# On-Demand Security Awareness Training is Now Available

New for 2016! Employees now have access to 12 online security awareness training modules in TEC, our LMS. You can enroll in these on-demand modules by accessing TEC via My Tri-C Space. These modules will help teach you safe practices relating to computer, email, and web and can be helpful to protect you both at home and at work.

Should you have questions about IT Security practices you should be following, please consult the [***Summary of Information Security Practices for Employees***](http://itservices.tri-c.edu/security/documents/information-security-summary.pdf) document, available from the IT Service catalog, <http://itservices.tri-c.edu> from the drop-down *Security* menu.

# Security Awareness Training

Every employee who uses a computer should take one of the following courses Security Awareness Training modules. Modules in this section are all variants with different durations and mostly similar content. The 30 minute “*KnowBe4 Basic Security Awareness*” has the best balance of topic coverage and length and is our recommendation for most employees.

**Kevin Mitnick Security Awareness Training 2016 (15-min) SECUR1002**

This 15-minute module is an advanced, condensed version of the full 45-minute training, often assigned to management. It covers the mechanisms of spam, phishing, spear-phishing, spoofing, malware hidden in files, and Advanced Persistent Threats with an interactive “Red Flags” phishing test at the end, including email best practices.

**Kevin Mitnick Security Awareness Training 2016 (25-min) SECUR1001**

This 25-minute module is a shorter version of the full 45-minute training session. It covers the mechanisms of spam, phishing, spear-phishing, spoofing, malware hidden in files. It has an interactive test at the end.

**Kevin Mitnick Security Awareness Training 2016 (45-min) SECUR1000**This is a 45-minute web-based interactive training using common traps, live demonstration videos, short tests and the new scenario-based Danger Zone exercise. It specializes in making sure you understand the mechanisms of spam, phishing, spear-phishing, malware, ransomware and social engineering, and are able to apply this knowledge in your day-to-day job. The training is split in 4 modules.

**KnowBe4 Basic Security Awareness Training Course (30-min) SECUR1003**

This KnowBe4 Security Awareness Training is 30 minutes long. It has the Your Role section from our 45 min. course. It also contains the shortened Red Flags section and a new "Common Threats" section that covers the Fake Excel/CEO fraud threat as well as ransomware, and has a 10-question assessment at the end.

# Information Handling

Courses from this section are recommended for those employees who work with sensitive data. *Handling Sensitive Information Securely* is recommended for anyone who falls into this category. The *Basics for Credit Card Security* and/or *PCI Compliance Simplified* are for anyone who handles credit cards or credit card data.

**Basics of Credit Card Security SECUR1008**

This 20-minute module covers the basics of credit card security. It is meant for all employees in any organization who handle credit cards in any form, whether taking orders on the phone, swipe cards on terminals or through devices connected to smart phones. It teaches employees to handle credit card information securely to prevent data breaches. Different types of cards are covered, which specific elements the hackers are after, and explains how malware like keyloggers, password crackers, and spyware can endanger credit card information. Employees are taught the rules for paper copies of credit card data, and things to remember during data entry, including things NOT to do like sending credit card information through email and text and more. A quiz ends off this module.

**Handling Sensitive Information Securely SECUR1006**

This 15-minute module of the Kevin Mitnick Security Awareness Training series focuses on the importance of safely handling sensitive information, like Personally Identifiable Information (PII), Protected Health Information (PHI), Credit Card data (PCI DSS), including proprietary information. This will help you apply this knowledge in your day-to-day job for compliance with regulations.

**PCI Compliance Simplified SECUR1009**

This 30-minute module uses real examples of credit card fraud, and how to protect your organization against this by being PCI compliant. This course is for anyone that’s responsible for handling credit cards in your organization and qualifies as Security Awareness Training. Especially owners, the CFO or Controller, managers and IT people in charge of credit card processing should take this course. After the training, you are able to download essential references regarding being or becoming PCI compliant.

# Other Topics

These are for anyone who desires to learn more about specific topics or needs additional training in specific areas. Modules *Mobile Device Security*, *Safe Web Browsing*, and *Strong Passwords* would be helpful topics to a quite a number of employees.

**Business Email Compromise/CEO Fraud SECUR1010**

In this 10-minute module, employees are quickly brought up to speed to inoculate them against what the FBI calls "Business Email Compromise" and what is commonly known as CEO Fraud. Concepts like social engineering, email spoofing, and the two ways that CEO Fraud is being perpetrated are covered. There is a short video with a live demo of an infected Excel file, and a short quiz to test understanding at the end. Downloadable PDF Resources: Social Engineering Red Flags, and Security Awareness: Best Practices.

**Mobile Device Security SECUR1007**

This 15-minute module teaches the importance of Mobile Device Security. You will learn the risks of their exposure to mobile security threats and apply this knowledge in your day-to-day job.

**Ransomware SECUR1004**

This course takes an employee through the basics of what ransomware is, how it came to be, and what the risks of ransomware are. It's 25 minutes long and has a 10-question assessment at the end.

**Safe Web Browsing SECUR1011**

This interactive module will teach you how to safely use the internet to stay safe while online. Learn about common pitfalls online and how to avoid them. Please note that there is no sound with this training.

**Strong Passwords SECUR1005**

This 15-minute module covers the rules of how to create and use strong passwords in both an office environment and at the house. Learn the 10 important rules for safer passwords, minimum password length, how to remember long passwords, get trained in best practices like using pass phrases and how to use a different password for every website.

# Example curriculum

A sample well-rounded curriculum for an employee that works with sensitive data and credit cards might include:

* **KnowBe4 Basic Security Awareness Training Course (30-min) SECUR1003**
* **Handling Sensitive Information Securely SECUR1006**
* **Basics of Credit Card Security SECUR1008**
* **Safe Web Browsing SECUR1011**
* **Strong Passwords SECUR1005**

# Signing Up

Employees can sign up for these modules by accessing our TEC system via My Tri-C Space.

1. Log in to My Tri-C Space ([www.my.tri-c.edu](http://www.my.tri-c.edu))
2. Click on the *Employee* tab
3. Click on the TEC logo: 
4. Either type SECUR in the Search box or
5. Highlight *Learning* then select *Browse for Training*
6. Click on *Technology* under the subject
7. Click on *Security* under subject
8. Click on the desired training module
9. Click *Launch*

Brought to you by the Office of Safe and Secure Computing