

# Cybersecurity

| *Online Course Catalog*



# Cybersecurity Course Catalog

Threats of cybersecurity breaches are on the rise, and agencies must be proactive in protecting sensitive corporate and personal information. Vector Solutions’ online cybersecurity training catalog features courses with up-to-date lessons for browser, email and password security to improve cybersecurity awareness amongst employees and mitigate risks to your agency’s data. With thousands of courses spanning public safety industries, more than 10,000 public agencies rely on Vector Solutions to assign, deliver, track, and report online and in-person training in one place.



## Table of Contents

Cybersecurity training helps public sector personnel recognize and respond to potential cyber threats, safeguarding critical infrastructure and preventing breaches that could lead to significant disruptions and liability risks.



Cybersecurity Training .....	3
State Mandated Training – Texas .....	6





## CYBERSECURITY TRAINING

- [Brain Bites - Staying Safe Online](#)
- [Browser Security Basics](#)
- [Cybersecurity Awareness for Employees: Classifying and Safeguarding Data for Corporate and Personal Use](#)
- [Cybersecurity Awareness for Employees: End-User Best Practices](#)
- [Cybersecurity Awareness for Employees: Security Awareness Essentials](#)
- [Cybersecurity Awareness for Employees: Social Engineering](#)
- [Cybersecurity Overview](#)
- [Email and Messaging Safety](#)
- [Password Security Basics](#)
- [Protection Against Malware](#)



### **Brain Bites - Staying Safe Online (0.25-hour)**

Meet the hackers trying to break into your company, and learn how to recognize the ways they try to use you and your colleagues to steal money, data, and more. Brain Bites micro-learning courses are information-rich and convey important topics with an engaging mix of video and animation. With 5 minute video lessons and 30-minute-or-less courses, Brain Bites are the perfect tool to educate today's busy workforce.

### **Browser Security Basics (0.25-hour)**

A large number of cyber attacks target browser activity. This course provides all staff members with an overview of browser security and ways to browse the web safely. Topics include: the types of browser threats, the basics of browser security and safe browsing practices.

### **Cybersecurity Awareness for Employees: Classifying and Safeguarding Data for Corporate and Personal Use (0.5-hour)**

Failing to become cyber aware, failing to put measures in place that will protect our devices and network is also failing to protect our personal information, our place of business, and our customers. In this interactive online course we will discuss why classifying and safeguarding data is a priority that must not be ignored. We will also list the main types of classifications and state objectives for securing data.

### **Cybersecurity Awareness for Employees: End-User Best Practices (0.5-hour)**

We live in a busy, busy world. When it is so easy to connect to the internet and access vast amounts of information, it is easy to forget the dangers that lie in wait. From hotspots to password management, this interactive online course will walk you through end-user best practices. We will also discuss the importance of administrative rights, define types of physical attacks against privacy, and recommend ways to protect against malware and viruses.

### **Cybersecurity Awareness for Employees: Security Awareness Essentials (0.5-hour)**

In our digital world today, attackers seem to be lurking behind every click of the mouse or tap on the screen. Many people forget that they are the keepers of their own security safety and the security safety of the institutions for which they are employed. In this interactive online course, we learn about the who, what, how, and why of security attacks. We discuss the potential losses associated with a successful security breaches by hackers and will understand the different way in which those security breaches can occur. Finally, we cover important actions you can take within your organization to limit security risks.

### **Cybersecurity Awareness for Employees: Social Engineering (0.5-hour)**

Social engineering is the art of extorting information from employees that can assist a hacker to breach the security of an organization and can be done by a human or it can be done digitally. In this

[\*\*BACK\*\*](#)

interactive online course we will define phishing and identify common features, examples, and how to avoid phishing scams. We will also discuss identity theft and how to protect against it.

### **Cybersecurity Overview (0.25-hour)**

The convenience of web access makes it easy to forget that we need to protect and care for our information. This introductory course provides an overview of cybercrime and cybersecurity, including the basics of cybersecurity along with the effects of cybercrime, the types of cyber threats and how users are susceptible.

### **Email and Messaging Safety (0.25-hour)**

Email is the primary means of attack from cyber-perpetrators. This course provides an overview of cybercrime via email, and how to employ safe email and messaging practices to avoid and help prevent cyber threats, attempts at fraud and identity theft.

### **Password Security Basics (0.25-hour)**

This course provides an overview of password security and management, including the basic principles of password security, the elements of a strong password, and strategies of how to create and maintain passwords.

### **Protection Against Malware (0.25-hour)**

Malware is a primary means of attack for cyber-perpetrators. This course provides staff members with an overview of basic protection against malware. Topics include: the types of malware, how malware works and protective strategies.





## STATE MANDATED TRAINING - TEXAS

- Texas Cybersecurity Awareness for Employees Program

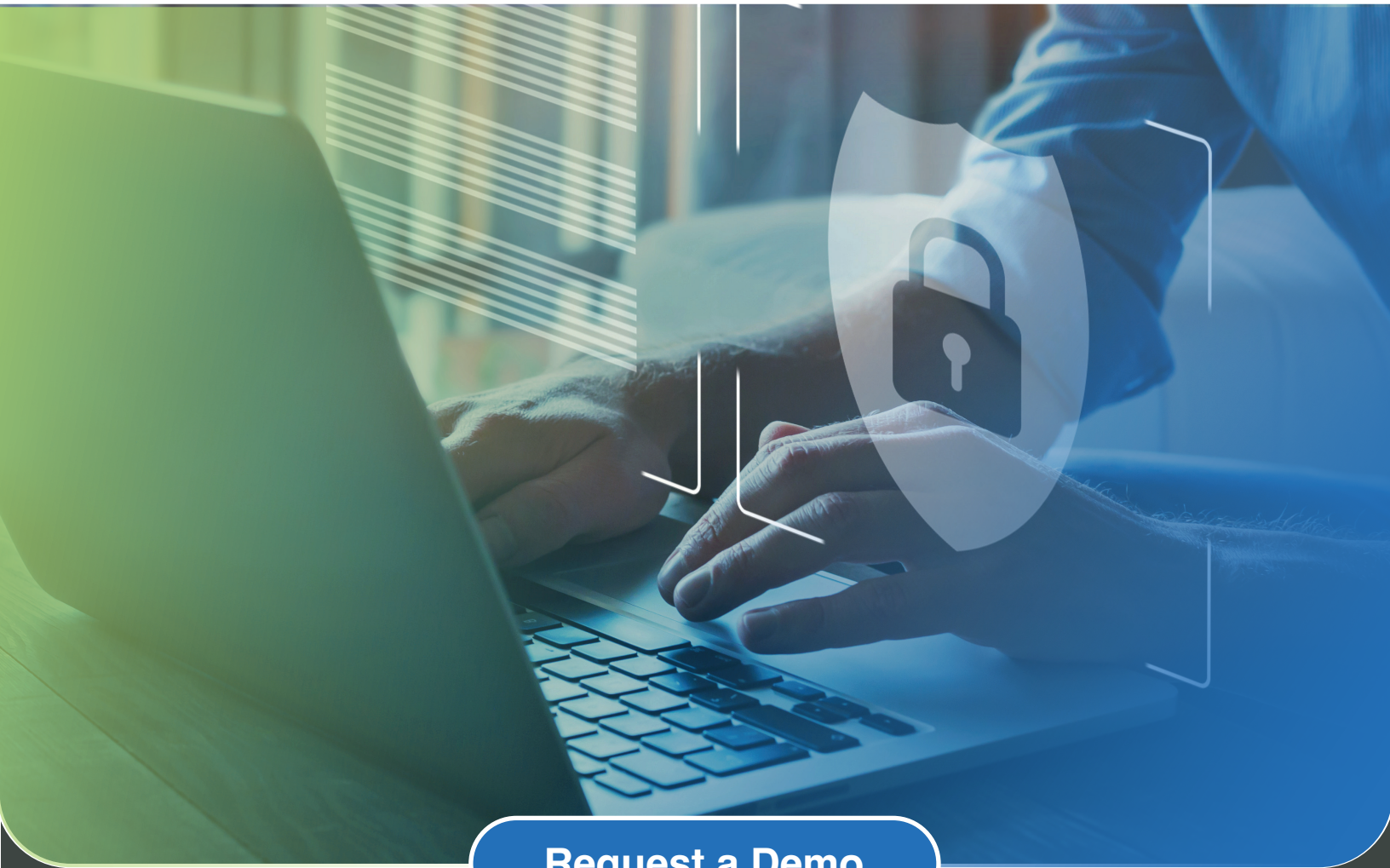




## Texas Cybersecurity Awareness for Employees Program (2-hour)

In our digital world today, attackers seem to be lurking behind every click of the mouse or tap on the screen. Many people forget that they are the keepers of their own security safety and the security safety of the institutions for which they are employed. This program is intended to familiarize employees with Cybersecurity Awareness. The program addresses how an employee is aware and identify the security risk involved with working with an organization's data. Lessons in this program are listed below. Lesson 1: Cybersecurity Awareness for Employees: Security Awareness Essentials Lesson 2: Cybersecurity Awareness for Employees: Social Engineering Lesson 3: Cybersecurity Awareness for Employees: Classifying and Safeguarding Data for Corporate and Personal Use Lesson 4: Cybersecurity Awareness for Employees: End User Best Practices.

[BACK](#)



**Request a Demo**

VectorSolutions.com | 800.840.8046

Technology to  
**TRAIN | PREPARE | RETAIN**  
Your People

