IBM i Cloud Backup & DRaaS
VAULT400

KnowBe4
Human error. Conquered.

KnowBe4 Modules – Platinum Program

Updated 02/15/2018

Kevin Mitnick Security Awareness Training 15 min

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.

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.

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 attack

KnowBe4 Security Awareness Training

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.

Executive Series: Remote and Travel WiFi Dangers

This course is less than five minutes in length. In this module executives and board members will learn about the dangers associated with accessing WiFi remotely or while traveling, which include device loss or theft, remote-access requirements, and vigilance regarding corporate assets.

Executive Series: Securely Working From Home

This course is less than five minutes in length. It provides executives and board members with a high-level view of precautions they need to take to protect sensitive data when working off-site.

Executive Series: Ransomware and Bitcoin

This five-minute course is a high-level view of ransomware and delves into strategies that organizations can use to mitigate potential losses.

Executive Series: Safe Web Browsing With Corporate Devices

In this five-minute course, executives and board members will learn how to operate more safely in a digital environment by creating strong passwords, using biometrics, and incorporating a virtual private network.

Executive Series: Decision-Maker Email Threats

This five-minute course shows executives and board members how to defend themselves against disingenuous communications and use authentication to protect their identity and secure information.

CONTINUED

Executive Series: Social Media Precautions for Executives

In this five-minute course, executives and board members will learn about the dangers of oversharing information, controlling access, assessing potential threats, and identifying vulnerabilities.

Executive Series: Secure Destruction of Sensitive Information

In this five-minute course, executives will learn about destroying sensitive information in a secure way as well as compliance mandates for archiving and maintaining archived data and clearly defining procedures for handling, retrieving, archiving, and destroying sensitive information.

Executive Series: Mobile Device Security

This five-minute course covers key steps executives and board members can take to reduce mobile security risks associated with using their devices, which range from routine device assessments to adding encryption to sensitive access points.

Executive Series: CEO Fraud

This course is less than five minutes in length. It was expressly created for executives and board members. It is a high-level view of strategies that can be used to counter what the FBI calls "business email compromise" and what is commonly known as "CEO fraud."

Executive Series: Social Engineering the Executive

This course is five minutes in length. It was created to show executives and board members techniques social engineers and hackers use to trick senior executives and steps they can take to reduce the risk of falling victim to sophisticated phishing attacks.

Your Role, Internet Security and You

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 is a 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.

The Danger Zone

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.

Common Threats

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.

Creating Strong Passwords

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.

Safe Web Browsing

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.

Social Engineering Red Flags

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.

CONTINUED

Micro-module - Danger Zone Exercise

This 5-minute micro-module is an interactive course all about phishing. There are four scenarios where the learner is asked to spot the potential threat. Each scenario provides valuable feedback based on the learner's responses. There are two versions of this course, one with sound and one without. This version has sound.

Micro-module - Ransomware

This powerful 5-mionute micro-module takes an employee through the basics of ransomware, the different methods used to infect a machine, and how hackers trick unsuspecting users into downloading infected files.

Micro-module - USB Attack

This 5-minute micro-module covers the risks of picking up a USB stick and plugging it into a workstation.

Micro-module - Safe Web browsing

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.

Micro-module - Social Media Best Practices

This 5-minute micro-module provides a brief overview of best practices that businesses and employees can implement to prevent attacks and protect sensitive information from social media hackers.

Micro-module - Handling Sensitive Information Part 2

This 5-minute micro-module covers part 2 of safely handling sensitive information and goes into Protected Health Information (PHI).

Micro-module - Handling Sensitive Information Part 1

This 5-minute micro-module covers the basics of safely handling sensitive information and goes into Personally Identifiable Information (PII).

CEO Fraud

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.

Handling Sensitive Information

This 15-minute module of the Kevin Mitnick Security Awareness Training series specializes in making sure your employees understand the importance of safely handling sensitive information, like Personally Identifiable Information (PII), Protected Health Information (PHI), Credit Card data (PCI DSS), Controlled Unlimited Information (CUI), including your organization's proprietary information and are able to apply this knowledge in their day-to-day job for compliance with regulations.

Micro-module - Credit Card Security Part 1

This 5-minute micro-module covers why it's so important to protect credit card information; what hackers are after, how employees are a key factor in keeping credit card information secure; and how malware can be used to capture this information.

Micro-module - Danger Zone Exercise - No Audio

This 5-minute micro-module is an interactive course all about phishing. There are four scenarios where the learner is asked to spot the potential threat. Each scenario provides valuable feedback based on the learner's responses. There are two versions of this course, one with sound and one without. This version has no audio.

Micro-module - Credit Card Security Part 2

This 5-minute micro-module covers why it's so important to protect credit card information; what hackers are after, how employees are a key factor in keeping credit card information secure; and how malware can be used to capture this information.

CONTINUED

Micro-module - Email Spoofing

This 5-minute micro-module covers the very important topic of email spoofing. It defines social engineering and shows how hackers can infiltrate an organization and create spoofed emails that trick unsuspecting employees. It also covers a real-life example of just how dangerous email spoofing can be.

GLBA Security Awareness Training

In this module, employees of financial institutions are stepped through the concepts of "Non-Public Personal Information", or NPPI, best practices for protecting customers' personal information, the employee's role in ensuring protection of NPPI, what is social engineering and how not to get tricked, how to protect against unauthorized access and misuse of protected information, and how to provide notice of an incident that may compromise customer information security.

Mobile Device Security

This 15-minute module specializes in making sure your employees understand the importance of Mobile Device Security. They will learn the risks of their exposure to mobile security threats so they are able to apply this knowledge in their day-to-day job.

Handling Sensitive Information - Canadian

This 15-minute training module specializes in making sure your employees understand the importance of safely handling sensitive information like Personally Identifiable Information (PII), Protected Health Information (PHI), credit card data (PCI DSS), and other proprietary information. Employees will learn how to identify sensitive information and keep it secure.

Ransomware

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. 20 min.

Creating Strong Passwords

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.

Basics of Credit Card Security

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 explain how malware like key loggers, 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.

Ransomware for Hospitals Training

Hospitals are currently targeted by cyber criminals, penetrating their networks and locking patient files with crypto-ransomware so that no data is accessible for any hospital worker. This short (7-minute) module gives anyone working in a hospital the basics of ransomware, email security and Red Flags they need to watch out for to help prevent very expensive attacks like this.

PCI Simplified

This 15-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. The training covers topics like Merchant levels, Merchant types, Self-Assessment Questionnaires, new changes in the industry, chip cards, TIP Program, Qualified Integrated Resellers and the key security requirements for any organization.

CONTINUED

Financial Institution Physical Security

This 20-minute module covers the protection of your employees, your customers and their funds, the premises, any security devices, computers, and networks, from physical circumstances and events that could cause serious losses or damage. This includes protection from robbery, kidnap/extortion, bomb threat, fire, natural disasters, burglary, and nuclear emergencies.

Micro-module - Strong Passwords

This 5-minute micro-module covers the rules of how to create and use strong passwords in both an office environment and at home. Employees learn the 10 important rules for safer passwords, minimum password length, and how to remember long passwords.

Micro-module - Social Engineering

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.

GDPR

This interactive module provides an overview the General Data Protection Regulation. The goal of this module is to familiarize you with the General Data Protection Regulation, also known as the "GDPR"; what it means to your organization; and what it means to your job function. There will be a few ungraded knowledge checks along the way to help you retain information for real-life scenarios, followed by a graded quiz at the end on how to protect your organization from these threats, then apply this knowledge in three real-life scenarios.

How to Stay Safe for the Holidays

The holidays are a time of great joy and celebration for people around the world…and for cyber criminals. In this video we will go over 5 practices to follow to make yourself a hard target.