகிப்பது உங்கள் கணக்குகளைப் பாதுகாப்பாக வைத்திருக்க உதவும்.

- வெவ்வேறு கணக்குகளுக்கு தனித்தனி கடவுச்சொற்களைப் பயன்படுத்தவும்.
- பணி மற்றும் தனிப்பட்ட கடவுச்சொற்களை தனித்தனியாக வைத்திருங்கள்.
- கடவுச்சொற்களை ஒருபோதும் எவருடனும் பகிர வேண்டாம்.
- கடவுச்சொல்லை அடிக்கடி மாற்றவும்.
- உலாவிகளில்(Browser) கடவுச்சொற்களைச் சேமிப்பதை தவிர்க்கவும்.
- கூடுதல் பாதுகாப்புக்காக பல காரணி அங்கீகாரத்தை (MFA) பயன்படுத்தவும்.



4. உங்கள் சாதனங்களைப் பாதுகாக்கவும்

உங்கள் பணியிடத்தைப் பூட்டிவதன்(Lock) மூலம் உங்கள் சாதனங்களை நீங்கள் வெளியேறும் போது பாதுகாக்க முடியும்..

- எப்போதும் உங்கள் கணினித் திரையைப் பூட்டவும்.
- உங்கள் ஃபோன் மற்றும் கையடக்க சாதனங்களை உங்களுடன் எடுத்துச் செல்லவும் அல்லது அவற்றைப் முறையாக பாதுகாக்கவும்.
- எப்போதும் போதெல்லாம் வலுவான அங்கீகார முறைகளைப் பயன்படுத்தவும்.



5. முக்கியமான கோப்புகளை காப்புப் பிரதி எடுக்கவும்

உங்கள் முக்கியமான தரவுகள் தொடர்ந்து காப்புப் பிரதி எடுக்கப்படுவதை உறுதிசெய்யவும்.

- காப்புப்பிரதிகளை அசலில் இருந்து வேறு ஒரு தனி இடத்தில் சேமிக்கவும்.
- நிறுவனத்தால் அங்கீகரிக்கப்பட்ட சேமிப்பக தீர்வுகளைப் பயன்படுத்தவும்.
- காப்புப்பிரதிகள் சரியாகச் செயல்படுவதை உறுதிசெய்ய, அவற்றைத் தொடர்ந்து சோதிக்கவும்.



6. சந்தேகத்திற்கிடமான செயல்பாடுகளை புகாரளிக்கவும்

ஏதேனும் சந்தேகத்திற்குரியதாகத் தோன்றினால், உங்கள் உள்ளுணர்வை நம்புங்கள்— சந்தேகத்திற்குரியவைகளை புகாரளிக்கவும்!

- சந்தேகத்திற்குரிய மோசடிகள் அல்லது சந்தேகத்திற்கிடமான செயல்களுக்கு உங்கள் மேற்பார்வையாளரை எச்சரித்து, உங்கள் நிறுவனத்தின் அறிக்கையிடல் நெறிமுறையைப் பின்பற்றவும்.



7. நீங்களும் சுற்று மற்றவர்களுக்கும் சுற்பிக்கவும்

சமீபத்திய இணைய பாதுகாப்பு அச்சுறுத்தல்கள் மற்றும் போக்குகள் குறித்து தொடர்ந்து அறிந்திருங்கள்.

- பயிற்சி அமர்வுகளில் கலந்து கொள்ளுங்கள் மற்றும் உங்களுக்கு வாய்ப்பு கிடைக்கும் போது சக ஊழியர்களுடன் பகிர்ந்து கொள்ளுங்கள்.
- பாதுகாப்பு நெறிமுறைகளை நன்கு அறிந்த குழு அச்சுறுத்தல்களுக்கு எதிரான பாதுகாப்பில் முன்னிறுந்து போராடும்.



8. பாதுகாப்பான நெட்வொர்க்குகளைப் பயன்படுத்தவும்

எப்போதும் பாதுகாப்பான

நெட்வொர்க்குகளுடன் இணைக்கவும், குறிப்பாக முக்கியமான தகவல்களை அணுகும் போது.

- நிதி பரிவர்த்தனைகள் அல்லது முக்கியமான வேலைகளுக்கு பொது வைஃபையைத் தவிர்க்கவும்.
- கூடுதல் பாதுகாப்பிற்கு தேவையான போது மெய்நிகர் தனியார் நெட்வொர்க்கை (VPN) பயன்படுத்தவும்.



9. சமூக ஊடகங்களில் எச்சரிக்கையாக இருங்கள்

ஆன்லைனில் நீங்கள் பகிரும் தனிப்பட்ட தகவல்களின் அளவைக் கட்டுப்படுத்துங்கள். நீங்கள் உங்கள் தனியுரிமையைப் பாதுகாக்கலாம், உங்கள் பாதுகாப்பை மேம்படுத்தலாம் மற்றும் மேலும் நேர்மறையான ஆன்லைன் அனுபவத்தை உருவாக்கலாம்.

- சமூக ஊடக தளங்களில் தனியுரிமை அமைப்புகளை மதிப்பாய்வு செய்யவும்.
- நண்பர் கோரிக்கைகள் மற்றும் உங்கள் தகவலை அணுகக்கூடியவர்கள் குறித்து கவனமாக இருங்கள் பூட்டப்பட்ட சுயவிவரத்திலிருந்து கோரிக்கைகளை ஏற்க வேண்டாம்.
- சாத்தியமான அபாயங்களைக் குறைக்க உங்கள் ஆன்லைன் இருப்பை தவறாமல் தணிக்கை செய்யுங்கள்.

நினைவில் கொள்ளுங்கள்: சைபர் பாதுகாப்பு என்பது
அனைவரின் பொறுப்பு!