

Symantec Security Awareness

Train Your Organization and Prevent the Next 'Big One'

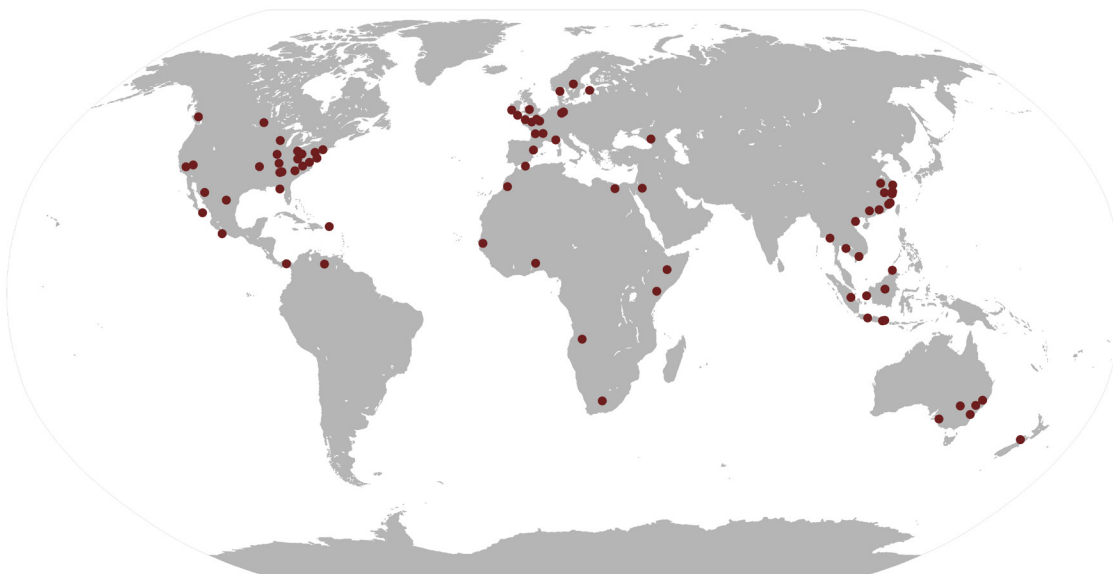
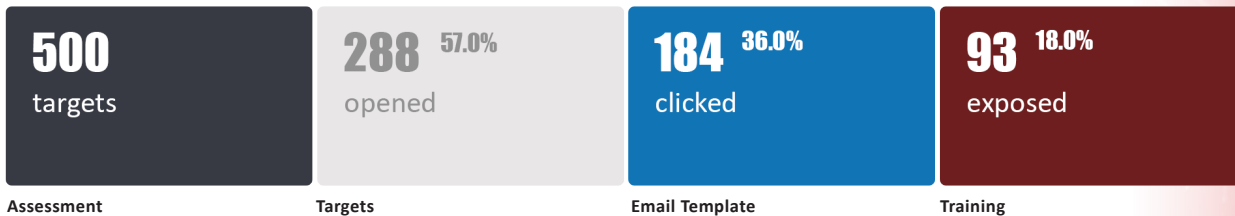
Keep your network safe by training your entire organization with Symantec Security Awareness web-based training. The modules can be integrated into your organization's learning system. We can even customize the training, and provide communications tools and other services to meet your company's security awareness needs and goals.



Your proprietary information is at risk every day and it's not just data that you lose. Data breaches cost money, customers, and even market share. Unfortunately, many breaches result from a lack of employee awareness of the security risks inherent in their actions.

Information security demands that employees practice proactive, security-conscious behavior. The **Symantec Security Awareness Program** trains your employees to understand information security issues and behave in a manner that minimizes risks—all in accordance with current regulatory requirements.

Company sample demo assessment



Symantec Security Awareness Service

Module List and Descriptions

INFORMATION SECURITY, RESPONSIBILITIES, AND PRINCIPLES

Acceptable Use

Language: English

Time: 3 min

Description: Users are consistently told which sites they cannot visit while at work, but many do not know why. This module outlines how those sites may pose a threat to your organization's security in order to discourage users from visiting those sites while at work.

Phishing

Language: English

Time: 5 min

Description: One of the biggest threats to an organization's security is a user that is susceptible to phishing attacks. This module teaches users how to identify different types of phishing attacks.

Passwords

Language: English

Time: 5 min

Description: Creating a complex password isn't hard; remembering it is. This module teaches efficient new methods of creating and remembering complex passwords required for your organization's security.

Privacy

Language: English

Time: 7 min

Description: We all enjoy our privacy, and in today's world, privacy is especially important. This module teaches users what needs to be kept private, and how to best ensure that privacy.

Insider Threats

Language: English

Time: 5 min

Description: Most know that an organization can be attacked from outsiders like hackers and social engineers, but few understand that an organization can be attacked from the inside. This module outlines different ways an organization can be attacked from the inside, as well as how a user can recognize and prevent these types of attacks.

Access Control and Provisioning

Language: English

Time: 4 min

Description: Access Control is a collection of methods and components used to protect information assets. It is used to control the confidentiality and integrity of a secure system and ensures that certain information is available only to those authorized. In this module, we will discuss these methods to help identify those who are not authorized to view or modify secure information.

Media Handling

Language: English

Time: 4 min

Description: A critical component of your organization's security is how your employees handle the data that they are entrusted with. This means they have to manage how they ship, store, destroy, label, and back up media that they use for work purposes.

Information Security for Program Management

Language: English

Time: 4 min

Description: This module focuses on the characteristics of a comprehensive information security program, variables that could impact goals, and how to communicate the effectiveness of the program to internal stakeholders.

Information Security Program for IT Security

Language: English

Time: 4 min

Description: Every member of the IT security team should be aware of all aspects of the security program. More so, they need to understand how those areas affect their current role, as it relates to the overall success of the program.

PROTECTING INFORMATION ON THE INTERNET

Staying Secure Online

Language: English

Time: 9 min

Description: The Internet is a wonderful resource, but without precautionary measures it can be a real source of trouble. This module outlines how to securely use the Internet so that users can take advantage of its resources without exposing themselves to the risks.

THREATS AND RESPONSE

Vulnerabilities, Threats and Controls

Language: English

Time: 4 min

Description: This module will provide an overview of what a software vulnerability is and how they may be exploited. It will also provide a basic understanding of how to position security controls to defend against threats targeting vulnerable systems.

COMPLIANCE

Payment Card Industry Data Security Standard (PCI DSS)

Language: English

Time: 6 min

Description: PCI DSS is an information security standard which was developed to increase security of and protect cardholder data during and after a financial transaction. It provides a global standard of technical and operational requirements, which ultimately result in a much more protected customer. This module is a high level explanation of what PCI DSS is, and how every employee is affected by it.

HIPAA and HITECH

Language: English

Time: 6 min

Description: The Privacy and Security Rules of the Health Insurance Portability Act of 1996 (HIPAA) was created to protect the use, storage and transmission of patients' healthcare information. The Health Information Technology for Economic and Clinical Health (HITECH) is a set of regulations under the American Recovery and Reinvestment Act of 2009 that were put in place to increase the security requirements for handling protected health information. This module provides an overview of HIPAA compliance and a background on HITECH.

SECURING YOUR WORKING ENVIRONMENT

Data Protection and Destruction

Language: English

Time: 5 min

Description: Every day, we handle data that needs to be appropriately disposed of. This module outlines what constitutes sensitive data and how to make sure it remains secure both during and after its use.

Working Remotely

Language: English

Time: 5 min

Description: Working remotely has become very common, leading social engineers to take advantage and hack sensitive information. This module illustrates different practices that should be avoided while working in public to ensure that you and your work are secure.

Physical Security

Language: English

Time: 12 min

Description: This module explains the importance of physical security and keeping the information within your organization safe from a physical standpoint. It focuses on details such as door locks and access cards, making sure that only those who are granted access to a certain location can access it.

Backups

Language: English

Time: 6 min

Description: Do you have insurance on your house, car, or even your life? Backups for your information are like insurance for everything else. It doesn't seem necessary until something terrible happens. This module highlights the importance of backing up your information, and how to effectively do so to avoid losing your data in the event of a compromise.

INFORMATION SECURITY PROGRAM BASICS

SDLC Security Awareness

Language: English

Time: 4 min

Description: Each technology that an organization deploys goes through distinct phases of its deployment. Information security controls need to be integrated at each step to ensure that risk is minimized and each technology runs smoothly. This module focuses on the different steps to ensure this happens.

System Policies

Language: English

Time: 4 min

Description: While federal and program-level policies help establish broad foundational standards, system-specific policies play a key role to ensure the security of computers, networks, applications, and data.

Securing Network Communications

Language: English

Time: 4 min

Description: Ensuring that sensitive information is kept safe and doesn't get into the wrong hands is critical. One example is segregating devices to protect the data that is being submitted. This module focuses on transmitting and storing data via secure methods, such as encryption.

Partnering with the Information Security Department

Language: English

Time: 4 min

Description: The IT department is, in many organizations, the first responder to a security incident. Because of this, it is a critical piece of the overall Information Security puzzle. IT and InfoSec need to work together as a single unit in order to provide a more secure environment.

The Role of the Help Desk in an InfoSec Program

Language: English

Time: 3 min

Description: The Help Desk is a crucial part of the information security program in many organizations. Accordingly, Help Desk personnel should have an understanding of security concepts. This module provides a high level overview of this role and how it relates to the information security program.

Network Security Overview

Language: English

Time: 4 min

Description: Organizations have a large financial investment in network security appliances. What do these expensive devices do, exactly? This module is designed to help end users, network security professionals and CISOs gain a better understanding of optimal placement of network security devices on a network.

Information Security Risk Basics

Language: English

Time: 4 min

Description: Risk is a word we hear quite often: risk of earthquake, risk of stock market meltdown, risk of heart attack. Risk is part of everything we do as humans, and it is something we must consider with our digital information.

Information Security Risk Management

Language: English

Time: 5 min

Description: This module provides an introduction to Information Security Risk Management, including a high level description of key tasks within common information security risk frameworks.

Audit Overview

Language: English

Time: 3 min

Description: The purpose of the Audit and Assessment team is to provide an objective, external set of eyes as a third party to ensure any IT solution is as secure and effective as possible. This module covers those aspects and explains how Audit and Assessment fits into the overall information security posture.

Information Security Roles

Language: English

Time: 11 min

Description: This module explains the importance of each role within an IT department. What do they do? Like a well-oiled machine, each part of team must work efficiently together in order to achieve success.

Overview of Operational Security

Language: English

Time: 14 min

Description: At some point, everyone is entrusted with information that requires protection. Whether it's the password for your work email address or the personal identification number for your bank, keeping this information secure is an important responsibility.

Contracting and System Acquisition

Language: English

Time: 3 min

Description: This module is intended to highlight information security concerns when dealing with third-party providers during the procurement process. After viewing this module, you will be better informed to help identify potential areas of concern and take general steps to reduce the overall level of risk to your organization.

Disaster Recovery and Business Continuity

Language: English

Time: 5 min

Description: What would happen to your organization in the face of disaster? How do you plan for when things go wrong within your organization? With a properly developed and tested disaster and business continuity plan, any potential impacts to your organization can be minimized.

FUTURE RELEASES

Introductory Module

Language: English

Time: 3 min

Description: This module welcomes you to the Security Awareness Training series and provides a sample of the topics addressed within the modules.

Internet of Things (IoT)

Language: English

Time: 5 min

Description: What is the Internet of Things? What does it mean? The Internet of Things is literally a thing that has access to the Internet. In this module, we will highlight the terms associated with the Internet of Things and help you understand the risk versus rewards of internet-connected devices.

General Data Protection Regulation (GDPR)

Language: English

Time: 5 min

Description: While it is a very important European-based privacy regulation, the General Data Protection Regulation (GDPR) reaches worldwide even if you don't live or work in Europe. This module provides an overview of the GDPR, including appropriate security processes for handling and storing sensitive or personal data and proper reporting of any data leakage.

Cloud Access Awareness

Language: English

Time: 5 min

Description: As organizations increase their reliance on cloud-based services, it has become evident that information security organizations need visibility into these services and the management of the associated data.

Ransomware

Language: English

Time: 5 min

Description: Ransomware can appear on your computer at any moment, without notice. Data ranging from important work or personal documents could be encrypted and held hostage until you pay a ransom. This module will provide a high level overview of what to do, should you become a victim.

User Security

Language: English

Time: 4 min

Description: In security, we talk about threats to our users all the time. Yet every organization spends time, money, and resources on security awareness training. The most important thing to remember is that awareness training is two separate acts. The first goal of what we call “awareness training” is literacy. We put users through this training so they have a common vocabulary about information security. The second step in creating a security-aware user is behavior design. Changing user behavior is often taken for granted.

About NetX Information Systems

Trust • Value • Partnership

Established in 1997, we remain a leader in customer service and an innovator in approaching the challenges IT Departments are faced with today. Our philosophy is to establish trust, add value and maintain a long term partnership with our customers and vendors.

Our dedication to a single vendor in each technology area allows us to focus on being subject matter experts in the products we recommend to our customers.

**Data Protection • High Availability • Endpoint Management
Archiving • eDiscovery • Security**