

# Click Thinking Spotlight

## PCI—DSS

Payment cards are the backbone of modern commerce. Understanding Payment Card Industry Data Security Standards can protect both those who use them and the companies that process them.

- It's important to understand the Payment Card Industry Data Security Standards, or PCI-DSS, developed to keep cardholder and transaction data from falling into the wrong hands.
- PCI-DSS applies to any business that facilitates payment card transactions and stores, transmits or processes card data.
- A secure network includes a variety of technical controls designed to protect the cardholder data environment. When creating this network, do not use vendor-supplied defaults for system passwords and other security parameters.
- When transmitting cardholder data across open, public networks, it must be encrypted. Furthermore, all paper copies of cardholder data should be stored securely and shredded when no longer needed, and any conversations about cardholder data should be kept private.
- Most data breaches involve some level of social engineering. PCI DSS requires a security awareness program that includes new-hire and annual training to help employees understand how to identify these threats.
- Restrict access to cardholder data on a need-to-know basis and assign a unique ID to each individual with computer access. Physical access to cardholder data should also be restricted.
- Establish a program that outlines and supports information security policies for employees, vendors and contractors.
- Make sure guidelines are clearly communicated, and that resources are available to help clarify, educate and answer questions.
- Adhering to and upholding PCI-DSS is everyone's responsibility. As standards are updated annually it's important to know where to turn if you have questions. A Qualified Security Assessor can be a valuable ally to your company.

### PCI—DSS



For the animated training module on this topic, see your manager or information security rep.