Guidance for PCI DSS Training

The Payment Card Industry Data Security Standard requires *a formal security awareness program to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.*

For workforce members who transact credit card payments or access cardholder data

9.5.1.3 Training is provided for personnel in point of interaction (POI) environments to be aware of attempted tampering or replacement of POI devices, and includes:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behavior around devices.
- Periodically inspecting POI devices to look for tampering (e.g., "skimmers") or unauthorized substitution.
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to:

- Phishing and related attacks.
- Social engineering.

12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies.

For the organization's incident response team (including outsourced IT support)

12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.

For software developers (where applicable)

6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

Frequency

12.6.3 Personnel receive security awareness training as follows:

- Upon hire and at least once every 12 months.
- Multiple methods of communication are used.
- Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.

Retention

Retain records of completed training as evidence of compliance including:

- Training materials
- Date
- Attendee names
- Policy acknowledgement for each attendee (recorded in writing or electronically)

Reference: Payment Card Industry Data Security Standard Version 4.0.1 (June 2024)