भाग्यलक्ष्मी बँक

दि भाग्यलक्ष्मी महिला सहकारी बँक लि., नांदेड

मुख्य कार्यालय : "भाग्यलक्ष्मी भवन" महावीर चौक, नांदेड

सायबर जागरुकता

दैनंदिन जीवनात ज्याप्रमाणे आपण खाण्याच्या बाबतीत (Food Hygine) आपल्या शारिरीक स्वच्छते बाबत (Health Hygine) पाळतो, त्याचप्रमाणे सायबर विश्वात वावरतांना देखील जागरूक (Cyber Hygine) राहणे आवश्यक आहे.

दैनंदिन कामकाजात तंत्रज्ञानाचा वापर करतांना घ्यावयाची काळजी -

सायबर जागरुकता :

१. आपल्या बँकेतील खात्यास चालु अद्ययावत मोबाईल क्रमांक जोडण्यात यावा.

२. खात्यातील व्यवहारासंदर्भात येणारे सर्व एस.एम.एस. काळजीपूर्वक वाचावेत.

३. आपल्या खात्यावरील व्यवहाराचे खाते उतारे वेळोवेळी तपासण्यात यावेत.

४. आपल्या के.वाय.सी. कागदपत्र (आधारकार्ड, पॅनकार्ड, जन्मदिनांक व मोबाईल क्रमांक) बाबत जागरूक असावे. आवश्यक तेथेच माहिती पुरविण्यात यावी.

५. आपला बदललेला पत्ता व मोबाईल क्रमांकाबाबतची माहिती बँकेस त्वरीत कळविण्यात यावी.

६. के.वाय.सी. फसवणुकी बाबत जागरूक राहावे.

७. एस.एम.एस. द्वारे आलेली कोणतीही लिंक उघडण्यात येऊ नये.

८. लॉटरी , बक्षीस, फ्रि ट्रिट यांसारख्या फसवणुकी बाबत जागरूक राहावे.

ए.टी.एम.वापराबाबत घ्यावयाची काळजी :

१. बँकेने दिलेले कार्ड सेफ नावाच्या ॲपद्वारे आपले डेबीट कार्ड वापर नसतांना बंद व वापर करतांना चालु करता येते तसेच ई-कॉम., पॉस, आय.एम.पी.एस व यु.पी.आय. इत्यादी सर्व्हिससाठी लिमीट कमी अथवा जास्त करता येते. या ॲपद्वारे आपल्या ए.टी.एम. कार्डचे पिन क्रमांक देखील बदलता येतो.

२. आपल्या ए.टी.एम. कार्डचा पिन क्रमांक, ओ.टी.पी., सी.व्ही.व्ही., खाते क्रमांक कोणासही फोनवर सांगु नये तसेच ए.टी.एम. कार्डच्या मागे किंवा मोबाईल मध्ये फिड करून ठेऊ नये.

३. आपल्या ए.टी.एम. कार्डचा पिन दर तिमाही बदलण्यात यावा.

४. ए.टी.एम. मशीन वापरण्यापूर्वी मशीनला छेडछेड करण्यात आली नाही, याची खात्री करूनच व्यवहार करावेत तसेच रहदारी नसलेल्या ठिकाणी ए.टी.एम. मशीनचा वापर करू नये.

मोबाईल फोन वापराबाबत घ्यावयाची काळजी :

१. मोबाईल फोनला लॉक असावे तसेच सिमकार्डला देखील लॉक करण्यात यावे.

२. वापरात नसलेले मोबाईल क्रमांक खात्यावरून काढुन टाकावेत.

३. कोणाच्याही सांगण्यावरून कोणतेही मोबाईल ॲप आपल्या मोबाईलमध्ये इनस्टॉल करू नयेत.

४. Wi-Fi वापरात नसतांना बंद ठेवावा तसेच त्यास स्ट्रॅांग पासवर्ड ठेवावा जेणेकरून आपल्या Wi-Fi चा गैरवापर होणार नाही.

५. मोबाईल फोनचा आय.एम.ई.आय. क्रमांक संग्रहित ठेवावा तसेच मोबाईल ट्रॅकिंग सिस्टीम चालु करून ठेवावी, जेणे करून मोबाईल हरवल्यानंतर तो शोधणे शक्य होईल.

६. सार्वजनिक ठिकाणी असलेले मोबाईल चार्जिंग युनिटचा वापर करू नये.

७. सार्वजनिक वाय-फाय वरून कोणतेही आर्थिक व्यवहार करू नये.

८. आपल्या मोबाईल फोनचे वेळोवेळी बॅकअप घेण्यात यावे व मोबाईल मधील सॉफ्टवेअर वेळोवेळी अपडेट करावे.

सोशल मिडीया वापराबाबत घ्यावयाची काळजी :

१. आपली संवेदनशिल माहिती उदा.- मोबाईल क्रमांक, पॅनकार्ड क्रमांक, जन्मतारीख इत्यादी माहिती सोशल मिडीयावर उपलब्ध करू नये अथवा शेअर करू नये.

२. आपले लाईव्ह लोकेशन व पर्सनल फोटो सोशल मिडीयावर उपलब्ध करू नये अथवा शेअर करू नये.

३. अनोळखी व्यक्तीची फ्रेन्ड रिक्वेस्ट ॲक्सेप्ट करू नये तसेच आपली पोस्ट / फोटो शेअर करतांना कोणापर्यंत पोहचणार आहे याची काळजी घेऊनच पोस्ट करण्यात यावी.

४. सर्व सोशल मिडीया उदा. गुगल, फेसबुक, व्हॉट्स ॲप, इस्टाग्राम इत्यादींना उपलब्ध असलेल्या सेक्युरीटीचा जास्तीत जास्त उपयोग करण्यात यावा व टु फॅक्टर ऑथेन्टीकेशन चालु करण्यात यावे.

पासवर्ड बाबत घ्यावयाची काळजी :

१. आपण वापरत असलेल्या सर्व ॲप, सोशल मिडीया खाते , जि-मेल, ऑनलाईन खाते, संगणक व लॅपटॉप इत्यादींना असणारा पासवर्ड हा अत्यंत स्ट्रॅांग असावा. ज्यामध्ये आठ ते अकरा अक्षर असुन त्यात कॅपीटल, अंक, स्पेशल कॅरेक्टर इत्यादींचा समावेश असावा.

२. आपल्या घरात वापरात असलेल्या सर्व संगणक विषयक उपकरण उदा. Wi-Fi डोंगल, BSNL राऊटर, इत्यांदीचे डिफॉल्ट पासवर्ड बदलणे गरजेचे आहे.

ई–मेल वापराबाबत घ्यावयाची काळजी :

१. ई-मेल उघडण्यापूर्वी पाठविणा-या व्यक्तीचा ई-मेल ॲड्रेस तपासल्याशिवाय ई- मेल व ॲटॅचमेंट उघडु नये तसेच अनोळखी व्यक्तीचा ई-मेल उघडु नये.

२. ई-मेल किंवा एस.एम.एस.द्वारे आलेली लिंक व कोणतीही यु.आर.एल. किंवा वेबसाईट त्या लिंकद्वारे उघडु नये.

३. कोणतीही वेबसाईट उघडण्यापूर्वी वेबसाईटची सेक्युरीटी व वेबसाईट अधिकृत असल्याची खात्री करूनच ती उघडण्यात यावी.

।। तंत्रज्ञानाचा वापर करा ज्ञानाने व ध्यानाने ।।