सत्यमेव जयते

સંઘ પ્રદેશ દાદરા અને નગર હવેલી અને દમણ અને દીવ

UT OF DADRA AND NAGAR HAVELI AND DAMAN AND DIU

CYBER SECURITY AWARENESS FOR CITIZENS

YES! I AM YOUR CYBER FRIEND

Version 1.0

Table of Content

1. Preface

With the growing adoption of Digital platforms by citizens of India, rate of digital crimes is also increasing day by day. Since internet is widely used by people in their daily lives, it is necessary to spread awareness among users for safe and secure use of these platforms/services accessible through internet. UT Administration of DNH and Daman & Diu has taken up the task of educating the people on cyber frauds and online safety. As a part of this initiative UT Administration is Introducing a Booklet for Cyber Security Awareness for Adults as well for Children.

This booklet is a collection of awareness tips for Phishing, Vishing, Malware, Social Media Fraud etc. This Tips are created with the help Indian Computer Emergency Response Team (CERT-In) and Indian Cyber Crime Coordination Centre (I4C) Awareness for Citizen of India as a part of Cyber Swachhta Kendra (CSK) which was initiative by CERT-In.

2. What is Cyber Security Awareness :

Cyber Security Awareness is a method to read the types of threats and implement the protection against such threats from the internet to protect our privacy and secure our data. Internet is used by us on regular basis and we all are aware of the security threats on the internet. We need to protect our privacy from such cyber attacks.

As the world of cyber is getting huge, the threats to us also increases on the regular basis and we need to be protective against such attacks. The internet and connectivity devices are making our life easier, but they also bring danger online.

A cyber security awareness is an important to protect our data from the cyber-attacks, and unknown login. We need to get aware from the online threats like phishing and malware that cybercriminals use to steal our data. We need to identify and avoid frauds that are conducted online, via email, or on social media.

3. Importance of Cybersecurity Awareness

At earlier times, only the computer viruses were a problem but now we have antivirus software to protect us from them. But now the cyber threats have grown large and advanced that is becoming dangerous to all of us. Malware, phishing, DDoS attacks, data breaches and fraud email some common example where we trap ourselves and become a victim. Following are some points to know the importance of cybersecurity awareness:

1. As the world of digital era is increasing, the cyber-attacks and threats are also increasing day to day and we need to be aware from such cyber threats and protect our data.

2. Multiple malware, phishing, DDoS attacks, data breaches and fraud email are sent to user through the internet to access and breach their personal and professional data on daily basis.

3. It is important to protect yourself from the various cyber threats such as phishing scams, malware attacks, and data breaches and protect our personal and professional data.

4. We need our professional data to be Private and Confidential because the personal loss can be compromised at a stance, but professional data breach cannot only harm our self but can also damage the entire company by the cyber threats.

5. There is a huge risks of identity theft on the internet so it is important to keep our personal information safe and prevent identity fraud.

6. It is seen that a lot of victims are made by making financial scams, fraud transactions and ransom attacks which causes a huge financial loss to the victim.

7. We also need to Secure our digital assets and cybersecurity awareness helps us to do so by protecting our digital assets which includes email accounts, our social media profiles, and the online banking accounts from the cybercriminals.

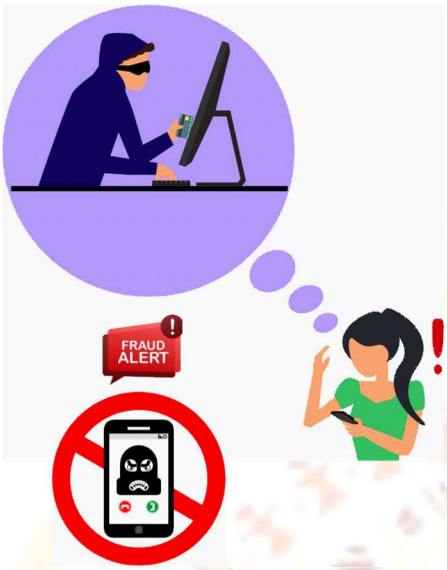
4. Phishing

Phishing is a common method that cybercriminals use to do the fraudulent activity by creating authentic-looking emails or websites to trick victims into sharing personal information or financial data.

Safety Tips

- ✓ Carefully check the URL before clicking on it.
- ✓ Never react to the messages which shows urgency.
- ✓ Do not trust promotional offers which look “too good to be true”.
- ✓ Do not hesitate to report to Law Enforcement Agencies, if you become a victim of phishing.
- ✓ Verify the email ids in emails addressed to generic recipients. Look for typing errors (eg., Acc0unt, ema1l, dep0sit, passw0rd) “Do yu kare about yurself?” Look for poor grammar and unprofessional Language.

5. VISHING



Fraudsters contact the victim pretending to be calling from trusted sources like bank/ income tax/ Gas agency etc.

They ask victim's for bank account details & collect financial information about debit/credit cards, expiry date etc.

The fraudster tells the victim to share OTP sent on mobile for depositing the amount.

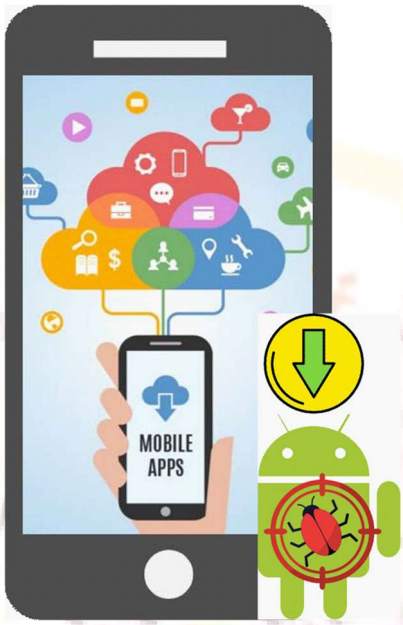
Once the victim shares the OTP, money is deducted from their account.

Safety Tips

- ✓ Never share OTP, PIN, CVV, Debit/Credit card details with anyone.
- ✓ Do not share any OTP/UPI PIN for receiving money.
- ✓ Do not respond to any calls asking to confirm or share bank account, credit/debit card details or sensitive information.
- ✓ Do not provide personal information in order to receive prize/ lottery/ gifts/ updating KYC etc.,
- ✓ Do not call the numbers of service providers randomly found in search engines as they can be fake numbers.
- ✓ Use the customer care service numbers available on authorized websites of the institute/ organisations/ banks etc.
- ✓ In case of any incident, user should call 1930 and change the password of their account immediately or block the card/ freeze the account to prevent financial loss.
- ✓ Users should regularly review bank & credit card statement & report any irregularities.
- ✓ Beware of calls asking to share personal information or asking to install any remote access apps on the pretext of helping.

6. Malicious Mobile Applications

Infected mobile applications may contain malware that can steal your data, login credentials and auto subscribe to premium services.



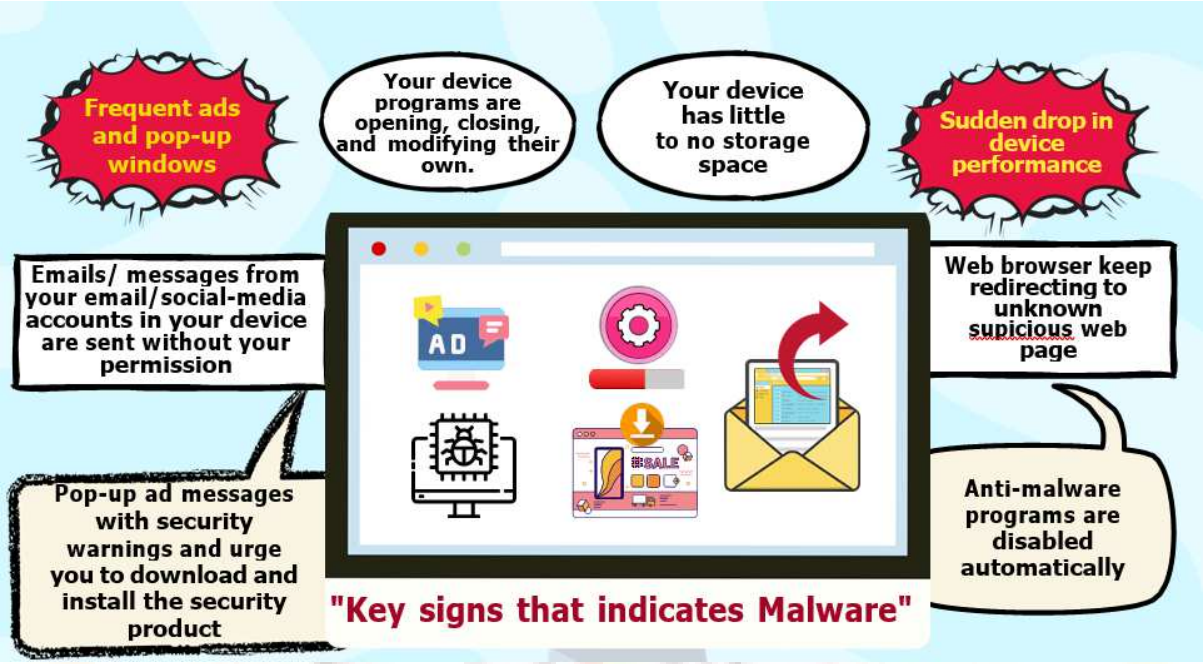
Safety Tips

- ✓ Before downloading any mobile application check for play protect feature on Play Store.
- ✓ Always download applications only from trusted sources like legitimate websites or authorized app store.
- ✓ Avoid downloading apps from SMS, emails, social media messages.
- ✓ Be cautious about allowing any new permissions during the installation of the application.
- ✓ Pay attention to reviews and comments of the users, before installing any mobile application.

\

7. Malware

Malware is a piece of malicious code inserted in an application, program or system by threat actors. They can infect your systems and perform malicious operations.



Safety Tips

- ✓ Avoid clicking on suspicious emails, links, and sites from unknown source.
- ✓ As soon as you click on any malicious link, your mobile can be hacked or your data can be stolen.
- ✓ Browse only secure and authorised websites.
- ✓ Always keep your computer software/browser up to date. Maintain backup of your data regularly.
- ✓ Install software like pop-up/ ad-blocker to block the malicious advertisements appearing on websites.
- ✓ Install antivirus and antimalware solutions in your devices and keep them updated.
- ✓ Hover (Mouse Over) over the images/links to find the actual link.
- ✓ Do not install any apps through links received on chats or social media posts.

8. Social Media Frauds

- Scammers use "bots" to trick unsuspecting users into making online payments to accounts under their control, such as through internet banking or UPI transfers.
- Fraudsters use Fake Profile of the victim:
  1. To spread false or fake information.
  2. Sends friend requests to other friends of victim to gain financial benefits.
  3. To damage the reputation of the victim.

Safety Tips

- ✓ 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.
- ✓ Never click on suspicious links or download any app received through messages until you verify the authenticity of the source.
- ✓ Use different passwords for different social media accounts and emails.
- ✓ 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 anyone.
- ✓ 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 users.

9a. Attacks Targeting Senior Citizens

Fraudsters target Senior citizens as they are more vulnerable to online financial scams and frauds.

Senior Citizens must exercise caution when they are online.

Financial frauds targeting Senior Citizens.

- Fraudsters target senior citizens as they are more vulnerable to online financial scams and frauds.
- Senior citizens must exercise caution when they are online.
- Fraudsters trick victims to provide personal sensitive information like Date of Birth, credit or debit card numbers, passwords, OTPs, etc to steal their money.
- Fraudsters target senior citizens through fake insurance schemes, low- cost medications, card renewal, KYC verification, free gifts and offers.
- Fraudsters exploit the loneliness of elderly people and deceive them with fake relationships.
- Fraudsters also create fake social media accounts to target senior citizens and convince them to pay money or share banking credentials/OTP/PIN.

Safety Tips

- ✓ Be aware of fraudsters disguising themselves to be from banks or other institutions asking for personal sensitive information.
- ✓ Never share OTP, username, passwords, credit/debit card details, PIN over phone or internet.

- ✓ Never click or download any link/attachments from unknown sources. Avoid shopping online if you are not familiar with it.
- ✓ Always have a lock, PIN, password, or fingerprint to access your mobile/laptop/computer.
- ✓ Enable multi-factor authentication to your emails, banking and social media accounts.
- ✓ Never share sensitive personal information with strangers and in social media.
- ✓ Avoid making charity contributions over phone.
- ✓ Always remember that banks or other financial institutions never ask for your username/password, OTP, PIN, credit/debit card details.

9b. Attacks Targeting Children

Cyberbullying is a form of harassment that includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.

Safety Tips

- ✓ Review your social media privacy settings and restrict to family and known friends.
- ✓ Educate children about password safety.
- ✓ Check their social media accounts and keep track of it. Ensure they don't share easily identifiable information like trackable location.
- ✓ Stop regular engagement on social media.
- ✓ Do not accept “Friend Requests” from strangers on social media. When bullied log off the site, save the chat/ messages/ e-mail, and inform your parents/ teachers/ elders whom you trust.
- ✓ Don't respond. Block the e-mail /messages. Think well before sharing online.
- ✓ Make use of privacy setting and control the posts you do online. Never share your password. Even your friends may misuse your password.
- ✓ Being kind to others online will help to keep you safe.
- ✓ Talk to an adult you trust, about any messages/posts you get online. They can help you to get rid of the bullying.

9c. Attacks Targeting Women

- Morphing is altering or changing the pictures of the person using morphing tools available online. Young girls and women usually fall prey at the hands of the online criminals, who use their photographs posted online and misuse these images by morphing the pictures.
- 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.

Safety Tips

- ✓ Enable your security and privacy features on social media accounts
- ✓ Never share your personal pictures online publicly on social media accounts
- ✓ Use watermark while sharing pictures
- ✓ Enable multi-factor authentication with strong passwords for your social media accounts.
- ✓ Save the evidence and the screen shots for referring to the incident later.
- ✓ Don’t suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.
- ✓ If you observe your fake profile or any such objectionable posts in social media, report to the respective social media help centre.

9d. Attacks Targeting Person with Disability

Fraudulent individuals often pose as authorized representatives to scam people with disability. These scammers will call or email the victim and ask for their personal information. Fraudsters often of er them promising opportunities such as chance to work from home and make extra income.

Safety Tips

- ✓ Before engaging with any unknown person or business online or over the phone make sure no confidential information is shared without confirming who is on the receiving end of any communication.
- ✓ Be aware about the different types of threats and learn to spot a scam.
- ✓ Call 1930 if you become a victim
- ✓ Don't click on any suspicious links and attachments.
- ✓ Don't download any application received through chats, e- mail and social media platforms.

9e. Attacks Targeting Organisation

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.

Safety Tips

- ✓ Do not click on direct link received through emails, text messages etc. asking you to enter your personal/ sensitive information.
- ✓ Avoid using public networks.
- ✓ Avoid reuse of passwords between any website or services.
- ✓ Report any suspicious emails to at your workplace, instead of deleting the mail.
- ✓ Invest in password management tool, as it is hard to remember multiple passwords.
- ✓ Always change the passwords when employees leave the organisations. Implement multi-factor authentication.
- ✓ Keep your software up-to-date.
- ✓ Use a secure file-sharing solution to encrypt data. Use updated antivirus and anti-malware solutions.
- ✓ Use a VPN to encrypt your connection and protect your private information. Backup important data.

10. Always use strong and complex passwords

Safety Tips

- ✓ Never use your name, age, birthday, phone number, address, place, or any other sensitive personal information as part of your password.
- ✓ Use unique password for each account.
- ✓ Make long passwords by mixing upper case, lower case, numbers and symbols.
- ✓ Don't share your password with anyone. Enable multi-factor authentication.
- ✓ Regularly change passwords.

11. Ransomware

Ransomware is a specific type of malware or malicious software that holds data hostage in exchange for a ransom. It threatens to publish, block, or corrupt data or prevent a user from working or accessing their computer unless they meet the attacker's demands.

Safety Tips

- ✓ Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- ✓ Do not pay the ransom. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
- ✓ Lookout for the latest scams! Currently, “ransomware” is on the rise. Make sure you do not click or download links from unknown sources. Hackers can steal your credentials and encrypt your data and demand ransom to decrypt it
- ✓ Ensure your applications and operating systems (OS) have been updated with the latest patches. Vulnerable applications and OS are the target of most ransomware attacks.
- ✓ Always perform regular backups on important data and keep the backup copies disconnected from the computer.
- ✓ Always disconnect system from internet whenever such attack happen.

12. IMMEDIATE STEPS TO FOLLOW IN CASE OF CYBER ATTACK.

- ✓ Disconnect your internet.
- ✓ Disable remote access.
- ✓ Maintain your firewall settings.
- ✓ Change your passwords.
- ✓ Install any outstanding security updates or patches.

13. Basic Cyber Hygiene

- Use genuine software
- Keep your software up-to-date Avoid opening suspicious emails
- Think before you click on suspicious links/ attachments

- Use updated anti-virus and anti-malware
- Use updated browsers
- Use strong passwords and regularly change them
- Don't share your passwords with anyone
- Enable Multi-Factor Authentication
- Avoid using public Wi-Fi networks for secured transactions
- Regularly take backup of your data

14. Advisories

Visit : https://www.cert-in.org.in
Visit : https://www.csk.gov.in/security-best-practices.html
Visit : https://i4c.mha.gov.in/

CYBER SWACHHTA KENDRA

Security Tools

Free Bot Removal Tool- For Microsoft Windows
eScan Antivirus K7 Security Quick Heal
Free Bot Removal Tool - For Android

eScan Antivirus

Free Mobile Security Application - For Android

M-Kavach 2

Other Relevant tools:

USB Pratirodh
App Samvid
Browser JSGuard

15. INCIDENT REPORTING CONTACT DETAILS

A). UT Helpdesk (DNH & DD) for reporting Cyber Incidents.

	Cyber Cell Dadra Nagar Haveli	Cyber Cell Daman	Cyber Cell Diu
Address	Police Head Quarters, Dadra & Nagar Haveli	Technological & Cyber Criminal Cell(TAC Cell) Office of Suprintendent of Police, Daman, Near State Bank of India, Paanch Rasta, Nani Daman.	SP Office , Fudam, Diu.
Helpline No.	155260		
Contact No.	0260-2642130	0260-2250942/0260-2251104	02875-254441
Email id:	Itcell : dnhp@mha.gov.in	phq-dd@gov.in	Ps.diu-dd@nic.in

	Cyber police : dnh@gov.in		

B). Cert-In contacts details for reporting (Central Help Desk).

Incident Computer Emergency Response Team (Cert-In)

Address : Ministry of Electronics and Information Technology

Government of India, Electronics Niketan,

6, CGO Complex, Lodhi Road, New Delhi – 110 003, INDIA.

- If the query related to cyber security incident, you can report or contact at:
  - Contact: 1800114949
  - Email: incident@cert-in.org.in
  - Fax: 1800116969
- If the query related to vulnerability report, security alert, or any other technical issues/feedback, you can contact at:
  - Ph: 011-22902657 / 1800114949
  - Email: info@cert-in.org.in , advisory@cert-in.org.in , subscribe@cert-in.org.in , csk@cert-in.org.in
  - Fax: 1800116969

C). For Reporting Cyber Fraud & Crime to I4C.

Visit website: https://www.cybercrime.gov.in

Call : 1930