सायबर सुरक्षेकरिता ह्या नऊ अत्यावश्यक सवयी आजच अंगीकारा

1. क्लिक करण्यापूर्वी थोडा विराम घ्या

संलग्नक उघडण्याच्या लिंकवर क्लिक करण्यापूर्वी दोनदा विचार करा, ते तुमच्या ओळखीच्या व्यक्तीकडून आलेले दिसत असले तरीही.

- कुठल्याही अज्ञात लिंकवर क्लिक करण्याएवजी नेहमी कायदेशीर स्रोताद्वारे (उदा. HTTPS) परिक्षीत वेबसाइटवर नेव्हिगेट करा.
- अटॅचमेंट अनपेक्षित वाटल्यास, विश्वसनीय पद्धतीद्वारे प्रेषकाकडून पुष्टी करा अथवा सुरक्षिततेसाठी क्लिक करण्यास टाळा.

2. वैयक्तिक माहितीसाठी विनंती सत्यापित करा

खाजगी वा वैयक्तिक माहितीसाठी विनंत्यांची नेहमी पुष्टी करा—मग ती तुमची असो किंवा इतर कोणाचीही.

- स्कॅमर तुमच्या विश्वसनीय संपर्काची सहजपणे तोतयागिरी करू शकतात.
- असामान्य क्रियाकलापांसाठी नियमितपणे आर्थिक नोंदी आणि क्रेडिट रिपोर्टचे पुनरावलोकन करा.
- अनेक फिशिंग संदेशांमध्ये स्पेलिंग आणि व्याकरणाच्या चुका असतात.
- विनंती वैध आहे की नाही? व्यक्ती किंवा संस्थेला त्या माहितीची आवश्यकता असण्याची शक्यता आहे का? याचा विचार करा.

3. तुमचे पासवर्ड नियंत्रित करा

तुमची खाती सुरक्षित ठेवण्यासाठी मजबूत, जटिल पासवर्ड तयार करणे आणि त्यांचा हुशारीने व्यवस्थापन करणे आवश्यक आहे.

- विविध खात्यांसाठी अद्वितीय पासवर्ड वापरा.
- कार्य आणि वैयक्तिक पासवर्ड वेगळे ठेवा.
- पासवर्ड कधीही शेअर करू नका.
- पासवर्ड वारंवार बदला.
- ब्राउझरमध्ये पासवर्ड जतन करणे बंद करा.
- सुरक्षिततेसाठी मल्टी-फॅक्टर ऑथेंटिकेशन (MFA) सक्षम करा.

4. तुमची उपकरणे सुरक्षित करा

तुमचे वर्कस्पेस लॉक करा आणि दूर जाताना तुमचे डिव्हाइस सुरक्षित करा.

- तुमची संगणक स्क्रीन नेहमी लॉक करा.
- तुमचा फोन आणि पोर्टेबल डिव्हाइस तुमच्यासोबत घ्या किंवा सुरक्षितपणे ठेवा.
- जेव्हा शक्य असेल तेव्हा मजबूत प्रमाणीकरण पद्धती वापरा.

5. महत्त्वाच्या फाइल्सचा बॅकअप घ्या

तुमचा महत्वाचा नियमितपणे बॅकअप केला जात असल्याची खात्री करा.

- बॅकअप मूळस्थानापासून वेगळ्या ठिकाणी स्टोर करा.
- संस्थेद्वारे मंजूर स्टोरेज सोल्यूशन्सचा वापर करा.
- ते योग्यरित्या कार्य करतात याची खात्री करण्यासाठी नियमितपणे बॅकअपची चाचणी घ्या.

6. संशयास्पद क्रियाकलाप नोंदवा

काहीतरी संशयास्पद वाटत असल्यास, तुमच्या अंतःकरणावर विश्वास ठेवा—त्याची तक्रार करा!

- तुमच्या पर्यवेक्षकाला सतर्क करा आणि संशयित स्कॅमर किंवा संशयास्पद क्रियाकलापांसाठी तुमच्या संस्थेच्या रिपोर्टिंग पद्धतीचे अनुसरण करा.

7. स्वतःला आणि इतरांना शिक्षित करा

नवीनतम सायबर सुरक्षा धोके आणि प्रचलणबद्दल माहिती मिळवा.

- प्रशिक्षण सत्रांना उपस्थित राहा आणि जेव्हा तुम्हाला संधी मिळेल तेव्हा सहकाऱ्यांसोबत ज्ञानाची देवाण घेवाण करा.
- एक चांगली माहिती असलेली टीम ही तुमची सायबर धोक्यांपासून बचावाची पहिली पायरी आहे.

8. सुरक्षित नेटवर्क वापरा

नेहमी सुरक्षित नेटवर्कच्या सम्पर्कात रहा, विशेषत: संवेदनशील माहितीची देवाण-घेवाण करताना.

- आर्थिक व्यवहार किंवा संवेदनशील कामासाठी सार्वजनिक वाय-फाय टाळा.
- अतिरिक्त संरक्षणासाठी आवश्यक असेल तेव्हा वर्च्युअल प्रायव्हेट नेटवर्क(VPN) वापरा.

9. सोशल मीडियाबाबत सावध रहा

तुम्ही ऑनलाइन शेअर करत असलेल्या वैयक्तिक माहितीचे प्रमाण मर्यादित करा. त्यामुळे तुम्ही तुमच्या गोपनीयतेचे रक्षण करू शकता, तुमची सुरक्षितता वाढवू शकता आणि अधिक सकारात्मक ऑनलाइन अनुभव घेऊ शकता

- सोशल मीडिया प्लॅटफॉर्मवर गोपनीयता सेटिंगचे पुनरावलोकन करा.
- मैत्रीच्या विनंत्या आणि तुमची माहिती कोणाकडे आहे याची काळजी घ्या. लॉक केलेल्या प्रोफाइलच्या विनंत्या स्वीकारू नका.
- संभाव्य धोके कमी करण्यासाठी तुमच्या ऑनलाइन उपस्थितीची नियमितपणे तपासणी करा.

लक्षात ठेवा: सायबर सुरक्षा ही प्रत्येकाची जबाबदारी आहे!