PCI Security Standards Council

Work from Home Training Supplement

Abbreviations & Definitions:

Account Data	Also known as payment account data, account data includes CHD and SAD.
Cardholder Data (CHD)	Includes the following account data: • Account number or PAN • Cardholder Name • Expiration Date • Service Code
Card Security Code or Value (CSC/CSV)	The three to four digits value visible on either the front or the back of a payment card.
Internet of Things (IOT) Devices	Any wi-fi connected object or device, such as smart speakers, cameras and appliances, that sends and receives data automatically through the Internet.
PCI Data Security Standard (DSS)	A data security standard or set of rules for securing systems and protecting payment account data.
Phishing	A type social engineering attack, most commonly orchestrated through emails and text messages, used to persuade individuals to hand over sensitive information, such as passwords, financial information, and other sensitive data, or to get them to perform certain tasks, such as downloading malware or completing a payment or wire transfer.
PIN Block	A PIN formatted, and encrypted a certain way, used to protect the PIN when outside of a secure device.
Primary Account Number (PAN)	The account the number printed on the front or back of a payment card.
Ransomware	A type of malware that attackers use to infect computers and encrypt computer files until a ransom is paid. When downloaded, ransomware will attempt to spread to connected systems, including shared storage drives and other accessible computers.
Sensitive Authentication Data (SAD)	Includes the following account data: • Data encoded in the magnetic stripe or chip • Card security code or value • PIN, or “personal identification number” • PIN Block
Service Code	A value in the magnetic stripe of a payment card, used for restricting card usage and differentiating between how international and national payments are processed.
Virtual Private Network (VPN)	A secure service that creates a private network from a public internet connection and establishes secure and encrypted connections in which to send and receive communications.
Wi-Fi Protected Access (WPA)	A security protocol or setting for wi-fi enabled devices, which is designed to create secure wireless networks.

PCI Security Standards Council

Key WFH Training Takeaways:

- Reduce handling of CHD and SAD to situations and locations where it is absolutely needed.
- Avoid writing, recording, transmitting, or storing of account data whenever possible.
- Any account data recorded on forms, notes, and applications, must be properly protected, or immediately destroyed after use using a **crosscut** shredder or stored in secure containers, specifically intended for media destruction.
- SAD should **never** be stored after authorization under any condition.
- Never send account data is through insecure messaging technologies, such as e-mail, instant messaging, SMS, and chat windows.
- Use an approved VPN service to secure communications between your computers and handheld devices and your organization's corporate network.
- Secure your home wireless router by changing or disabling default user accounts, passwords, and SSID, enabling WPA2 or WPA3 security, and disabling the SSID broadcasting.
- Place wireless access points in physically secure locations to help prevent unauthorized access.
- Try to avoid using public wi-fi whenever possible, such as within airports, hotels and cafes, and instead use a personal hot-spot or mobile phone connection instead.
- Connect only necessary IoT devices to your home network, using a separate guest network (when possible) to segment them from work computers and devices.
- Change default credentials for IoT devices.
- Routinely update your work devices with the latest firmware and security patches from approved vendors and sites. Set the devices to auto-update whenever possible or feasible.
- Use sufficiently complex and unique passwords. Do not share or write passwords down.
- Only use company approved devices for handling of cardholder data and sensitive authentication data.
- Only use and install approved and necessary applications, software, and services on your work devices.
- Ensure that your antivirus software is installed, actively running, and enabled for auto updates for all work devices.
- Disable Bluetooth and wireless functions on work devices when they are not needed or being used.
- Do not open suspicious looking e-mails. Instead, notify your organization's information security team, hotline or IT desk of any suspicious looking emails and follow their recommended course of action.
- Do not connect any devices to the corporate network, or install any software, applications, or peripherals, without first checking your organization's acceptable use policy to determine whether that device or technology has been approved.
- Lock your workstation and secure all sensitive materials when you are away from your work area. Do not leave laptops, smartphones, or other work devices unattended in public areas.

Useful References and Links:

PCI Standards Security Council Website
https://www.pcisecuritystandards.org

Getting Started with PCI:
https://www.pcisecuritystandards.org/merchants/

FAQs
https://www.pcisecuritystandards.org/faqs

PCI Newsroom and Announcements:
https://www.pcisecuritystandards.org/about_us/newsroom_overview

Document Library
https://www.pcisecuritystandards.org/document_library

Payment Data Security Essentials: Patching
https://youtu.be/0NGz1mGO3Jg

Payment Data Security Essentials: Remote Access
https://youtu.be/MxgSNFgvAVc

Payment Data Security Essentials: Strong Passwords
https://youtu.be/dNVQk65KL8g