2017 On-Demand Security Awareness Training

On-demand interactive and video security awareness training modules are available to all Tri-C employees. These modules will teach you how to avoid threats relating to computer, email and the web. This information will not only help you at work, but will help you protect your home computer and personal accounts as well.

All modules are accessible via TEC on your *my Tri-C space* employee page.

Should you have specific questions about IT security practices at Tri-C, please consult the **Summary of Information Security Practices for Employees**, accessible from the Security drop-down menu in the IT Service catalog (http://itservices.tri-c.edu), or contact David Mastny, manager of information security, at david.mastny@tri-c.edu.

Security Awareness Training

Every employee who uses a computer should take one of the following core modules. Because these modules include similar and overlapping content, it is not necessary to take more than one. We recommend the 30-minute "KnowBe4 Security Awareness Training" module for most employees.

**Denotes new or updated content*

*Kevin Mitnick Security Awareness Training (15 mins.)

This module is an advanced, condensed version of the full 45-minute training. It covers the mechanisms of spam, phishing, spear-phishing, spoofing, malware hidden in files and Advanced Persistent Threats.

*Kevin Mitnick Security Awareness Training (25 mins.)

This fully interactive module takes you on a tour of the threat landscape and shows you the most common ways bad guys try to trick you. You'll learn how to spot red flags that alert you to possible danger in an email and then you'll help Jake Sanders, a typical computer user, steer clear of six real-world social engineering attacks.

*Kevin Mitnick Security Awareness Training (45 mins.)

This fully interactive module takes you on a tour of the threat landscape and shows you the most common ways bad guys try to trick you. Three real-world scenarios show you strategies and techniques hackers use to take control of your computer system. Kevin Mitnick then takes you behind the scenes to see how the bad guys do what they do. You'll learn about the seven areas of an email that can contain red flags that alert you to a possible attack. The Danger Zone exercise will let you apply what you've learned when you help Jake Sanders, a typical computer user, steer clear of six real-world social engineering attacks.

*KnowBe4 Security Awareness Training (30 mins.)

This fully interactive module takes you on a tour of the threat landscape and shows you the most common ways bad guys try to trick you. Three real-world scenarios show you strategies and techniques hackers use to take control of your computer system. You'll learn about the seven areas of an email that can contain red flags that alert you to a possible attack. The Danger Zone exercise will let you apply what you've learned when you help Jake Sanders, a typical computer user, steer clear of six real-world social engineering attacks.

Other Topics

These modules are for those who would like additional training in specific areas. “Mobile Device Security,” “Safe Web Browsing,” “Creating Strong Passwords,” and “Handling Sensitive Information Securely” are helpful topics for most employees to explore.

Basics of Credit Card Security (20 mins.)

This 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, swiping cards on terminals or through devices connected to smartphones. It teaches employees how to handle credit card information securely to prevent data breaches. The module covers different types of cards, which specific elements hackers are after and how malware like keyloggers, password crackers and spyware can endanger credit card information. Employees learn the rules for keeping paper copies of credit card data as well as for electronic data entry, including why credit card information should never be sent via email or text.

Business Email Compromise/CEO Fraud (10 mins.)

In this module, employees learn how to protect themselves against what the FBI calls "Business Email Compromise" and what is commonly known as CEO fraud. Concepts like social engineering and email spoofing are covered. The module includes a short video with a live demo of an infected Excel file, along with downloadable PDF resources and a short quiz to test understanding.

*Common Threats (15 mins.)

In this module, you’ll learn about strategies and techniques hackers use via three real-world scenarios. At the end of each scenario, Kevin Mitnick will take you behind the scenes and reveal exactly how each type of hack is accomplished.

*Creating Strong Passwords (10 mins.)

This module covers 10 rules for creating strong passwords. You can test your own password to get an idea of how strong it is. Also learn about the latest trend in password security — the passphrase — and how to create one.

*Danger Zone Exercise (10 mins.)

In this module, you will learn to spot real-world social engineering attacks by helping to guide Jake Saunders, a typical computer user, through six potential attacks. Jake must make the right decisions or suffer the consequences.

Handling Sensitive Information Securely (15 mins.)

This module focuses on the importance of safely handling sensitive information, like Personally Identifiable Information (PII), Protected Health Information (PHI) and credit card data (PCI DSS), including proprietary information. Learn how to apply this knowledge in your day-to-day work for compliance with regulations.

Mobile Device Security (15 mins.)

This module teaches the importance of mobile device security. Learn the risks of exposure to mobile security threats and apply this knowledge in your day-to-day work.

PCI Compliance Simplified (30 mins.)

This module uses real examples of credit card fraud to teach you how to protect your organization by being PCI compliant. This course is for anyone responsible for handling credit cards, particularly owners, CFOs, controllers,

managers and IT staff in charge of credit card processing. Includes downloadable reference materials regarding PCI compliance.

Ransomware (25 mins.)

This course takes an employee through the basics of what ransomware is, how it came to be and what the risks are.

Safe Web Browsing (10 mins.)

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

*Social Engineering (4 mins.)

This micro-module defines social engineering and describes what criminals are after. It covers the three main areas of attack: digital attacks, in-person attacks and phone attacks.

*Social Engineering Red Flags (8 mins.)

This interactive module covers the seven areas of an email to pay attention to if you don't want to be hacked. Learn to spot red flags with seven real-life examples.

*Social Media Best Practices (5 mins.)

This micro-module provides a brief overview of best practices for businesses and employees to prevent attacks and protect sensitive information from social media hackers.

*USB Attack (3 mins.)

This micro-module covers the risks of picking up a USB stick and plugging it into a workstation.

*Your Role, Internet Security and You (9 mins.)

Today's threats are sleek, sophisticated and very slippery. They can slide right through your organization's antivirus software and spam filters and go straight to your inbox. This module takes you on a tour of the threat landscape and shows you some of the common ways the bad guys try to trick you.

Signing Up

Employees can sign up for these modules via the TEC system on *my Tri-C space*.

1. Log in to *my Tri-C space* (my.tri-c.edu)
2. Click on the *Employee* navigation button
3. Click on the TEC logo
4. Type SECUR in the search box **OR**
5. Highlight *Learning*, then select *Browse for Training*
6. Click *Technology* under subject
7. Click *Security* under subject
8. Click on the desired training module
9. Click *Launch*