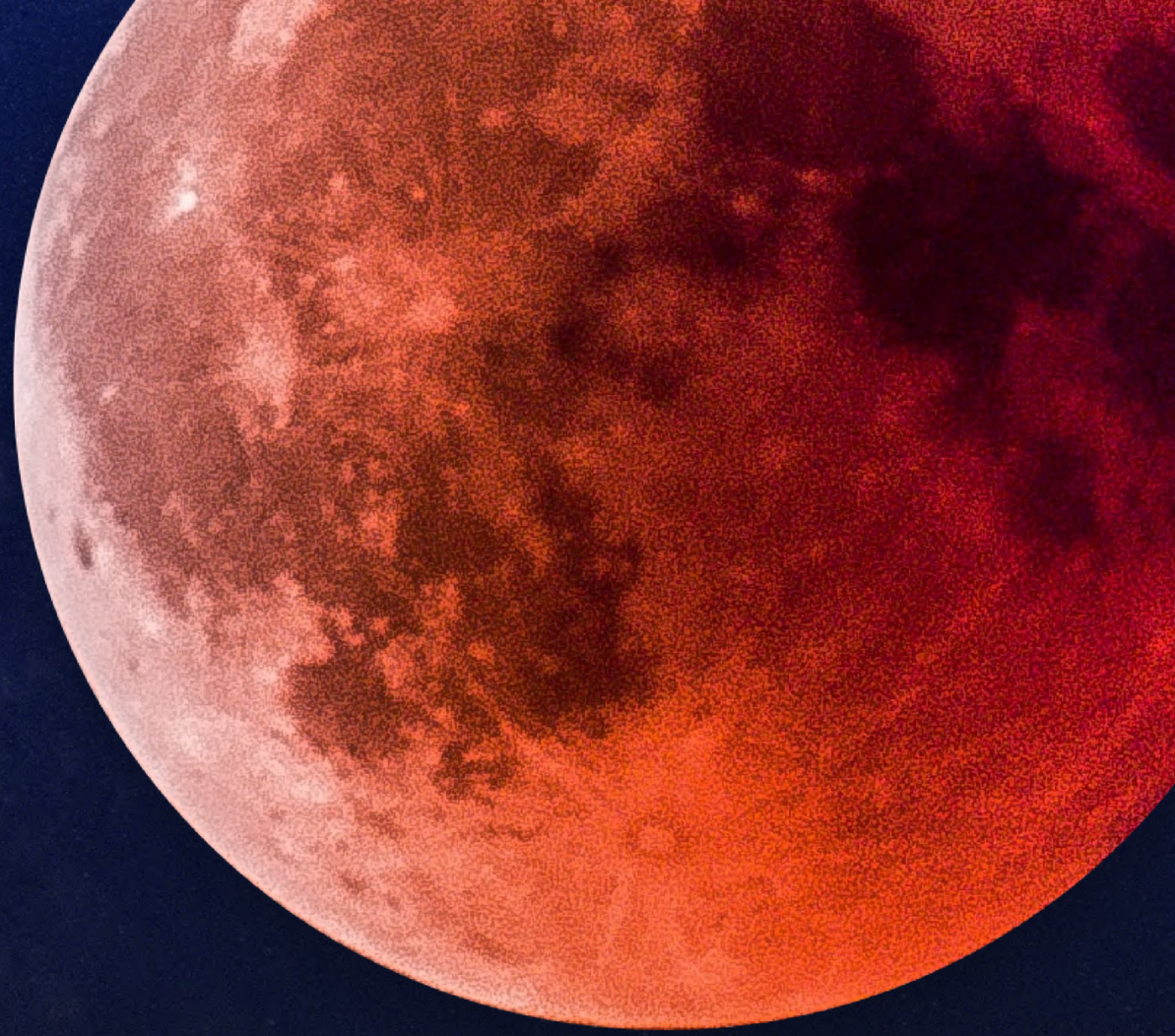
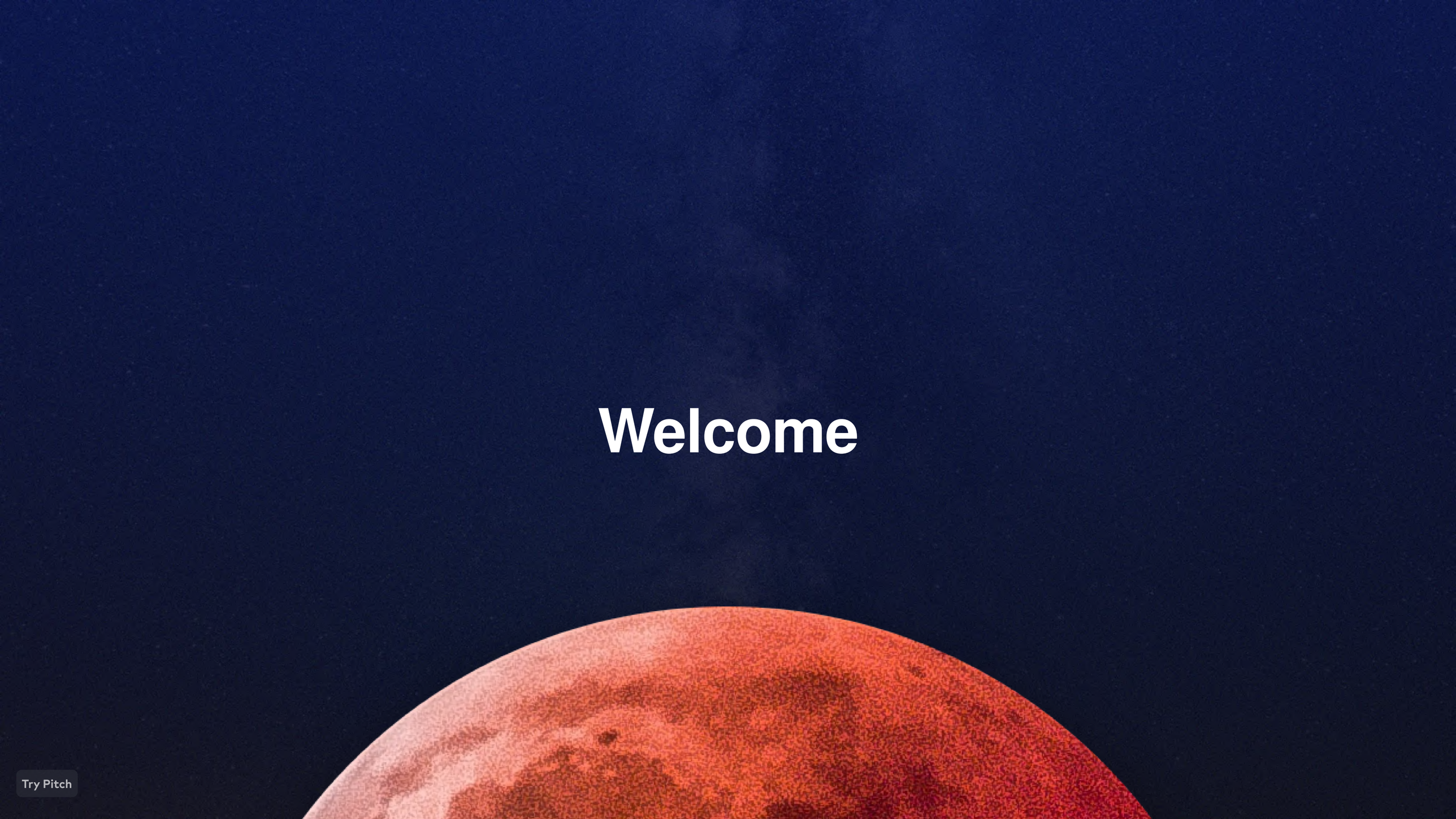


PCI DSS

Data Security Awareness Training

Welcome



SECTION 01

PCI DSS Basics

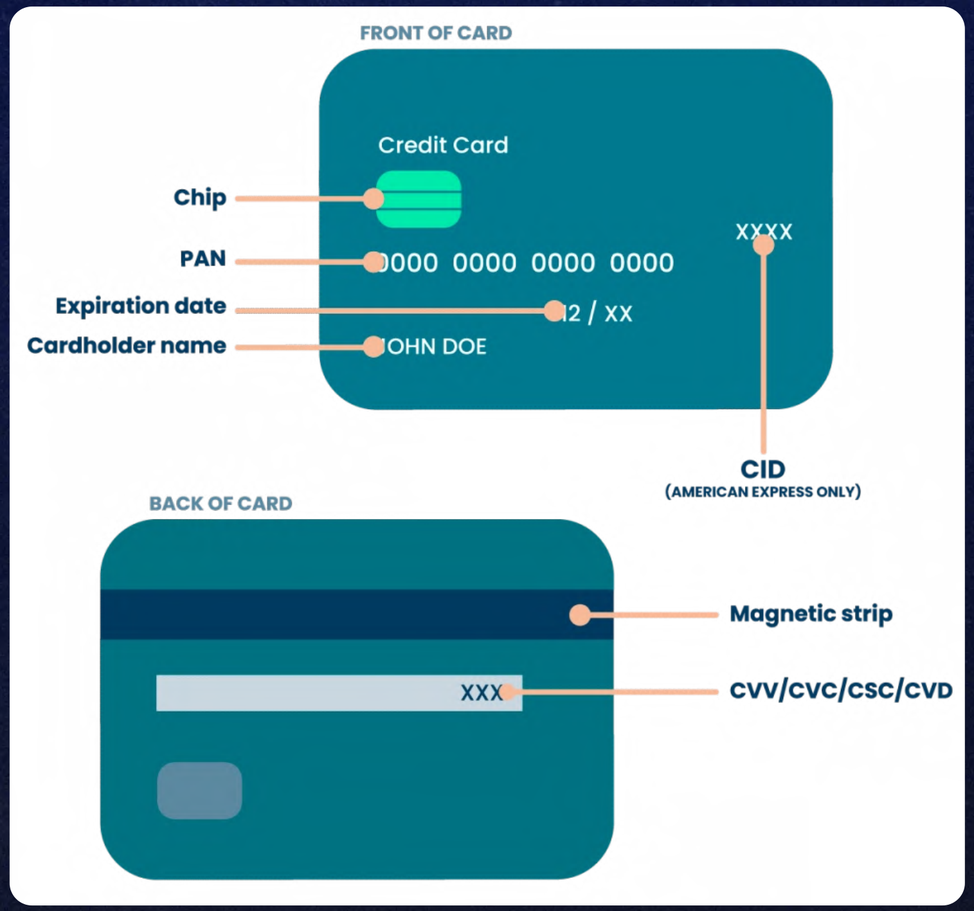
What is PCI DSS?

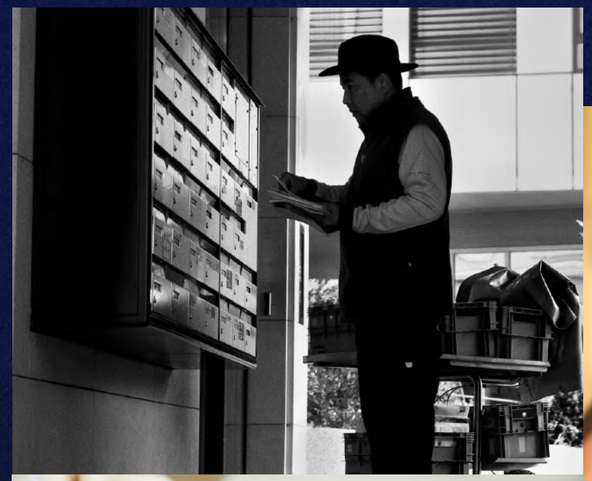
- The Payment Card Industry Data Security Standards (PCI-DSS) are requirements of the merchant card brands (Visa, MasterCard, Discover, American Express)
- PCI-DSS were created on behalf of the brands by the PCI Security Standards Council
- The goal of PCI-DSS is to protect cardholder data

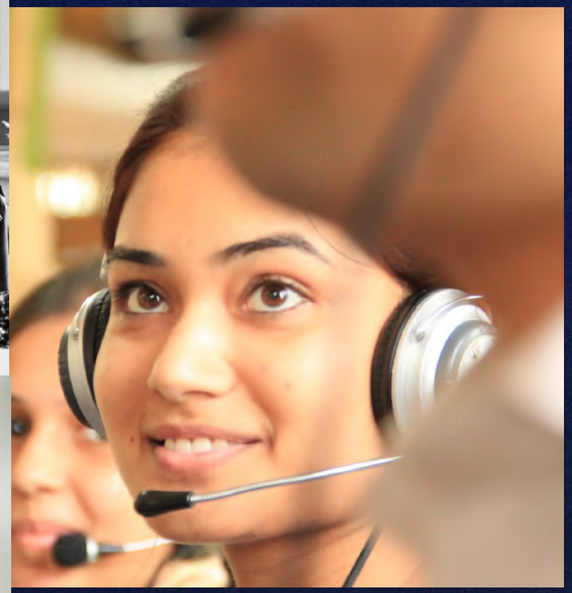
What is Cardholder Data?

1. Cardholder data to be protected includes:
   - Cardholder's name
   - Primary account number (PAN)
   - Expiration date (month/year)
   - Track data (On magnetic strip)
   - Security code / Card Verification Value (CVV)
   - PIN number (Debit cards only)

2. Cardholder data can be in:
   - Paper form or
   - Electronic form







Applicability of PCI-DSS

- PCI-DSS apply to anyone who does any one of the following:
  - Stores
  - Processes, or
  - Transmits cardholder data

- PCI-DSS apply to all forms of payment card acceptance:
  - Mail
  - Phone
  - Fax
  - Point-of-sale Online (Web)

Twelve Requirements of PCI-DSS

BUILD AND MAINTAIN A SECURE NETWORK

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

PROTECT CARDHOLDER DATA

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

IMPLEMENT STRONG ACCESS CONTROL MEASURES

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

REGULARLY MONITOR AND TEST NETWORKS

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY

12. Requirement 12: Maintain a policy that addresses information security

SECTION 02

How to ensure data security

Personal Responsibility

- As an employee, contractor, or volunteer who interacts with credit card details frequently, becoming the first line of defense against fraud and security breaches
- You are expected to know the organization’s policies and procedures, like data protection policy, data confidentiality policy, etc. as this helps you to be vigilant when working with payment card data and credit card transactions

Best Practices

CREDIT CARD RECEIPTS

Ensure credit card receipts are stored securely or disposed of responsibly

TRUNCATE PANS

Verify that both the card receipts only bear truncated versions of the primary account number (PAN)

PHYSICAL PROTECTION OF DEVICES

Physically inspect for fraudulent skimmers that may be attached to devices, and to check for fraudulent substitution by checking the serial numbers of the devices

PHYSICAL SECURITY OF CARD MEDIA

Do not leave any paper or electronic card media physically unsecured

EMAIL CONTAINING PANS

Do not send any unencrypted emails containing the full primary account number (PAN). The truncated last four digits are okay to send

RESTRICTED ACCESS

Restrict physical access to areas where cardholder data is handled and stored. Visitors in areas where cardholder data is stored must be identified and escorted, with a visitor's log being maintained

SECURITY ID CODES

Never write down, store, or email the security ID code. If provided to you, the number is only to be retained until the authorisation has been approved by the card processor

PASSWORDS

Do not write down passwords for others to find, or share your password. Do not use vendor-supplied defaults for system passwords and other security parameters

OWASP Secure Coding Practices Guide can be accessed by clicking here

In case you aren't in a development role, please feel free to skip this slide

General Coding Practices

- Use tested and approved managed code
- Utilise task-specific built-in APIs to conduct operating system tasks.
- Use checksums or hashes to verify the integrity of interpreted code, libraries, executables, and configuration files
- Utilize locking to prevent multiple simultaneous requests
- Utilize synchronization mechanism to prevent race conditions
- Protect shared variables and resources from inappropriate concurrent access
- Explicitly initialize all variables and data stores
- If elevated privileges are required, raise privileges as late as possible, and drop them as soon as possible
- Avoid calculation errors by understanding your programming language's underlying representation and how it interacts with numeric calculation.
- Do not pass user supplied data to any dynamic execution function
- Restrict users from generating new code or altering existing code
- Review all secondary applications, third party code and libraries to determine business necessity and validate safe functionality
- Implement safe updating. If the application will utilize automatic updates, then use cryptographic signatures for your code and ensure your download clients verify those signatures. Use encrypted channels to transfer the code from the host server

What Constitutes a Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of card holder data.

A breach could result from many activities.

- Accessing more than the minimum necessary information
- Failing to log off when leaving a workstation
- Unauthorized access to Card Holder Data either physical or digital
- Sharing confidential information, including passwords
- Improper disposal of confidential materials in any form
- Copying or removing Card Holder Data from the appropriate area

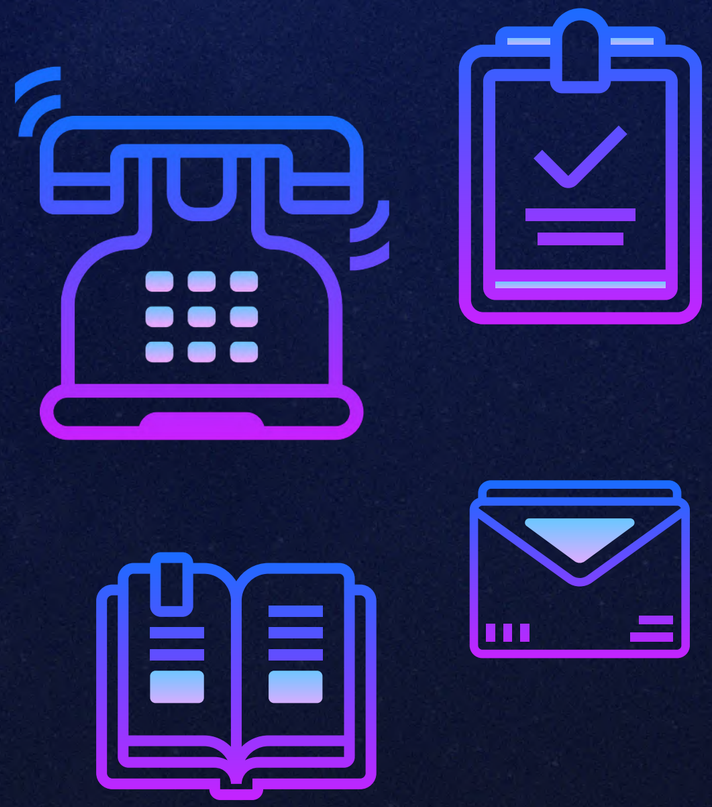
Security Incident Reporting

The below steps need to be followed in the event of a breach.

1. Notify your supervisor immediately of any suspected or real security breach or of stolen cardholder data
2. Document any information you know while waiting for a response to the incident, including date, time, and the nature of the incident

In case of a network environment:

1. Do not access or alter compromised systems
2. Do not turn the compromised machine off
3. Isolate compromised systems from the network
4. Preserve logs and electronic evidence
5. Log all actions taken



THANK YOU

Stay Safe