SECL

Cyber Jagrukta Diwas

Online awareness program
on
electronic payment security

Knowing Credit/Debit Cards/UPI

Debit card: A card that allows paying for products or services by deduction of available funds in a bank account of the cardholder.

Credit card: A card that allows paying for products or services by availing unsecured/secured credit from a financial institution. Issued by both Banks and NBFCs.

Card number: The number assigned by a card issuing association or bank to a card. This information must be provided to a merchant by a customer in order to make a card payment but should not be shared with anyone else. The string of digits is printed on the card.

CVV: Stands for Card Verification Value. This is a 3-digit number printed on the card which is mandatory for completing most online transactions. These details are confidential are confidential and must NEVER be shared with anyone.

UPI: Unified Payments Interface (UPI) is a payment system developed by NPCI (National Payments Corporation of India) that allows users to link more than one bank account in a single smartphone app and make fund transfers without having to provide IFSC code or account number. This is a real-time payment system where funds are credited instantly on a real-time basis.

Credit Score: A credit score is a number from 300 to 900 that rates a consumer's creditworthiness. The higher the score, the better a borrower looks to potential lenders.

Types of frauds

❑ Skimming

- Fraud- In this type of scam, your card details are stolen with the help of a device called a skimmer. When your card gets swiped through a skimmer, it stores all the data from your card. This information can then be duplicated on another card. Thus, scammers use your credit card information to make monetary transactions. This type of fraud can happen at POS or ATM.

- Prevention- Ensure you do not swipe through any machine that looks suspicious. You can also use chip-based credit cards as these are much more secure than those with a magnetic strip. While chip cards deliver the same information as magnetic stripe, they are safeguarded by encryption and similar technologies. This makes it harder for scammers to commit frauds. Chip cards give card issuers the ability to generate individual transaction data for each transaction and secure the information created.

❑ Phishing

- Fraud- A phishing attack is when fraudulent emails or SMS are sent to your email account or phone. Phishing involves persuasion i.e. you receive an email that looks convincing as it is from a well-known bank or financial organization. The goal of these phishing emails is to get users to click malicious links or download infected attachments in email. Your general reaction might be to click and check what the email is about. Once you click on the link, it will redirect to a fake website where you are asked to put your personal information or might download and install a malware on your device. Most people fall into these traps – allowing hackers to steal confidential information.

- Prevention- You must always remember that banks do not generally send emails requesting your details. If you ever receive any such email or SMS, make sure to inform your financial organization (bank/credit card issuer) so that you do not get into the trap. In addition, you must be very observant while clicking on any link received or replying to any such email or SMS. Some banks have the feature of setting security question, which could be used to identify the genuineness of a website.

Types of frauds

❑ Keystroke Capturing

- Fraud- Hackers mostly use keystroke logging through certain software to find your credit card details. This can happen if you click on a link redirecting you to download malware, and you unknowingly do that. If any such software gets installed in your device, it will record every key that you press. Hence your ids and passwords are recorded as well.

- Prevention- To avoid any such situation, make sure not to click on any suspicious links received in email or phone number. You can also use a virtual keyboard while feeding personal information like passwords and id details. Lastly, you must have reliable antivirus software to protect your system.

❑ SIM Swapping (also known as SIM jacking)

- Fraud- Cybercriminals can call any mobile operator and pretend to be an existing user requesting a duplicate SIM card. In addition, they would ask the operator to deactivate the original cardholder's number. Or scammers would call you as your mobile service operator and explain that call is regarding upgrading your network etc. Every SIM card has a unique number printed on it. The scammers simply call you and try to convince you to share your 20-digit unique number. Once the sim swap is successful, the scammer can create new IDs, receive OTPs and execute online transactions.

- Prevention- If you ever receive a warning regarding a duplicate sim request or feel your number has been blocked, immediately inform your mobile service operator and report about this. You are locked out of your phone's online account. Your phone loses service, or you cannot receive calls or texts even with good reception. You receive phone service notifications for actions you didn't take. If you remain cautious and let the service provider know at the time, you will be able to prevent such scams. Contact your cell phone provider immediately, as you might be under attack.

Types of frauds

❑ Vishing (Voice Phishing)

- Fraud- Scammers use fraudulent phone numbers, text messages, voice-altering software, and social engineering to lure users into divulging sensitive information. The scammer generally tries to get you to share personal information and financial details during vishing phone call. The scammer might say your account has been compromised, KYC is pending, claim to represent your bank or law enforcement or insurance agent, or offer to help you install software which is probably a malware.

- Prevention- Bank officials / financial institutions / RBI / any genuine entity never ask customers to share confidential information such as username / password / card details / CVV / OTP. Never share these confidential details with anyone, even your own family members, and friends. Vishing calls generally try to create fear in your mind, and most people give their sensitive information. However if you have any genuine doubt about safety of your interests, it is advisable to physically visit your bank/finance institution.

❑ SIM Cloning

- Fraud- Many times, people try to put SIM swapping and SIM cloning under that same umbrella. However, SIM cloning is more hands-on than the other option. In a SIM clone attack, the hacker first gains physical access to your SIM card and then creates a copy of the original. Naturally, for copying your SIM card, the hacker will first take out your SIM from the smartphone. They do this with the help of a smart card copying software, which copies the unique identifier number—assigned to you on your SIM card—onto their blank SIM card.

- Prevention- Keep your mobile device securely. Never leave it unattended in public surroundings. Also using a reliable antivirus can protect you against sim cloning. Once the sim is removed from sim tray temporarily and put again, the antivirus is able to detect that sim was removed and notifies you about the same. Use https://tafcop.dgtelecom.gov.in/ to check no. of mobile numbers active on your aadhar.

Types of frauds

❑ Hacking

- Fraud- One of the most common types of fraud in India must be hacking. It is probably the oldest method of performing fraudulent activities. With the advancement of technology, hackers are also developing their skills. They can hack any of your devices and steal all your personal information. Similarly, hackers can steal data from those firms with whom you have performed transactions. Thus, they can breach data for scams.

- Prevention- Although it is unpredictable to notice when you are hacked, so you need to be very careful while performing online transactions. If any website seems suspicious, do not provide your details. You also must not click on every link you get. These hackers can break into your online space and get the required data for conducting scams.

❑ Juice Jacking

- Fraud- The charging port of a mobile, can also be used to transfer files / data. Fraudsters use public charging ports to transfer malware to customer phones connected there and take control / access / steal data sensitive data such as emails, SMS, saved passwords, etc. from the customers' mobile phones.

- Prevention- Avoid using public / unknown charging ports / cables.

Some important points

❑ UPI

- The secure transfer of funds through UPI requires you to create a UPI ID and a UPI PIN. The UPI ID acts as a virtual payment address for the users and is created while setting up a UPI account. UPI PIN, on the other hand, is a password that must be set by the user to authorize the transaction from a particular bank account.
- Never share your UPI pin and use genuine UPI apps only.
- **Entering UPI PIN will always result in Money being debited from your account.**

❑ International Transactions

- One can do an international transaction with an Indian credit card without OTP/PIN. International transactions only need Card number, Expiry Date & CVV. And it involves some charges too.
- You would still get the SMS about your card being used. **Prevent the wrong usage by Disabling your card for International transactions.**

❑ NFC Cards (Near Field Communications)

- Tap and Pay feature of NFC cards is quite handy. However one should take precaution and choose to set the limit for such transactions on their card.

❑ Credit Score Report

- Is it possible for someone to misuse my credit score? Yes, fraudsters can steal your financial information like PAN details and other identity information and apply loans in your name.
- Periodically check your CIBIL report to see your credit history like loans/ credit cards. If you see any loan/ credit card entry which you don't recognize, report it immediately as it might be a loan fraud by identity theft.

General Precautions

- Keep the card/UPI PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
- Avoid saving card details on websites/ cloud storage drives / devices / public laptop / desktops.
- Turn on two-factor authentication where such facility is available.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- Do not share copies of chequebook, KYC documents with strangers.
- Change passwords at regular intervals.
- Install antivirus on your devices and install updates whenever available.
- Do not install any unknown applications or software on your phone / laptop.
- Avoid using public terminals (viz. cyber cafe, etc.) or public wifi for financial transactions.
- Keep your device applications updated and check the permissions given to applications on your mobile device.

Report Cybercrimes at

cybercrime.gov.in

or

Call

1930

(Earlier 155260)

For Assistance

Please refer http://www.secl-cil.in/cyber.php for more updates on Cyber Jagrookta

Not secure | secl-cil.in/cyber.php

साउथ ईस्टर्न कोलफील्ड्स लिमिटेड
South Eastern Coalfields Limited
(भारत सरकार का उपक्रम)
(A Government of India Undertaking)

एक मिनीरत्न कंपनी...

स्किप | स्क्रीन रीडर | शब्द आकार: अ+ अ अ- | रंग बदलें: अ अ

भाषा बदलें : ENGLISH

कोल इण्डिया लिमिटेड
Coal India Limited

Ministry of Coal
Government of India

हमसे संपर्क करें | वेबसाईट अंतिम अद्यतन : November 02 2022 10:23:05

होम / Cyber Jagrookta Diwas

Cyber Jagrookta(Awareness) Diwas

Cyber Jagrookta Diwas is celebrated on first wednesday of every month to generate sustained awareness among public on Cyber Security.

Cyber Jaagrookta Quote for the Day : "Beware of remote screen sharing apps, as fraudsters may use them to steal your information."

Cyber Security Awareness Month : October 2022- Theme is **"See Yourself in Cyber"**