



## WORK FROM HOME SECURITY AWARENESS TRAINING

### IS THIS COURSE RIGHT FOR YOU OR YOUR STAFF?

Let us help you decide – simply answer these few questions...

#### Do you want to:

- ☒ Understand how to better secure your home office environments
- ☒ Build your knowledge of security requirements and best practices for remote working environments
- ☒ Understand potential cyber threats and attacks common to home and remote networks

If you answered YES to any of the above, then the [PCI Work from Home Security Awareness](#) course is for you – or for your staff!

The PCI Working from Home – Security Awareness training course outlines many of the threats and challenges of handling and securing payment account data within home offices and remote working environments. This training also reinforces how following a PCI DSS compliant organization's information security policies and requirements can help ensure that payment account data remains safe.

### WHAT'S IN IT FOR YOU?



Learn about threats facing remote-based working environments and gain tangible, real-world insights on security requirements and best practices.



Understand how you can impact and enforce security of sensitive payment card data and what considerations should be taken to keep your remote working environment protected.



Drive secure payment data handling and compliance with information security policies within your organization.

### WHO SHOULD ATTEND?

Geared to all audiences including executives, managers, as well as staff who are affected by PCI DSS compliance requirements, this course is for anyone working from a home office or remote office environments that may handle payment account data or could affect the security of those individuals or environments that do.

Typical roles can include, but are not limited to, the following:

Operations, customer service, service delivery, human resources, finance, back-office support, order entry, billing, information security/compliance, IT, software development, engineering, data analysis, database administration, service providers, contractors

### WHAT'S COVERED IN THE COURSE?

This course helps to improve security, reduce the risk of data loss, and simplify understanding and adhering to PCI DSS requirements.

- High-level overview of the PCI SSC, and basics around the PCI DSS, including key terms, payment account data and its handling requirements
- Potential security impacts and considerations around home office environments, as well as different types of job roles and functions and how they could impact the security of payment account data
- Common home office equipment security best practices and requirements to mitigate threats to sensitive payment account data
- Types of phishing and ransomware attacks, how to better identify, report and avoid them

## PEOPLE ARE TALKING

“ Not only do I know how to better help keep my company's sensitive data safer, but I now understand what I can do to better keep my own home network environment more secure from outside threats and attacks. ”

“ The transition to work from home environments happened so quickly. I am relieved to have additional reinforcement and guidance on what I should be doing to keep my home office equipment safe and up to date. ”

“ I really enjoyed how straightforward and digestible this training was. Not only do I better understand how to keep my organization's data better secured, but I feel like I now know what I need to do to keep my home office, data and equipment safe from attackers. Thank you! ”

- Guidance around the “dos and don'ts” of remote working
- Understanding Information Security Policies and their intended purpose
- Helpful resources and additional guidance provided through the PCI SSC for securing home office and remote working environments

Upon completion of the course, you (or your staff) will be able to:

- Understand security responsibilities and best practices
- Understand how to identify payment account data and other sensitive data and apply specific handling requirements to keep data secure
- Better identify common phishing and ransomware attacks and what steps to take to avoid unauthorized sharing or disclosure of sensitive data
- Better understand information security policies and why they are important to maintaining a secure cardholder data environment
- Access additional guidance on work from home security requirements and best practices
- Have tools and insight to secure your organization's payment account data
- Support your organization's compliance efforts through your knowledge of how to apply security requirements and best practices to your home office environments

## WHAT TO KNOW BEFORE YOU BEGIN

Previous PCI DSS knowledge is not required, however, it is suggested that you understand the types of sensitive data you handle in your job role and functions and how you can potentially impact the security of your organization's secure environment.

## COURSE DELIVERY

Authoritative course content is delivered as:

- Self-paced, short computer-based training (CBT) course

\* You will earn one (1) Continuing Professional Education (CPE) hours for the CBT course.

There is no exam or qualification required as part of this course.

**REGISTER NOW**



## LOOKING FOR SOMETHING MORE ADVANCED?

Consider [PCI Professional \(PCIP\)](#) eLearning course

**Maximize Knowledge.  
Minimize Risk.**

For more information, please visit our Awareness page on the website, call us at: +1-781-876-6295, or email us at: [administration@pcisecuritystandards.org](mailto:administration@pcisecuritystandards.org)