TIPS for protecting yourself online

1. KEEP YOUR COMPUTERS & MOBILE DEVICES UPDATED
   Always keep updated operating system, browsers, anti-virus software of computer / laptops / palmtops / tablet / smart phone and other devices used by you. Turn on automatic updates so you receive the newest fixes as they became available. It gives very strong protection against viruses, malware, and other threats.

2. USE OF ANTI VIRUSE SOFTWARE
   Always install a good quality paid Anti-Virus / malware software in your device.

3. SET STRONG PASSWORDS
   Always set strong passwords. A strong password is at least 8 characters in length and incudes a mix of capital(A-Z) & lower case (a-z) letters, minimum one number (0,1....9) & minimum one special character (@, #, $, %, etc).

4. DO NOT SHARE YOUR SENSITIVE FINANCIAL DETAILS
   Bank does not ask accounts number, debit, or credit card number, CVV number, Expiry date, PIN, OTP, mobile or internet banking login, password, MPIN or TPIN personally or on call or through email. Never share this information to anybody on phone / SMS / email.

5. KEEP PERSONAL INFORMATION PERSONAL
   Hackers can use social media profiles to figure out your passwords and answer security questions to reset your password. Lock your privacy settings on social media profile and avoid posting things like birthdays, address, mother name, etc. Do not answer to request from unknown person.

6. SECURE YOUR INTERNET CONNECTION
   Always protect your home & office wireless network with a strong password. Be cautious while using public Wi-Fi networks.

7. SHOP SAFELY
   Always make sure that online shopping site you are using is official & secured. In checkout screen verify that the web address begins with **https** and check to see padlock symbol (🔒)appears on the page.

8. WATCH OUT FOR PHISHING SCAM
   Phishing scams use fraudulent emails and websites to trick users into disclosing account, login, personal & KYC information. Do not click on links or open any attachments or pop-up screens from unknown / unrecognized source.

આપને ઓનલાઈન માધ્યમ પર સુરક્ષીત રાખવા માટેના સૂચનો

1. **તમારા કોમ્પ્યુટર અને મોબાઇલ ઉપકરણોને અપડેટ રાખો.** તમારા દ્વારા ઉપયોગમાં લેવામાં આવતા કમ્પ્યુટર/ લેપટોપ/ પામટોપ/ ટેબ્લેટ/ સ્માર્ટફોન વગેરે ઉપકરણો ની ઓપરેટીંગ સીસ્ટમ, બ્રાઉઝર્સ, એન્ટી વાયરસ સોફ્ટવેર ને યોગ્ય સમયાંતરે અથવા ઓટો અપડેટ મોડ માં રાખી અપડેટ કરતા રહો. આ પ્રકાર ની સામાન્ય સંભાળ આપના ઉપકરણો ને વાયરસ, માલવેર તેમજ અન્ય પ્રકારના ઓનલાઈન જોખમો થી મહદ અંશે રક્ષણ આપે છે.

2. **એન્ટીવાયરસ સોફ્ટવેર** આપના દ્વારા ઉપયોગમાં લેવામા આવતા ઉપકરણો લાયસન્સ એન્ટીવાયરસ સોફ્ટવેર દ્વારા સુરક્ષિત હોવા જ જોઈએ.

3. **સ્ટ્રોગ પાસવર્ડ્સ સેટ કરો.** હંમેશા સ્ટ્રોગ પાસવર્ડ સેટ કરો. સ્ટ્રોગ પાસવર્ડ ની લંબાઈ ઓછામાં ઓછી આઠ, કેપીટલ અને સ્મોલ અક્ષરો નુ મીશ્રણ, ઓછામાં ઓછો એક અંક (૦,૧...૯), ઓછામાં ઓછો એક વિશેષ અક્ષર (@,#,$,%,^,&,*,! વગેરે) નું સંયોજન હોવુ જોઈએ.

4. **કોઈ પણ વ્યક્તી ને તમારી નાણાકીય વ્યવહાર ને સંલગ્ન કોઈપણ વિગત આપવી નહિ.** કોઈપણ બેંક કે નાણાકીય સંસ્થા દ્વારા પોતાના ગ્રાહક પાસેથી તેમના બેંક ખાતા ના નંબર, ડેબીટ અથવા ક્રેડીટ કાર્ડ ના નંબર, સીવીવી, એક્સપાયરી ડેટ, પીન કે મોબાઇલ / ઈન્ટરનેટ બેન્કીંગ સંબંધીત લોગીન, પાસવર્ડ, એમપીન કે ટીપીન સંલગ્ન માહિતી ફોન, ઇમેઈલ કે રૂબરૂ માંગવા માં આવતી નથી. આ પ્રકારની માહિતી ફોન, ઇમેઈલ એસએમસ કે અન્ય કોઈપણ પ્રકારે માહિતી માંગનાર મોટા ભાગના સંજોગોમાં ફ્રોડ કરનારજ હોઈ શકે છે.

5. **વ્યક્તિગત માહિતી વ્યક્તિગત રાખો.** હેકર્સ આપની સોશિયલ મીડિયા પ્રોફાઇલનો ઉપયોગ કરીને પાસવર્ડ રીસેટ કરવા માટે જે સીકયુરીટી પ્રશ્ન મુકવામાં આવેલ હોય છે તેનો સહેલાયથી જવાબ આપી ને આપનો પાસવર્ડ આપની જાણ બહાર રીસેટ કરી શકે છે સોશિયલ મીડિયા પર આપની પ્રોફાઇલ ના પ્રાયવસી સેટિંગ્સને હંમેશા લોક રાખો.આપની જન્મતારીખ,લગ્નતારીખ, માતા, પિતા, દાદા, દાદી, નાના, નાની નું નામ, રહેણાંક તેમજ કાર્યક્ષેત્ર ના એડ્રેસ વગેરે પ્રકાર ની અંગત માહિતી સોશિયલ મીડિયા પર મુકવાનું ટાળો, અજાણ્યા લોકો તરફથી મળેલ રીક્વેસ્ટ નો પ્રત્યુત્તર આપતા પૂર્વે સાવચેત રહો.

6. **ઇન્ટરનેટ કનેક્શન.** વાયરલેસ નેટવર્કને સ્ટ્રોગ પાસવર્ડથી સુરક્ષિત કરો. સાર્વજનિક(પબ્લિક) Wi-Fi નેટવર્ક નો ઉપયોગ કરીને અગંત માહિતી તેમજ બેંક ખાતા ના વ્યવહારો ની આપલે કરતી વખતે સવિશેષ સાવચેત રહો.

7. **સલામત વેબસાઈટ પરથીજ ઓનલઈન ખરીદી કરો.** ઓનલઈન શોપીગ ખરીદી કરતા પહેલા, ખાતરી કરો કે જે તે વેબસાઈટ ઓફીશીયલ અને સિક્યોર્ડ છે. ખરીદી ના આખરી તબકકા માં જયારે તમે રકમની ચૂકવણી કરી રહયા હો ત્યારે આવશ્ય ચેક કરો કે તે વેબસાઈટ નું સરનામું (URL) https થી શરૂ થયેલું હોવું જોઈએ તેમજ તેની બાજુમાં નાના લોક નું પ્રતીક વેબસાઈટ ગ્રીન બાર શાથેની હોવી જોઈએ.

8. **લોભામણા ઇમેઇલ,ફોન કોલ અને વેબસાઇટ્સ પર ધ્યાન આપો.** આપને ત્વરીત નાણાકીય લાભ ની જાણકારી આપતા, કેવાયસી થયેલ ન હોય ખાતું બંધ થઈ જશે ફોન પર ત્વરીત તમારું કેવાયસી કરાવો એ પ્રકાર ની આપને ગભરાવીને ત્વરીત માહિતી આપવા મજબુર કરતા ઈમેઈલ, ફોનકોલ ના જવાબ આપતા પૂર્વે તેની ખરાઈની ચકાસણી અવશ્ય કરો. આ પ્રકાર ના મળેલ ઈમેઈલ માં આપવામાં આવેલ વેબસાઈટની લિંક પર ક્લિક કરશો નહી તેમજ પોપઅપ, નોટીફીકેશન એલાઉડ કરશો નહી.

खुद को ऑनलाइन सुरक्षित रखने के टिप्स

1. अपने कंप्यूटर और मोबाइल उपकरणों को अपडेट रखें।

अपने ऑपरेटिंग सिस्टम, ब्राउज़र, एंटीवायरस को हमेशा अपने कंप्यूटर / लैपटॉप / पामटॉप / टैबलेट / स्मार्टफोन और आपके द्वारा उपयोग किए जाने वाले अन्य उपकरणों में अपडेट रखें । स्वचालित अपडेट चालू करें ताकि आप नवीनतम सुधार प्राप्त कर सकें क्योंकि वे उपलब्ध हो गए हैं। यह वायरस, मैलवेयर और अन्य खतरों से बहुत मजबूत सुरक्षा देता है।

2. एंटीवायरस सॉफ्टवेयर का उपयोग

हमेशा अपने डिवाइस में एक अच्छी गुणवत्ता वाला भुगतान किया हुआ एंटी-वायरस / मैलवेयर सॉफ़्टवेयर इंस्टॉल करें।

3. मजबूत पासवर्ड सेट करें

हमेशा कम से कम 8 वर्णों का एक मजबूत पासवर्ड सेट करें और इसमें कैपिटल लेटर (A-Z) और लोअर केस (a-z) अक्षर, न्यूनतम एक संख्या (0,1 .... 9) और न्यूनतम एक विशेष वर्ण (@, #, &, %,आदि) शामिल करें।

4. अपना बैंक विवरण साझा न करें

बैंक खाता संख्या, डेबिट कार्ड या क्रेडिट नंबर, CVV नंबर, समाप्ति तिथि, PIN, OTP, मोबाइल या इंटरनेट बैंकिंग लॉगिन, पासवार्ड, MPIN या TPIN को व्यक्तिगत रूप से या कॉल पर या मेल के माध्यम से नहीं पूछता है। इस जानकारी को कभी भी फोन / एसएमएस / ईमेल पर किसी को साझा न करें।

5. व्यक्तिगत जानकारी को व्यक्तिगत रखें

हैकर्स आपके पासवर्ड का पता लगाने के लिए और आपके पासवर्ड को रीसेट करने के लिए सुरक्षा सवालों के जवाब देने के लिए सोशल मीडिया प्रोफाइल का उपयोग कर सकते हैं। सोशल मीडिया प्रोफाइल पर अपनी गोपनीयता सेटिंग को लॉक करें और जन्मदिन, पता, माता का नाम आदि जैसी चीजों को पोस्ट करने से बचें । अज्ञात व्यक्ति के अनुरोध का उत्तर न दें।

6. अपने इंटरनेट कनेक्शन को सुरक्षित रखें

हमेशा एक मजबूत पासवर्ड के साथ अपने घर और कार्यालय के वायरलेस नेटवर्क की रक्षा करें। सार्वजनिक वाई-फाई नेटवर्क का उपयोग करते समय सतर्क रहें।

7. सुरक्षित रूप से खरीदारी करें

हमेशा सुनिश्चित करें कि आप जिस ऑनलाइन शॉपिंग साइट का उपयोग कर रहे हैं वह आधिकारिक और सुरक्षित है। यह भी ध्यान रखें कि क्या चेकआउट स्क्रीन विकल्प पर https के साथ वेब पता शुरू हो रहा है और यह भी देखें कि पृष्ठ पर पैडलॉक प्रतीक () दिखाई देता है या नहीं।

8. फ़िशिंग घोटाले से अवगत रहें

फ़िशिंग घोटाला उपयोगकर्ताओं और खातों, लॉगिन, व्यक्तिगत और केवाईसी जानकारी का खुलासा करने के लिए धोखाधड़ी वाले ईमेल और वेबसाइटों का उपयोग करता है। लिंक पर क्लिक न करें या अज्ञात / अपरिचित स्रोत से कोई अटैचमेंट या पॉप-अप स्क्रीन न खोलें।