Fiscal Year 2019 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 questions about specific 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 30minute "KnowBe4 Security Awareness Training" module for most employees.

FY19 - Kevin Mitnick Security Awareness Training (25 min)
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.

FY19 - Kevin Mitnick Security Awareness Training (45 Min)
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.

FY19 - KnowBe4 Security Awareness Training (30 min)
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.

Reporting Phishing Emails

Everyone receives both junk and phishing emails. This module helps you to determine when to report a message as phishing as opposed to treating it as junk mail.

FY19 - Using the Phish Alert Button (7 min)
In this module, you'll learn about the Phish Alert Button (PAB), an email plugin that gives you a safe way to handle actual or potential phishing emails. We introduce you to Sam, your Security Awareness Mentor, as he teaches you how to distinguish between spam, phishing, and spear-phishing emails. Using the PAB will forward any suspicious emails to your organization's security team for analysis and delete the email from your user's inbox, preventing future exposure.

Other Topics

These modules are for those who would like additional or focused follow-up training in specific areas. "Mobile Device Security," "Safe Web Browsing," "Creating Strong Passwords," and "Handling Sensitive Information Securely" are helpful topics for many employees to explore.

Basics of Credit Card Security (20 min)
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.

FY19 - Business Email Compromise/CEO Fraud (10 min)
In this engaging and interactive module, you will learn how to defend yourself against what the FBI calls "business email compromise" and what is commonly known as "CEO fraud." You will also learn how and why these attacks occur, as well as how to protect your organization from this serious threat, and then apply this knowledge in a short exercise.

FY19 - Common Threats, Pt 1 - Miranda's Story (15 min)
In this module you'll learn about strategies and techniques hackers use to trick people just like you. We provide you with three real-world-based scenarios that show you how these common threats can take place. At the end of each scenario, Kevin Mitnick will take you behind the scenes and reveal exactly how each type of hack is accomplished.

FY19 - Common Threats, Pt 2 - Kyle's Story (15 min)
In this module, you'll learn about strategies and techniques hackers use to trick people just like you. We introduce you to Kyle Montgomery as he deals with three real-world-based scenarios: Ransomware, Spear phishing, and a Snapchat attack to show you how these common threats can take place. At the end of each scenario, Kevin Mitnick will take you behind the scenes and reveal exactly how each type of hack is accomplished.

FY19 - Creating Strong Passwords (10 min)
This 10-minute module covers 10 important rules for creating strong passwords. You'll test your own password to see how strong it is, and learn about the latest trend in password security, the passphrase and how to create one.

FY18 - Handling Sensitive Information Securely
This 15-minute module 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.

FY19 - Mobile Device Security (10 min)

Hackers want to use your mobile device as a gateway to your organization's data. This interactive module puts the power in your hands so you can protect that data. You will learn about the dangers surrounding Bluetooth, WiFi, apps, and even human error. You will also learn how to protect your organization from these threats, then apply this knowledge in three real-life scenarios.

FY19 – PCI Simplified (25 min)
This module uses real examples of credit card fraud and discusses how to protect your organization against it by being PCI compliant. It is especially important that company owners, the CFO or controller, managers, IT people, and anyone else in charge of credit card processing take this course. The training covers topics like merchant levels, merchant types, Self Assessment Questionnaires (SAQs), new changes in the industry, chip cards, TIP Program, Qualified Integrated Resellers, and the key security requirements for any organization.

FY19 – Ransomware (15 min)
This fun and engaging course will show you what ransomware is, how it works, and how to steer clear of potential threats. You'll meet Sergeant Vasquez, head of our cyber security task force as he takes you through a line-up of the top attack vectors that bad guys use to hold your computer systems hostage until you pay the ransom.

FY19 - Safe Web Browsing (10 min)
This fun, fully interactive course takes you through the basics of safe web browsing. You will learn interesting facts about the World Wide Web, how to avoid common dangers, and the "do's and "don'ts" of safe web browsing. In addition, you will gain some valuable tips on ways bad guys try to trick you and how to browse safely at home. This could be presented as a quiz to take and "see how much you know". One thing to note is that this course does not have any audio.

FY19 - Social Engineering Red Flags (8 min)
This totally interactive module shows you the seven areas of an email to pay attention to if you don't want to be hacked. Once you know where to look, it shows seven real-life examples, and you'll be asked to spot the red flags in each.

FY18 - Social Media Best Practices (5 min)
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.

FY19 - The Danger Zone (10 min)
Welcome to the Danger Zone. 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 social engineering attacks. Jake needs to make the right decisions or suffer the consequences.

FY19 - Your Role, Internet Security, and You (8 min)
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 high quality, 9-minute course takes you on a tour of the threat landscape and shows you some of the common ways the bad guys try to trick you.

FY19 - Micro-module - Social Engineering (5 min)
This 5-minute 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.

FY18 – Micro-module - USB Attack (3 min)
This 3-minute micro-module covers the risks of picking up a USB stick and plugging it into a workstation.