Grassroots Digital Hub

சைபர் பாதுகாப்பு (Cybersecurity) குறிப்புகள்

1.உங்கள் சாதனத்தை பாதுகாக்க

- **உங்கள் சாதனத்தை பாதுகாக்க** உங்கள் கைபேசி, லேப்டாப் அல்லது பிற சாதனங்களுக்கு கடவுச்சொல்லை (password) பயன்படுத்துங்கள்.
    - இது உங்கள் சாதனம் தொலைந்து போனாலோ அல்லது திருடப்பட்டாலோ அதைப் பாதுகாக்கும்.
- **உங்கள் தரவுகளை காப்புப்பிரதி சேமிப்பு (Backup) எடுக்கவும்.** பெரும்பாலான சாதனங்களில் இலவச காப்புப்பிரதி சேமிப்பு (Backup) வசதி வழங்கப்படுகிறது. இடம் (Space) குறைவாக இருக்கலாம். காப்புப்பிரதி சேமிப்பு (Backup) எவ்வாறு செய்யலாம் என்பதை கற்றுக்கொள்ளுங்கள். WikiHow.
    - காப்புப்பிரதி சேமிப்பு (Backup) என்பது உங்கள் சாதனத்தில் உள்ள அனைத்திற்குமான நகல் (Copy) ஆகும். உங்கள் சாதனம் இழக்கப்பட்டால் அல்லது கெட்டுப்போனால், அந்த தரவுகளை பேக் அப்பில் இருந்து மீட்டெடுக்கலாம்.
    - காப்புப்பிரதி சேமிப்பு (Backup) கள் உங்கள் சாதனத்திற்கு அப்பால் உள்ள இடத்தில் சேமிக்கப்படும், பெரும்பாலும் கிளவுட் (Cloud) இல். காப்புப்பிரதிகள் (Backup) உங்கள் சாதனத்தைத் தவிர வேறு இடத்தில் சேமிக்கப்படும், பொதுவாக கிளவுட் (Cloud). கிளவுட்(Cloud) என்பது கூகிள் (Google) போன்ற நிறுவனங்களால் நடத்தப்படும் கணினிகளின் வலையமைப்பாகும்
- **மென்பொருள் (software) ஆவண பாதுகாப்பு செய்யுங்கள** பல ஆவண பாதுகாப்பை மேம்படுத்துகின்றன.

SSHRC CRSH
Social Sciences and Humanities Research Council of Canada
Conseil de recherches en sciences humaines du Canada
NSERC CRSNG
We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council.

- **வெளியேறு (Log out).** ஒரு செயலி (Apps)அல்லது வலைத்தளத்தில் நீங்கள் முடித்ததும், அதிக பாதுகாப்பிற்காக வெளியேறு.

2. கடவுச்சொற்களை (Passwords) கவனமாக வைத்திருங்கள்.

- **நீண்ட கடவுச்சொற்களைப் பயன்படுத்தவும் (passwords).**
    - பெரிய மற்றும் சிறிய எழுத்துக்கள், எண்கள் மற்றும் சின்னங்களைப் பயன்படுத்தவும்.
    - நீங்கள் நினைவில் வைத்திருக்கும் சொற்றொடர்களை உருவாக்குங்கள்: 2-H@ppy-Small-Kids&Me
- **ஒவ்வொரு கணக்கிற்கும் வெவ்வேறு கடவுச்சொல்லைப் (password) பயன்படுத்த முயற்சிக்கவும்.**
- **கடவுச்சொல் (password) நிர்வாகியைப் பயன்படுத்தவும்.** இது அனைத்து கடவுச்சொற்களுக்கும் (passwords) உதவும்!
    - சில இணையதளங்கள் ஃபயர்பாக்ஸ் (Firefox) மற்றும் குரோம் (Chrome) போன்ற அல்லது விண்டோஸ் (Windows) போன்ற இயக்க முறைமைகள் இலவச கடவுச்சொல் (password) நிர்வாகத்தை வழங்குகின்றன.
- **சில கடவுச்சொல் (password) நிர்வாகிகளால் இரண்டு-காரணி அங்கீகாரம் வழங்கப்படுகிறது.** இதன் பொருள் உள்நுழைவதற்கு (Logging) இரண்டு படிகள் ஆகும், இது அதிக நேரம் எடுக்கும் ஆனால் மிகவும் பாதுகாப்பானது.

3. உங்கள் இணைப்பை கவனமாக வைத்திருங்கள்.

- உங்களிடம் **வீட்டு இணைய நெட்வொர்க் (Internet) இணைப்பு** இருந்தால், கடவுச்சொல் (password) உள்ளவர்கள் மட்டுமே அதை அணுகக்கூடிய வகையில் வலுவான கடவுச்சொல்லைப் (Password) பயன்படுத்தவும்.
- நீங்கள் **இலவச அல்லது பொது வைஃபையைப் (Wi-Fi)** பயன்படுத்தினால்:

- VPN ஐப் பயன்படுத்தவும். ProtonVPN போன்ற இலவச VPNகள் உள்ளன.
- ஒரு VPN இணைப்பை குறியாக்கம் செய்யும் (தனிப்பட்டதாக்கும்), இது உங்கள் சாதனத்தை வைரஸ்களிலிருந்தும் உங்கள் தரவு திருடப்படுவதிலிருந்தும் பாதுகாக்கிறது.

4.உங்கள் தனியுரிமையைக் கட்டுப்படுத்துங்கள்

உங்கள் தரவு - நீங்கள் ஆன்லைனில் என்ன செய்கிறீர்கள், பார்க்கிறீர்கள் மற்றும் வாங்குகிறீர்கள் என்பது பற்றிய தகவல்கள் - மிகவும் மதிப்புமிக்கவை, ஆனால் நிறுவனங்கள் அதற்கு உங்களுக்கு பணம் கொடுக்க விரும்பவில்லை.

- **அமைப்புகள்:** சாதனங்கள், வலைத்தளங்கள் மற்றும் பெரும்பாலான பயன்பாடுகள் உங்கள் தரவைப் பாதுகாக்க முடியும், ஆனால் நீங்கள் இதை அமைக்க வேண்டும்.
  - தேடலுக்குச் செல்லுங்கள் "setting"சாதனம் அல்லது செயலியில் (Google, Instagram, ChatGPT போன்றவை) "அமைப்புகள்" அல்லது "தனியுரிமை" உள்ளதா எனப் பாருங்கள்.
  - மேலும் உதவிக்கு, பயன்பாடு அல்லது சாதனத்தின் பெயரையும் "தனியுரிமையை எவ்வாறு அமைப்பது" என்பதையும் தேடுங்கள்.
- **வரலாறு:** உங்கள் இணைய உலாவி மற்றும் AI கணக்கில் "வரலாற்றை அழிக்க" முடியும்.
- **குக்கீகள் (Cookies):** ஒரு வலைத்தளம் "குக்கீகளை (Cookies) அனுமதி" என்று கேட்கும்போது, "தேவையானதை மட்டும் ஏற்றுக்கொள்" என்பதைத் தேர்ந்தெடுக்கவும் அல்லது "விளம்பரப்படுத்துதல்" அல்லது "இலக்கு" என்பதைத் தேர்வுநீக்கவும்.
- **சமூக ஊடகங்கள்:** உங்கள் சமூக ஊடகக் கணக்கை யார் பார்க்க வேண்டும் என்று நீங்கள் விரும்புகிறீர்கள் என்று சிந்தியுங்கள். உங்களுடன் இணைய முயற்சிக்கும் ஒரு அந்நியன் உங்கள் தரவைச் (Data) சேகரிக்கும் ஒரு பாட் ஆக இருக்கலாம்.
- **கிரெடிட் கார்டுகள்:** வலைத்தளங்களில் கிரெடிட் கார்டு தகவல்களைச் சேமிப்பதைத் தவிர்க்கவும்.

5. ஒன்றாகப் பாதுகாப்பாக இருப்போம்

- **கிளிக் பெய்ட் (Bait):** உங்களை வருத்தப்படுத்தும் ஒன்றை நீங்கள் கண்டால், நிறுத்தி ஆழ்ந்த மூச்சை எடுங்கள். இது உங்களை இடுகையிட/பகிர/மேலும் படிக்க வைக்க வடிவமைக்கப்பட்ட ஒரு தந்திரமாக இருக்கலாம்.
- **பகிர்வதற்கு முன்:**
  - நீங்கள் பகிரும் இணைப்புகள் பாதுகாப்பானவை என்பதை உறுதிப்படுத்திக் கொள்ளுங்கள்.
  - நீங்கள் பகிரும் தகவல் உண்மையானது என்பதை உறுதிப்படுத்திக் கொள்ளுங்கள்.
  - மற்றவர்கள் ஆர்வமுள்ள இணைப்பு அல்லது இடுகையைக் காணக்கூடும் என்பதற்கான காரணத்தை தெளிவாகக் கூறுங்கள்.
- **நண்பர்கள் மற்றும் குடும்பத்தினரிடம் கேளுங்கள்**
  - அவர்களின் தகவல்களையும் புகைப்படங்களையும் பகிர்ந்து கொள்வது உங்களுக்கு சரியென்றால்.
  - மரியாதைக்குரியவர்களாக உணரவும், மரியாதைக்குரியவர்களாகவும் இருக்க அவர்கள் ஆன்லைனில் என்னென்ன நடவடிக்கைகளை எடுக்கிறார்கள்.

மேலும் தகவலுக்கு

- GetCyberSafe.ca – உங்கள் அடையாளத்தைப் பாதுகாப்பாக வைத்திருப்பதற்கான உதவிக்குறிப்புகள், ஆன்லைன் மோசடிகள் மற்றும் பல, கனடா அரசு உதவி செய்கிறது.
- SecurityPlanner.ConsumerReports.org – இந்த தளம் உங்கள் ஆன்லைன் தகவல்களை எவ்வாறு பாதுகாப்பாக வைத்திருப்பது என்பதைக் காட்டுகிறது. முதலில் கனடாவில் உருவாக்கப்பட்டது, இப்போது இது ஒரு அமெரிக்க இலாப நோக்கற்ற (Non-profit) நிறுவனத்தால் நடத்தப்படுகிறது.