ABHYUDAYA
CO-OPERATIVE BANK LTD.
(MULTI - STATE SCHEDULED BANK)

सायबर जागरूकता

Cyber security is buzz word now days. Cyber security refers to the practices, technologies, and processes designed to protect digital information, computer systems, networks, and electronic data from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes protection against malware, viruses, trojans, phishing, ransomware, and other types of cyber threats.

Effective cyber security measures ensure the confidentiality, integrity, and availability of sensitive information and prevent cyber attacks that can compromise individual or organizational security.Effective cybersecurity measures involve a combination of technology, policies, and user awareness to stay ahead of emerging threats and protect against cyber attacks.

Cybersecurity is crucial in today's digital age due to the following reasons:

1. Protection of sensitive information:
2. Prevention of financial loss:
3. Maintenance of privacy:
4. Protection of critical infrastructure:
5. Business continuity:
6. National security:
7. Protection of intellectual property:
8. Compliance with regulations:
9. Reputation and trust:
10. Evolving threats:

Cybersecurity helps safeguard personal, financial, and confidential data from unauthorized access and theft.Cyber attacks can result in significant financial losses, damage to reputation, and legal liabilities.It ensures that personal information remains private and is not exploited for malicious purposes.It is essential for safeguarding critical infrastructure, such as power grids, healthcare systems, and transportation networks.It helps ensure uninterrupted business operations and minimizes downtime.It is vital for protecting national security and preventing cyber espionage.It helps safeguard intellectual property, trade secrets, and proprietary information.It helps organizations comply with data protection regulations and avoid legal consequences.It helps maintain customer trust and protects an organization's reputation.It is essential for staying ahead of emerging threats, such as AI-powered attacks, IoT vulnerabilities, and social engineering tactics.

Some Security tips…….

Password Security:

Protecting Yourself Online :

Here are some password protection tips:

1. Use strong passwords: Mix uppercase and lowercase letters, numbers, alphanumeric and special characters.Use different passwords for each account.Don't use easily guessable words like names, birthdays, or common phrases,places.Update passwords at specific interval of time.
2. Password length: Ideally 12 characters or more.
3. Don't reuse passwords: Never reuse passwords across multiple accounts.
4. Two-factor authentication (2FA): Enable 2FA whenever possible to add an extra layer of security such as OTP or Biometric.
5. Avoid phishing scams: **Be cautious of emails or links asking for password resets or logins.**
6. Keep passwords private: Don't share passwords with others or write them down in accessible locations.

Remember, strong passwords are your first line of defense against cyber threats!

Types of Cyber Threats:

Malware, short for "malicious software," refers to any software designed to harm or exploit a computer system or its user.
Types of malware include:
1. Viruses: Replicate and spread to other files or systems.
2. Trojans: Disguise themselves as legitimate software, allowing unauthorized access.
3. Spyware: Secretly monitor and collect user data.
4. Ransomware: Encrypt files, demanding payment for decryption.
5. Adware: Display unwanted advertisements when you are using mobile phones or laptops.
6. Worms: Self-replicate and spread without human interaction.
7. Rootkits: Hide malware or unauthorized access.
8. Keyloggers: Record keystrokes, often to steal sensitive information, while entering password ,use virtual keyboard.

Malware can enter systems through:

1. Email attachments or links
2. Infected software downloads
3. Vulnerable network connections, public place wi-fi
4. Infected external devices(e.g., USB drives, pen drives)
5. Exploited system vulnerabilities

To protect against malware, attack:

1. Use antivirus software
2. Keep systems, smartphone and software up-to-date
3. Avoid suspicious downloads and links
4. Use strong passwords and enable firewall
5. Regularly back up important data
6. Download app from official /trusted source only. Ensure its guanines.
7. Do not respond to links/SMS/emails for high returns, investments schemes.

Remember, vigilance and caution are key to preventing malware infections!

Psychological tricks are where attackers play with the minds of the user to trap them with lucrative offers. Once trapped, the attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way. The entire basis of this kind of attack is to make the victim fall into their trap by sending fake e-mails, calls or SMSs.

Phishing is the act of sending fraudulent e-mail that appears to be from a legitimate source, for example, a bank, a recruiter or a credit card company etc. This is done in an attempt to gain sensitive personal information, bank account details etc. from the victim.

Vishing is similar to phishing. But, instead of e-mail, in this type of crime, the fraudster uses telephone to obtain sensitive personal and financial information.

Smishing is the SMS equivalent of phishing. It uses SMS to send fraudulent text messages. The SMS asks the recipient to visit a website/weblink or call a phone number. The victim is then tricked into providing sensitive personal information, debit/credit card details or passwords etc.

Phishing, Vishing and Smishing are done in an attempt to steal money from the victim or cause any other harm to the victim.

Social Media Frauds :→ Fraudsters use Fake Profile of the victim to spread false or fake information.Sends friend requests to other friends of victim to gain financial benefits. To damage the reputation of the victim.

To avoid above social media fraud_:→ Avoid sharing your personal information like address, mobile number, personal mail id and other sensitive identity related information on social media. Do not share your personal pictures online publicly on social media accounts. Never accept friend requests without appropriate verification and confirmation. Enable multi-factor authentication for social media accounts. Disable profile visibility from public searches. Log out after each session. Never share social media credentials with any one. Keep the privacy settings of social media profile at most restricted level, especially for public viewing. Apply maximum caution while sharing photographs, videos, status, comments etc. Criminals may collect enough information about users from the posts and profile of the user.Review your social media privacy settings and restrict to family and known friends. Be careful & alert while using social media platform like facebook, whatsapp , Linked IN Instagram, Twitter.

Educate children about password safety.Check their social media accounts and keep track of it.

QR code scam: scammers use QR codes to trick you to visit fake website or asking your login details …

Online shopping fraud- Like sales of fake products, phony online stores , unauthorized use of credit cards.

Online job fraud- Fraudsters create fake job search websites, job seekers share secure credentials of their bank account on these websites during registration, their accounts are compromised. Job seeker is then induced to transfer funds for registration, mandatory training program, laptop, etc.

Morphing is altering or changing the pictures of the person using morphing tools available online. The morphed pictures are then used by perpetrators for blackmailing the victims, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc., Morphing can damage the victim's online reputation and cause emotional trauma, can also be prone to threats from perpetrators and may fall prey to their attempts at blackmailing them.

Cybercriminals are persistently looking for new ways to expose security risks. They perform cyberattacks to steal, expose, alter, disable, or destroy organisation's assets through unauthorized access to computer systems. Cyber-attack could cause financial loss and disruption of business.

TIPS TO KEEP YOU SAFE… Do's & Don'ts

1. Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.

2. Protect systems/devices through security software such as anti-virus with the latest version.

3. Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.

4. Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone.

5. Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.

6. Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).

7. Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.

8. Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity.

9. Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.

10. Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.

11. Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/ block/trace a phone using the IMEI code, in case the cell phone is stolen.

12. Observe your surroundings for skimmers or people observing your PIN before using an ATM.

13. Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.

14. Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.

15. Update Mobile number to your branch time to time in case of changes in your mobile number so that regular SMS updates will receive.

16. For secured transactions use official mobile apps only.

17. If you think you are compromised, inform authorities immediately.

18.**आरबीआई/बैंक कभी भी लोगोंसे व्यक्तिगत जानकारी/बैंक का विवरण नहीं मांगताहै।आरबीआई के नकली लोगो और संदेशों से सावधान रहें।**

Where to Report a Cyber Fraud?

1. Visit the nearest police station immediately.

2. To report cybercrime complaints online, visit the National Cyber Crime Reporting Portal. This portal can be accessed at https://cybercrime.gov.in

You can also file a complaint by dialing the helpline number**1930**.

3. In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on Maharashtra Cyber's web portal by visiting www.reportphishing.in

4. Refer to the latest advisories which are issued by CERT-IN on https://www.cert-in.org.in/

5. Report any adverse activity or unwanted behavior to CERT-IN using following channels

E-mail : incident@cert-in.org.in

Helpdesk : +91 1800 11 4949 Provide following information (as much as possible) while reporting an incident.

- Time of occurrence of the incident
- Information regarding affected system/network
- Symptoms observed

6. To report lost or stolen mobile phones, file a First Information Report (FIR) with the police. Post filing the FIR, inform Department of Telecommunications (DoT) through the helpline number 14422 or file an online compliant on Central Equipment Identity Register (CEIR) portal by visiting https://ceir.gov.in After verification, DoT will blacklist the phone, blocking it from further use. In addition to this, if anyone tries to use the device using a different SIM card, the service provider will identify the new user and inform the police.

7. To hotlist cards you can follow any one of the steps mentioned below:
a) Dial "9223110011" from the MOBILE NUMBER registered with our Bank. After 2-3 rings call will be disconnected, the system will HOTLIST the card & you will get SMS confirmation for the same.
b) Customer can directly call 1800223131/ 022-68778900 and register a request to hotlist the card by providing necessary credentials asked by the staff member manning the desk.
c) If the card holder has availed our mobile banking services, he can hotlist the card by selecting card hotlist option.
d) Customer can also email to hotlist@abhyudayabank.net for necessary action.

Lodge a written complaint with the Base Branch in respect of the unauthorized electronic transaction.

Grievance Redressal Policy of Abhyudaya Bank in respect of Electronic Transactions
Bank has a separate Customer Grievances Redressal Cell (contact number 022- 27890636, 022-7890638, email address atmrecon@abhyudayabank.net for quick redressal of customer grievances including those arising from electronic transactions channel. The cell takes utmost care to settle

the issues relating to wrong/fraudulent debits and credits through the NPCI Dispute Management Scheme.

The customer having a grievance in respect of any of the electronic payments option can approach any branch of Abhyudaya Bank to file a written complaint with details of the matter. The complainant should bring along passbook, and an officially valid ID document, and also a passport-size photograph. In case of a fraudulent debit to or withdrawal from the customer's account, the customer should lodge a police complaint or file FIR. However, filing an FIR by the customer is not a precondition but to lodge police complaint (acknowledgement) is mandatory for any branch of Abhyudaya Bank accepting the complaint. The branch with which the complaint is filed will first assess the issue, record relevant information on complaint letter with signature held and forward the same immediately to the ATM-RECON Dept. Vashi, which at presently working as Customer Grievances Redressal Cell.

****