आज से अपनाई जाने वाली नौ आवश्यक साइबर सुरक्षा आदतें

1. क्लिक करने से पहले रुकें!

लिंक पर क्लिक करने या अटैचमेंट खोलने से पहले दो बार सोचें, भले ही वह आपके जानकार व्यक्ति द्वारा भेजा गया हों।

- अज्ञात लिंक पर क्लिक करने के बजाय हमेशा ज्ञात, वैध स्रोत (जैसे एचटीटीपीएस) के माध्यम से वेबसाइटों पर जाएँ।
- यदि कोई अटैचमेंट अप्रत्याशित लगता है, तो किसी विश्वसनीय पद्धति से प्रेषक से पुष्टि करें या सुरक्षित रहने के लिए क्लिक न करने का विकल्प चुनें।

2. व्यक्तिगत जानकारी के लिए अनुरोधों को सत्यापित करें!

निजी डेटा के अनुरोध की हमेशा पुष्टि करें – चाहे वह आपका हो या किसी और का।

- स्कैमर्स आसानी से विश्वसनीय सम्पर्कों का प्रतिरूपण कर सकते हैं।
- असामान्य गतिविधि के लिए वित्तीय विवरणों और क्रेडिट रिपोर्ट की नियमित समीक्षा करें।
- फ़िशिंग संदेशों में अधिकतर वर्तनी और व्याकरण संबंधी त्रुटियाँ होती हैं।
- इस बात पर विचार करें कि क्या अनुरोध वैध है। क्या व्यक्ति या संगठन को उस जानकारी की आवश्यकता है?

3. अपने पासवर्ड पर नियंत्रण रखें

अपने खातों को सुरक्षित रखने के लिए मजबूत एवं जटिल पासवर्ड बनाना तथा उनका समझदारी से प्रबंधन करना आवश्यक है।

- अलग-अलग खातों के लिए अलग-अलग पासवर्ड का उपयोग करें।
- कार्यस्थल और व्यक्तिगत पासवर्ड अलग रखें।
- पासवर्ड कभी साझा न करें ।
- पासवर्ड नियमित रूप से बदलें ।
- ब्राउज़र में पासवर्ड सेव ना करें ।
- अतिरिक्त सुरक्षा के लिए मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) सक्षम करें।

4. अपने डिवाइस सुरक्षित रखें

बाहर जाते समय अपने कार्यस्थल को लॉक कर दें और अपने डिवाइस को सुरक्षित रखें।

- अपने कंप्यूटर स्क्रीन को हमेशा लॉक रखें।
- अपने फोन और पोर्टेबल डिवाइस को अपने साथ ले जाएं या उन्हें सुरक्षित स्थान पर रखें।
- जब भी संभव हो, सशक्त प्रमाणीकरण विधियों का उपयोग करें।

5. महत्वपूर्ण फ़ाइलों का बैकअप लें

सुनिश्चित करें, कि आप नियमित रूप से महत्वपूर्ण डेटा का बैकअप ले रहें है।

- बैकअप को मूल प्रति से अलग स्थान पर संग्रहित करें।
- संगठन द्वारा अनुमोदित भंडारण समाधानों का उपयोग करें।
- बैकअप सही तरीके से कार्य कर रहा है कि नही, यह सुनिश्चित करने के लिए, नियमित रूप से बैकअप का परीक्षण करें।

6. संदिग्ध गतिविधि की रिपोर्ट करें

यदि कुछ संदिग्ध लगे, तो अपनी मूल प्रवृत्ति पर भरोसा करें - इसकी रिपोर्ट करें!

- संदिग्ध घोटालों (स्कैम) या संदिग्ध गतिविधियों के लिए अपने पर्यवेक्षक को सचेत करें और अपने संगठन के रिपोर्टिंग प्रोटोकॉल का पालन करें।

7. स्वयं को और दूसरों को जागरूक करें

. नवीनतम साइबर सुरक्षा खतरों और प्रवृत्तियों से अवगत रहें।

- जब भी आपको अवसर मिले, प्रशिक्षण सत्रों में भाग लें और सहकर्मियों के साथ जानकारी साझा करें।
- एक सुविज्ञ टीम साइबर खतरे के विरुद्ध आपकी पहली रक्षा पंक्ति है ।

8. सुरक्षित नेटवर्क का उपयोग करें

हमेशा सुरक्षित नेटवर्क से कनेक्ट रहें, विशेषकर संवेदनशील जानकारी को एक्सेस करते समय।

- वित्तीय लेनदेन या संवेदनशील कार्य के लिए सार्वजनिक वाई-फाई का उपयोग करने से बचें।
- अतिरिक्त सुरक्षा के लिए आवश्यक होने पर वर्चुअल प्राइवेट नेटवर्क (वीपीएन) का उपयोग करें।

9. सोशल मीडिया से सावधान रहें

अपनी गोपनीयता की रक्षा करने के लिए, अपनी सुरक्षा बढ़ाने के लिए तथा अधिक सकारात्मक ऑनलाइन अनुभव बनाने के लिए, ऑनलाइन साझा की जाने वाली व्यक्तिगत जानकारी को सीमित मात्रा में रखें ताकि आपकी जानकारी गोपनीय रहें, आपकी सुरक्षा बढ़ सके और आपका ऑनलाइन अनुभव अधिक सकारात्मक रहें ।

- सोशल मीडिया प्लेटफॉर्म पर गोपनीयता सेटिंग्स की समीक्षा करें।
- मित्र अनुरोधों और आपकी जानकारी तक किसकी पहुंच है, इसके प्रति सावधान रहें; लॉक किए गए प्रोफाइल से अनुरोध स्वीकार न करें।
- संभावित जोखिमों को कम करने के लिए अपनी ऑनलाइन उपस्थिति का नियमित रूप से ऑडिट करें।

याद रखें: साइबर सुरक्षा हम सबकी जिम्मेदारी है!