Card Security- Useful Tips

Theme-1

Plastic card, a very famous terminology, which is used to make payments e.g. Debit card, Credit card, ATM cum debit card, prepaid card etc. As the use of card is growing cyber criminals are finding lots of ways to dupe innocent users. To avoid being victim of any such frauds here is the list of some precautions, which one can follow:

1. Ensure you have chip-based card (EMV Compliant), if not get it replaced with the bank.
2. Change the default PIN, sent by the bank.
3. If card goes missing, immediately get it blocked by calling or writing to bank. Ensure the customer care number is handy.
4. Do not write pin anywhere instead remember it.
5. Like passwords, change PIN periodically.
6. Do not set predictable PIN like your DOB, 1234, 1111 or similar.
7. As contactless (NFC enabled) card are wide in use, keep secure your card from misuse. Use RFID-Blocking Wallet or disable the NFC usage functionality if not being used
8. Use bank provided application to temporary block/ unblock card, set usage limit, channels where it can be used etc.
9. Enable international transaction only if you use it.
10. Verify credentials and check the ID proof, if you are applying for credit card through sales executive.
11. Never gives card details to anyone.
12. Never share CVV even with your bank executive in any circumstances.
13. Do not respond over call if someone ask card details, in case of doubt call bank's customer care.
14. Do not send card details in unencrypted format via mails, messages.
15. Use card on trusted website and with https and padlock sign.

16. Ensure two factor authentication is enabled for the email if you receive transaction over the mail.
17. Do not hand over your card to anyone, where you will lose the sight of it.
18. Avoid using card over public Wi-Fi and public computers e.g. cyber café.
19. Ensure good and updated antivirus on the machines where you use your card.
20. Don't enter card details in the link shared over mail/ message, verify the sender first.
21. Don't save card details in the browser.
22. Register for SMS and email alert from bank for card transactions.
23. Define transactions limit for your card as per your requirement.
24. While entering PIN, cover it so as to ensure it's not being watched.
25. Do not post pictures of card on any social media or avoid sharing it with anyone.
26. Be careful for your receipt when you do transaction.
27. Keep your phone number updated with bank on which you receive transaction alerts or One Time Password (OTP).
28. Be observant of any "skimming devices" attached to the ATM.
29. Before leaving ATM, Wait for the transaction to complete and close. Ensure to collect your card.
30. Don't get carried away by strangers who try to help you use the ATM machine.
31. In case of suspected transaction immediately report to the bank.

*****

Top Tips to Desktop/ Laptop security

Theme-2

Desktops and laptops are gateway to all the information stored, transmitted and used in digital world. Any weakness exploited on these systems may result in information theft and loss. Below are few key practices to safeguard against Cyber threats:

DO's	DONT'S
• Always install Licensed Software so that you have regular updates of your Operating system and Applications. In case of open source software, make sure to update frequently and from genuine source. • While installing any software ensure to tick/ untick checkboxes to enable features as per your requirement instead of default installation. • Properly shutdown and switch off your personal computer after the use and when you leave office. • Antivirus software must be organization provided or downloaded from trusted website with auto update of latest signatures. • Keep browser and all other applications of the system up to date. • Configure authorized/ trusted (Network Time Protocol) NTP for accurate time sync. • Enable short duration auto lockout of screen after inactivity. • Setup BIOS password.	• Do not use administrator user account for routine activities. • Don't click on remember my password. • Don't plug any unknown USB to your computer. • Don't share your credentials to anyone to login to your system. • Don't leave your machine unlocked or unattended. • Don't allow Remote Desktop Protocol (RDP) by default. • Don't allow network sharing unless it is necessary and it should be limited to specific user/machines. • Don't install Peer to Peer (P2P) file sharing programs. Ex. Torrents etc.

DO's	DONT'S
• Ensure physical safety of the computer devices including printers, network switches and other networking devices like Wi-Fi Access points. • Use original equipment manufacturer or organization provided CD to install the operation system and drivers. • Use strong password (alphanumeric with special characters) for admin accounts and other users. • Periodically take back up of your computer data in a secure location and periodically test if it's restoring correctly.	• Don't fill hard drive to its full capacity. • Don't keep GPS, Bluetooth, NFC and other sensors enabled, unless required.

***

Key Aspects to Spot Fraudulent E-mail and Do's & Don'ts for Secure Email Usages

Theme-3

Increased usage of smart devices and employees working remotely also increased the use of email frequently. While email are easy to use, attackers are also finding it easy to target the people remotely. Below are few of the techniques, which fraudsters use, and some action one can follow to avoid being victim:

- **Phishing links:** Don't get caught in the scammer's net, phishing links may be identified by placing cursor over a link in a suspicious email which shows actual URL. Make sure not to click, only to hover mouse pointer over it.
- **Short link:** While link-shortening services such as Bitly, TinyURL are popular and common tools for creating shorter links, malware distributors and phishers use link shortening to conceal their links' true destinations. Be careful and verify source before clicking such short links.
- **Requests for personal information:** Bank will never ask you to reply in an email with any personal information such as your PAN, ATM or PIN.
- **Urgent appeals:** Bank will never claim your account may be closed if you fail to confirm, verify or authenticate your personal information via email.
- **Email about security updates:** Bank will never claim the need to confirm important information via email due to system upgrades.
- **Observe the new:** Always observe sudden and different email content even though email from office employee/ executive, as it may be spoofed mail or email account may be compromised. Cross verify with sender for suspect mails.
- **Spelling and grammar mistakes:** Observe spelling of the email address as fraudster make slight changes in email addresses.

DO's

1. Keep your inbox clean, Turn on the junk email filtering system.
2. Beware of links in emails. May divert you to a site containing a virus or spyware.

3. Confirm from the source if you're unsure about a link they have sent you in an email.
4. Use strong password for your email account. Use multi- factor authentication wherever possible.
5. Access website by typing the URL instead of clicking the link in email especially financial websites.
6. Always log out of your email account when finished.
7. While sharing important information, encrypt/protect it with password.

DON'T'S

1. DON'T open, forward attachments received from unknown sources. And do not set your e-mail program to "auto-open" attachments.
2. DON'T give your user ID or password to another person and change your password frequently.
3. DON'T post your email address on a social network site, chat-room or webpage.
4. DON'T: Believe everything you read. Spam emails will often have a false subject line to try and trick you into opening the message.
5. DON'T use your official email id for personal use and avoid giving your office email address to everyone and everywhere.
6. DON'T access office email from public Wi-Fi.
7. DON'T click the links received in email asking you to update information.

If you receive a suspicious email that uses Bank's name/ logo/ similar URL, forward it to Bank's information security team immediately.

*****

कार्ड सुरक्षा- उपयोगी युक्तियाँ

विषय-1

प्लास्टिक कार्ड, एक बहुत प्रसिद्ध शब्दावली, जिसका उपयोग भुगतान करने के लिए किया जाता है। डेबिट कार्ड, क्रेडिट कार्ड, एटीएम सह डेबिट कार्ड, प्रीपेड कार्ड आदि। जैसे-जैसे कार्ड का उपयोग बढ़ रहा है, साइबर अपराधी निर्दोष उपयोगकर्ताओं को धोखा देने के लिए कई तरीके ढूंढ रहे हैं। ऐसी किसी भी धोखाधड़ी का शिकार होने से बचने के लिए यहां कुछ सावधानियों की सूची दी गई है, जिनका कोई भी पालन कर सकता है:

1. सुनिश्चित करें कि आपके पास चिप-आधारित कार्ड (ईएमवी अनुरूप) है, यदि नहीं है तो इसे बैंक से बदलवा लें।
2. बैंक द्वारा भेजे गए डिफ़ॉल्ट पिन को बदलें।
3. अगर कार्ड गुम हो जाए तो तुरंत बैंक को फोन करके या लिखकर उसे ब्लॉक कराएं। सुनिश्चित करें कि ग्राहक सेवा नंबर उपलब्ध है।
4. पिन को कहीं भी न लिखें बल्कि याद रखें.
5. पासवर्ड की तरह, पिन भी समय-समय पर बदलते रहें।
6. अपनी जन्मतिथि, 1234, 1111 या इसी तरह का पूर्वानुमानित पिन सेट न करें।
7. चूंकि संपर्क रहित (एनएफसी सक्षम) कार्ड का व्यापक उपयोग होता है, इसलिए अपने कार्ड को दुरुपयोग से सुरक्षित रखें। यदि उपयोग नहीं किया जा रहा है तो आरएफआईडी-ब्लॉकिंग वॉलेट का उपयोग करें या एनएफसी उपयोग कार्यक्षमता को अक्षम करें
8. कार्ड को अस्थायी रूप से ब्लॉक/अनब्लॉक करने, उपयोग सीमा निर्धारित करने, चैनल जहां इसका उपयोग किया जा सकता है आदि के लिए बैंक द्वारा प्रदान किए गए एप्लिकेशन का उपयोग करें।
9. यदि आप इसका उपयोग करते हैं तो ही अंतर्राष्ट्रीय लेनदेन सक्षम करें।
10. यदि आप सेल्स एक्जीक्यूटिव के माध्यम से क्रेडिट कार्ड के लिए आवेदन कर रहे हैं, तो क्रेडेंशियल सत्यापित करें और आईडी प्रूफ जांचें।
11. कभी भी किसी को कार्ड की जानकारी न दें.
12. किसी भी परिस्थिति में अपने बैंक अधिकारी के साथ भी सीवीवी साझा न करें।
13. यदि कोई कार्ड विवरण मांगता है तो कॉल का जवाब न दें, संदेह होने पर बैंक के ग्राहक सेवा को कॉल करें।
14. मेल, संदेशों के माध्यम से कार्ड विवरण अनएन्क्रिप्टेड प्रारूप में न भेजें।
15. विश्वसनीय वेबसाइट पर और https और पैडलॉक साइन वाले कार्ड का उपयोग करें।
16. यदि आपको मेल पर लेनदेन प्राप्त होता है तो सुनिश्चित करें कि ईमेल के लिए दो कारक प्रमाणीकरण सक्षम है।

17. अपना कार्ड किसी को न सौंपें, अन्यथा आपकी नजर उस पर नहीं पड़ेगी।
18. सार्वजनिक वाई-फाई और सार्वजनिक कंप्यूटर जैसे पर कार्ड का उपयोग करने से बचें। साइबर कैफे।
19. जिन मशीनों पर आप अपना कार्ड इस्तेमाल करते हैं, वहां अच्छे और अपडेटेड एंटीवायरस सुनिश्चित करें।
20. मेल/संदेश पर साझा किए गए लिंक में कार्ड विवरण दर्ज न करें, पहले प्रेषक को सत्यापित करें।
21. कार्ड की जानकारी ब्राउजर में सेव न करें।
22. कार्ड लेनदेन के लिए बैंक से एसएमएस और ईमेल अलर्ट के लिए पंजीकरण करें।
23. अपनी आवश्यकता के अनुसार अपने कार्ड के लिए लेनदेन सीमा निर्धारित करें।
24. पिन दर्ज करते समय इसे ढक दें ताकि यह सुनिश्चित हो सके कि इस पर कोई नजर न रख सके।
25. कार्ड की तस्वीरें किसी भी सोशल मीडिया पर पोस्ट न करें या किसी के साथ साझा करने से बचें।
26. जब आप लेन-देन करें तो अपनी रसीद का ध्यान रखें।
27. जिस बैंक पर आपको ट्रांजैक्शन अलर्ट या वन टाइम पासवर्ड (ओटीपी) मिलता है, उस बैंक में अपना फोन नंबर अपडेट रखें।
28. एटीएम से जुड़े किसी भी "स्किमिंग डिवाइस" से सावधान रहें।
29. एटीएम छोड़ने से पहले, लेनदेन पूरा होने और बंद होने तक प्रतीक्षा करें। अपना कार्ड एकत्र करना सुनिश्चित करें.
30. एटीएम मशीन का उपयोग करने में आपकी मदद करने की कोशिश करने वाले अजनबियों के बहकावे में न आएं
31. संदिग्ध लेनदेन के मामले में तुरंत बैंक को सूचित करें।

डेस्कटॉप/ लैपटॉप सुरक्षा के लिए शीर्ष युक्तियाँ

विषय-2

डेस्कटॉप और लैपटॉप डिजिटल दुनिया में संग्रहीत, प्रसारित और उपयोग की जाने वाली सभी सूचनाओं के प्रवेश द्वार हैं। इन प्रणालियों पर उपयोग की गई किसी भी कमजोरी के परिणामस्वरूप सूचना चोरी और हानि हो सकती है। साइबर खतरों से बचाव के लिए नीचे कुछ प्रमुख अभ्यास दिए गए हैं:

करने योग्य	मत करो
• हमेशा लाइसेंस प्राप्त सॉफ़्टवेयर इंस्टॉल करें ताकि आपको अपने ऑपरेटिंग सिस्टम और एप्लिकेशन के नियमित अपडेट मिलते रहें। ओपन सोर्स सॉफ़्टवेयर के मामले में, बार-बार और वास्तविक स्रोत से अपडेट करना सुनिश्चित करें।	• नियमित गतिविधियों के लिए व्यवस्थापक उपयोगकर्ता खाते का उपयोग न करें।
• किसी भी सॉफ़्टवेयर को इंस्टॉल करते समय डिफ़ॉल्ट इंस्टॉलेशन के बजाय अपनी आवश्यकता के अनुसार सुविधाओं को सक्षम करने के लिए चेकबॉक्स को टिक/अनटिक करना सुनिश्चित करें	• मेरा पासवर्ड याद रखें पर क्लिक न करें
• उपयोग के बाद और जब आप कार्यालय छोड़ें तो अपने व्यक्तिगत कंप्यूटर को उचित रूप से शटडाउन और स्विच ऑफ करें	• किसी भी अज्ञात यूएसबी को अपने कंप्यूटर से कनेक्ट न करें।
• एंटीवायरस सॉफ़्टवेयर नवीनतम हस्ताक्षरों के ऑटो अपडेट के साथ संगठन द्वारा उपलब्ध कराया जाना चाहिए या विश्वसनीय वेबसाइट से डाउनलोड किया जाना चाहिए।	• अपने सिस्टम में लॉग इन करने के लिए अपने क्रेडेंशियल किसी के साथ साझा न करें।
• सिस्टम के ब्राउज़र और अन्य सभी एप्लिकेशन को अद्यतन रखें।	• अपनी मशीन को खुला या लावारिस न छोड़ें।
• सटीक समय समन्वयन के लिए अधिकृत/विश्वसनीय (नेटवर्क टाइम प्रोटोकॉल) एनटीपी को कॉन्फ़िगर करें।	• रिमोट डेस्कटॉप प्रोटोकॉल (आरडीपी) को डिफ़ॉल्ट रूप से अनुमति न दें।
• निष्क्रियता के बाद स्क्रीन का लघु अवधि का ऑटो लॉकआउट सक्षम करें।	• जब तक यह आवश्यक न हो, नेटवर्क साझाकरण की अनुमति न दें और इसे विशिष्ट उपयोगकर्ता/मशीनों तक सीमित रखा जाना चाहिए।
• BIOS पासवर्ड सेटअप करें.	• पीयर टू पीयर (पी2 पी) फ़ाइल शेयरिंग प्रोग्राम इंस्टॉल न करें। उदाहरण टोरेंट आदि।
• प्रिंटर, नेटवर्क स्विच और वाई-फाई एक्सेस पॉइंट जैसे अन्य नेटवर्किंग उपकरणों सहित कंप्यूटर उपकरणों की भौतिक सुरक्षा सुनिश्चित करें।	• हार्ड ड्राइव को उसकी पूरी क्षमता तक न भरें।

करने योग्य	मत करो
• ऑपरेटिंग सिस्टम और ड्राइवरों को स्थापित करने के लिए मूल उपकरण निर्माता या संगठन द्वारा प्रदान की गई सीडी का उपयोग करें। • व्यवस्थापक खातों और अन्य उपयोगकर्ताओं के लिए मजबूत पासवर्ड (विशेष वर्णों के साथ अक्षरांकीय) का उपयोग करें। • समय-समय पर किसी सुरक्षित स्थान पर अपने कंप्यूटर डेटा का बैकअप लें और समय-समय पर परीक्षण करें कि क्या यह सही ढंग से पुनर्स्थापित हो रहा है।	• जब तक आवश्यक न हो जीपीएस, ब्लूटूथ, एनएफसी और अन्य सेंसर सक्षम न रखें।

धोखाधड़ी वाले ई-मेल का पता लगाने के मुख्य पहलू और सुरक्षित ईमेल उपयोग के लिए क्या करें और क्या न करें

विषय-3

स्मार्ट उपकरणों के बढ़ते उपयोग और दूर से काम करने वाले कर्मचारियों ने भी ईमेल के उपयोग को लगातार बढ़ाया है। जहां ईमेल का उपयोग करना आसान है, वहीं हमलावरों का दूर से लोगों को निशाना बनाना भी आसान हो रहा है। नीचे कुछ तकनीकें दी गई हैं, जिनका उपयोग धोखेबाज़ करते हैं, और कुछ उपाय जिनका पालन करके कोई भी शिकार होने से बच सकता है:

- **फ़िशिंग लिंक:** घोटालेबाज के जाल में न फंसें, किसी संदिग्ध ईमेल में लिंक पर कर्सर रखकर फ़िशिंग लिंक की पहचान की जा सकती है जो वास्तविक यूआरएल दिखाता है। सुनिश्चित करें कि क्लिक न करें, केवल माउस पॉइंटर को उस पर घुमाएँ।

- **लघु लिंक:** जबकि Bitly, TinyURL जैसी लिंक-शॉर्टिंग सेवाएं छोटे लिंक बनाने के लिए लोकप्रिय और सामान्य उपकरण हैं, मैलवेयर वितरक और फ़िशर अपने लिंक के वास्तविक गंतव्य को छिपाने के लिए लिंक शॉर्टिंग का उपयोग करते हैं। सावधान रहें और ऐसे छोटे लिंक पर क्लिक करने से पहले स्रोत सत्यापित करें।

- **व्यक्तिगत जानकारी के लिए अनुरोध:** बैंक आपसे कभी भी आपके पैन, एटीएम या पिन जैसी किसी भी व्यक्तिगत जानकारी के साथ ईमेल में उत्तर देने के लिए नहीं कहेगा।

- **तत्काल अपील:** यदि आप ईमेल के माध्यम से अपनी व्यक्तिगत जानकारी की पुष्टि, सत्यापन या प्रमाणित करने में विफल रहते हैं तो बैंक कभी भी यह दावा नहीं करेगा कि आपका खाता बंद कर दिया जाएगा।

- **सुरक्षा अपडेट के बारे में ईमेल:** सिस्टम अपग्रेड के कारण बैंक कभी भी ईमेल के माध्यम से महत्वपूर्ण जानकारी की पुष्टि करने की आवश्यकता का दावा नहीं करेगा।

- **नए का निरीक्षण करें:** हमेशा अचानक और भिन्न ईमेल सामग्री पर ध्यान दें, भले ही कार्यालय कर्मचारी/कार्यकारी का ईमेल हो, क्योंकि यह नकली मेल हो सकता है या ईमेल खाते से छेड़छाड़ की जा सकती है। संदिग्ध मेल के लिए प्रेषक से दोबारा सत्यापन करें.

- **वर्तनी और व्याकरण की गलतियाँ:** ईमेल पते की वर्तनी पर ध्यान दें क्योंकि धोखेबाज़ ईमेल पते में मामूली बदलाव करते हैं।

करने योग्य:

1. अपना इनबॉक्स साफ़ रखें, जंक ईमेल फ़िल्टरिंग सिस्टम चालू करें।
2. ईमेल में लिंक से सावधान रहें. आपको किसी वायरस या स्पाइवेयर वाली साइट पर ले जा सकता है।
3. यदि आप किसी लिंक के बारे में अनिश्चित हैं जो उन्होंने आपको ईमेल में भेजा है तो स्रोत से पुष्टि करें।
4. अपने ईमेल खाते के लिए मजबूत पासवर्ड का प्रयोग करें। जहां भी संभव हो बहु-कारक प्रमाणीकरण का उपयोग करें।
5. ईमेल में दिए गए लिंक पर क्लिक करने के बजाय यूआरएल टाइप करके वेबसाइट तक पहुंचें, विशेषकर वित्तीय वेबसाइटों तक।
6. समाप्त होने पर हमेशा अपने ईमेल खाते से लॉग आउट करें।
7. महत्वपूर्ण जानकारी साझा करते समय उसे पासवर्ड से एन्क्रिप्ट/सुरक्षित करें।

ऐसा न करें:

1. अज्ञात स्रोतों से प्राप्त अनुलग्नकों को न खोलें, अग्रेषित करें। और अपने ई-मेल प्रोग्राम को "ऑटो-ओपन" अटैचमेंट पर सेट न करें।
2. अपना यूजर आईडी या पासवर्ड किसी अन्य व्यक्ति को न दें और अपना पासवर्ड बार-बार बदलें।
3. अपना ईमेल पता किसी सोशल नेटवर्क साइट, चैट-रूम या वेबपेज पर पोस्ट न करें।
4. आप जो कुछ भी पढ़ते हैं उस पर विश्वास न करें। स्पैम ईमेल में अक्सर गलत विषय पंक्ति होती है जो आपको संदेश खोलने के लिए प्रेरित करती है।
5. व्यक्तिगत उपयोग के लिए अपनी आधिकारिक ईमेल आईडी का उपयोग न करें और हर किसी और हर जगह अपना कार्यालय ईमेल पता देने से बचें।
6. सार्वजनिक वाई-फ़ाई से कार्यालय ईमेल का उपयोग न करें।
7. ईमेल में प्राप्त जानकारी अपडेट करने के लिए कहे गए लिंक पर क्लिक न करें।

यदि आपको कोई संदिग्ध ईमेल प्राप्त होता है जो बैंक के नाम/लोगो/समान यूआरएल का उपयोग करता है, तो इसे तुरंत बैंक की सूचना सुरक्षा टीम को अग्रेषित करें।