SECURITY AWARENESS

FOR THE 21st CENTURY

"I HAVE NEVER SEEN SUCH HIGH-QUALITY TRAINING, DISTILLED TO A PERFECTED MESSAGE, AND COMPRESSED INTO A TIMEFRAME THAT ANY ORGANIZATION SHOULD WILLINGLY COMMIT EMPLOYEE TIME TO TAKING AS A RISK-REDUCTION STRATEGY."

-JAMES A. (JIM) RICHARDS III
WV CHIEF INFORMATION SECURITY OFFICER

For more information or to demo the training, please visit:
info@securingthehuman.org
www.securingthehuman.org

SANS SECURING THE HUMAN

Introduction

Most organizations have invested in security technology to protect their information, putting in place solutions such as firewalls, encryption or IDS sensors. However, many of these same organizations have failed to address the human element. People, just like computers, store, process and transfer highly valuable information. Yet people remain highly insecure, since so little has been done to educate them. As a result, cyber attackers are actively targeting the human element. Until you address the human issue, technology alone cannot secure your organization.

High-impact security awareness training addresses these issues. It ensures that your users are aware that they are a target; it motivates and changes behavior by teaching them how to use technology securely and ensures your organization remains compliant. In addition, by teaching your users the indicators of compromise and how to report incidents, you go beyond just prevention and begin developing human sensors, creating a far more resilient organization.

Policy, Training and Awareness

Awareness cannot be created in a vacuum. It is the third tier in a pyramid that starts with policy and training. Policy, training and awareness go together in the following fashion:

- Policy tells the user what to do
- Training provides the skills to perform it
- Awareness changes their behavior

Users not knowing what they are supposed to do is a policy issue. If the users do not have the skills for performing what they are supposed to do, then it becomes a training issue. Quite often, the user does not understand why it is important. This is a behavioral issue that needs to be changed – that's the awareness issue.

A Framework for Training

A good security program must be built on a proper framework, thus ensuring there is always a valid reason for why we do what we do. ***Based on validation and effectiveness, SANS has chosen the 20 Critical Controls*** (www.sans.org/critical-security-controls/) ***as the framework for its user awareness program.*** These Critical Controls use knowledge of actual attacks that have compromised systems to identify specific technical and human security controls that are viewed as effective in blocking currently known high-priority attacks, as well as those attack types expected in the near future.

Updated Content

A significant issue for any organization in selecting/developing its own Security Awareness solution is the need to keep the training program fresh and up-to-date with the latest threat vector information. The level of effort needed to maintain the program and keep it updated with the latest attack vector data is significant and often underestimated.

However, this is a SANS core strength area. We use changes in the 20 Critical Controls as guidelines when we update our security awareness training content – a project we perform several times a year to address the latest threats.

Return on Investment

The cost to train an organization's staff to meet its mandated compliance needs significantly outweighs the cost of purchasing the most effective security awareness solution for an organization. Take the example of a company with 1,000 employees requiring security awareness training:

- Option 1: Use an internally-developed, one-hour security awareness presentation addressing required compliance needs and then answer any follow-up questions. The cost to train 1,000 users is (1,000 man-hours) x (an assumed $50 average cost per man-hour) = $50,000 *

  * This does not include the cost to develop your own program.

- Option 2: Invest in a computer-based training solution that takes 30 minutes per person and costs $10,000 to license. The cost to train 1,000 users is now (500 man-hours) x (an assumed $50 average cost per man-hour) + ($10,000 license cost) = $35,000

There are numerous challenges to on-site workshops. First, presentations are only as good as the skills of the presenters, so it is difficult to ensure your program will have a consistent, high-quality message. Plus, it can be difficult to get all members of your organization to attend on-site events at specific times (think about contractors, part-time employees or employees who were not on site). Computer Based Training (CBT) provides the following:

- The ability to scale the training across your organization
- Users can take training on their own schedule
- It ensures that your program communicates a standardized message
- It is easier to track who took the training, which is often required for compliance purposes.

End-User Training

How your organization communicates its awareness program message is as important as what it communicates. We simplify this process by breaking the awareness training program down into short, individual training modules.

Each training module focuses on a specific security topic, demonstrates how it affects the user, and then provides solutions. Multiple communication channels can be used to deliver your training message, including computer-based training, newsletters, posters, and screensavers, ensuring the greatest learning impact for your users.

Each module shares the same images, format and training message across the different communication channels, thereby ensuring your security message is continually reinforced in a consistent manner. And to ensure learning comprehension, each module also comes with quizzes developed by the Global Information Assurance Certification (www.giac.org) team.

All SANS Securing the Human End-User training is:

- SCORM-compliant, so all training activity by users can be tracked and reported.
- Available to host in your own Learning Management System; or SANS can host the training for you via the SANS Virtual Learning Environment – our hosted LMS solution.
- Branded with your company name and logo.
- Able to include links to your own security policies.
- US Federal 508 compliant, so that it is in compliance with the Americans with Disabilities Act.
- Available in 25 languages – Arabic, Chinese, Czech, Dutch, English (USA, British and Australian), Finnish, Flemish, French, German, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese (Brazil), Russian, Spanish, Swedish, Thai & Vietnamese.

Security Awareness Training Modules

Total Time: 77 minutes


You Are The Target

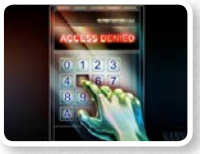

Social Engineering


Email

Browsing


Social Networking


Mobile Device Security



Passwords


Encryption


Data Security


Data Destruction


WI-FI Security


Working Remotely


Insider Threat


Help Desk


IT Staff

Physical Security


Protecting Your Personal Computer


Protecting Your Home Network


Protecting Your Kids Online


Hacked


Senior Leadership


Advanced Persistent Threat


Cloud

Compliance Training Modules

Total Time: 61 minutes


PCI DSS


FERPA


HIPAA


Personally Identifiable Information (PII)


Criminal Justice


Federal Tax

GLBA-EDU

GLBA-FIN


Red Flags Rule


Ethics

International Traffic in Arms Regulations

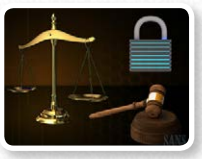

Data Retention

Social Security Numbers


Foreign Corrupt Practices Act


Federal PII


European Union Data Protection


Client Confidentiality for Law Offices

Privacy

Security Awareness Training Modules

MODULE: You Are A Target **TIME:** 2:09 minutes

Employees often believe they are not a target, exposing your organization to tremendous risk. This module addresses that misconception by explaining how they are under attack and why. In addition, we explain that this training will not only protect them at work, but at home as well. This engages people, helping ensure the success of your organization's security awareness program.

MODULE: Social Engineering **TIME:** 2:57 minutes

Many of today's most common cyber attacks are based on social engineering. As such, we explain what social engineering is, how attackers fool people and what to look out for. We then demonstrate a common social engineering attack. We finish with how people can detect these attacks and how to respond to them.

MODULE: Email & Instant Messaging **TIME:** 5:30 minutes

One of the primary means of attacks and exploitation is through email. Email is used for both simple, large scale attacks and more targeted spear phishing attacks. We explain how these attacks work, including recent examples of phishing, spear phishing, malicious attachments and links and scams. We then explain how to detect and stop these attacks.

MODULE: Browsing **TIME:** 3:10 minutes

The browser has become the gateway to the Internet; it is the primary tool that employees use for online activity. As such, browsers and their plugins have become a common target for attackers. We teach people how to browse safely, including keeping the browser and plugins updated, avoiding bad neighborhoods and being careful of and scanning what they download.

MODULE: Social Networking **TIME:** 5:04 minutes

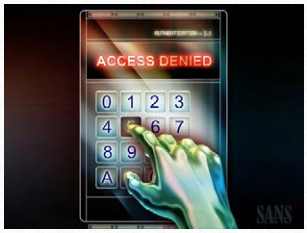
Social networking sites have exploded in popularity, with staff sharing all sorts of private information about themselves and work. Cyber attackers know this and use this information for identity theft, spreading malware, scams and even targeted attacks. We discuss these risks and the steps your employees can take to protect themselves and your organization.

MODULE: Mobile Device Security **TIME:** 3:40 minutes

Today's mobile devices (like tablets and smartphones) are extremely powerful. In most cases, these devices have the same functionality, complexity and risks of a computer, but with the additional risk of being highly mobile and easy to lose. We cover how to use mobile devices safely and how to protect the data on them.

Security Awareness Training Modules

MODULE: Passwords **TIME:** 4:29 minutes

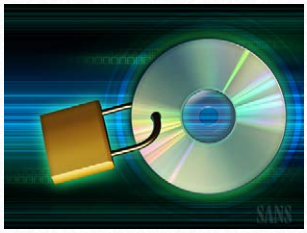


Passwords are the keys to the kingdom and employees must guard them well. We cover what passwords are, why they are important and what makes a strong password, with an emphasis on passphrases. In addition, we cover how to protect and safely use passwords, including the use of different passwords, password managers and not sharing passwords with others.

MODULE: Encryption **TIME:** 1:41 minutes

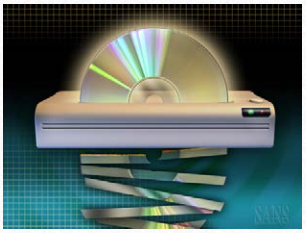
Many recommended security controls use encryption, yet few employees know or understand what encryption is or what it can and cannot do. This module explains in very simple terms what encryption is, how it works and commons examples of what can be encrypted.

MODULE: Data Security **TIME:** 3:47 minutes



Organizations have a tremendous amount of sensitive information that they must take extra steps to protect. This module explains these steps, including the use of only authorized systems to store or process sensitive information, restrictions on transferring or sharing such information and requirements for securely disposing of sensitive data.

MODULE: Data Destruction **TIME:** 1:56 minutes



Many employees mistakenly believe that when they delete data it is gone for good. They are unaware that it can be and is easily retrieved from almost any device. We explain the concept of securely wiping data, why it is important to do so and why you should not simply delete confidential data.

MODULE: WI-FI Security **TIME:** 2:12 minutes

Often, the most common way employees connect to the Internet is through wireless connectivity, usually WI-FI. This module discusses the risks of public WI-FI and the steps that employees can take to protect themselves. In addition, we cover that only authorized WI-FI access points with prior management approval can be deployed within your organization.

MODULE: Working Remotely **TIME:** 2:45 minutes

For many organizations, employees are no longer working at the office. Instead, they work from home or on the road while traveling. Since organizations no longer have physical control of the user's work environment, there are unique risks. This module focuses on how these employees can protect themselves, including laptop security and creating a secure, mobile working environment.

Security Awareness Training Modules

MODULE: Insider Threat **TIME:** 2:33 minutes

Insider threats are trusted employees, contractors or third party members that abuse that trust to exploit an organization. This module explains what this threat is, why this threat is so dangerous and ways employees can identify and report the threat.

MODULE: Help Desk **TIME:** 3:47 minutes

The help desk is often one of the most targeted groups within an organization. These people are trained to communicate with and assist a variety of members of your organization-- often people they cannot see nor people they personally know. As such, additional steps must be taken to both educate and protect these individuals.

MODULE: IT Staff **TIME:** 4:29 minutes

Your IT staff have privileged access to your critical systems. However, just because they are technical does not mean they are secure. This module teaches them why they are a primary target and how to protect themselves and your organization. Steps include proper use of privileged accounts, limiting the information they share and how they can detect if a system is compromised.

MODULE: Physical Security **TIME:** 2:22 minutes

While physical attacks against your data are less likely to happen, when they do occur they can have a greater impact on your organization. In this module we explain how attackers will attempt to trick and fool their way into restricted areas. We also discuss how employees can protect the physical security of your facilities.

MODULE: Protecting Your Personal Computer **TIME:** 2:39 minutes

Security is not just an issue at work, but at home. In this module we cover steps people can take to protect their personal computers, including the importance of updating their operating system, applications and plugins, the use of anti-virus and firewalls and the importance of backups. By building good security behaviors at home people are more likely to follow them in your organization.

MODULE: Protecting Your Home Network **TIME:** 2:30 minutes

Security is not just an issue at work, but also at home. In this module we cover steps people can take to protect their home networks, including securing WI-FI Access Points and identifying all the devices they have connected to the Internet. If you build good security behaviors at home, people are more likely to follow them in your organization as well.

Security Awareness Training Modules

MODULE: Protecting Your Kids Online **TIME:** 4:32 minutes

One of the greatest challenges of being a parent is giving your children the freedom to explore the Internet, while at the same time protecting them from many of its unique risks. We explain how parents can give their children freedom while protecting them online. This module helps motivate employees about your overall awareness program and gets them engaged.

MODULE: Hacked **TIME:** 2:20 minutes

No matter how effective a security team and their processes are, there will be incidents. This module focuses on how employees can identify and report an incident. We cover things to look for, such as suspicious activity or virus alerts, and whom to report an incident to.

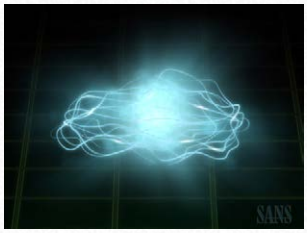
MODULE: Senior Leadership **TIME:** 4:58 minutes

Senior management is often one of the most challenging groups to train due to limited time and access. This module condenses all the key topics senior management needs to know in a single, high-impact training session.

MODULE: Advanced Persistent Threat **TIME:** 5:00 minutes

APT is not an individual acting on his own, but a highly trained team of professional cyber attackers targeting your organization. This module explains what APT is, how they operate, and how your employees can detect and protect against this dangerous cyber threat.

MODULE: Cloud **TIME:** 2:25 minutes



The Cloud is a powerful tool that enables your employees to increase their productivity while reducing organizational costs. But it also comes with tremendous risks, including how organizational data is stored and shared with others. This module explains to employees these risks and how to safely use authorized Cloud providers in your organization.

Compliance Training Modules

MODULE: PCI DSS **TIME:** 3:15 minutes

If your organization stores, transmits or processes any cardholder data it is required to follow PCI-DSS. This module teaches what cardholder data is and the required steps for protecting and safely handling cardholder data.

MODULE: FERPA **TIME:** 5:17 minutes

The Family Educational Rights and Privacy Act, also known as FERPA, is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds from the U.S. Department of Education. This module explains to all school faculty, staff, contractors and student employees the rules and regulations they must follow when handing student information.

MODULE: HIPAA **TIME:** 3:03 minutes

This module explains what PHI (Protected Healthcare Information) is and covers the steps required to store, process and use PHI. If your organization stores, transmits or processes any PHI, it is required to follow this standard.

MODULE: Personally Identifiable Information (PII) **TIME:** 2:48 minutes

This module explains what PII is and the extra steps employees must take to protect both it and other confidential information. Examples include use of encryption, use of personal email accounts, the sharing of sensitive information, using only authorized systems to store or process sensitive information, and securely disposing of sensitive data.

MODULE: Criminal Justice **TIME:** 3:22 minutes

The criminal justice and law enforcement community have several unique requirements in the use and handling of the information they collect in their daily job and activities. This module explains those requirements, including whom you can and cannot share information with and what dangers to look out for.

MODULE: Federal Tax **TIME:** 3:44 minutes

Any organization working with federal tax information is regulated by federal law and is required to take specific steps to protect that data. This module explains what federal tax information is and details the steps that employees must take to protect that data to ensure that your organization is compliant.

Compliance Training Modules

MODULE: GLBA - EDU **TIME:** 3:18 minutes

This module explains what GLBA is, what NPI (nonpublic personal information) is and the steps that individuals must take to protect it and ensure your organization remains compliant. In addition, this module explains the difference between FERPA and GLBA, and what parts of GLBA apply to schools.

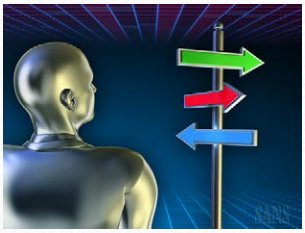
MODULE: GLBA - FIN **TIME:** 3:14 minutes

This module explains what GLBA is, what Financial NPI (nonpublic personal information) is and the steps that individuals must take to protect it to ensure your organization remains compliant.

MODULE: Red Flags Rule **TIME:** 3:23 minutes

The Red Flags Rule is a federal regulation that requires organizations to implement an Identity Theft Prevention program designed to detect the warning signs of identity theft. This module explains what these red flags are, what employees should be looking for and the actions they should take if they find them.

MODULE: Ethics **TIME:** 3:06 minutes



Ethics defines the socially accepted behaviors in your organization and culture. This module explains that employees are expected to behave in an ethical and fair manner, that cheating, stealing or lying will not be tolerated and shows how to get help if employees are confused or uncertain on the right actions to take.

MODULE: International Traffic in Arms Regulations **TIME:** 5:27 minutes

The U.S. government enforces a complex regime of export controls, trade sanctions and other requirements to prevent certain items, including data, software and technology, from going to unauthorized people, entities and countries. This module covers guidelines on when ITAR applies to your organization and its research, along with the steps employees, staff and faculty need to take to protect it.

MODULE: Data Retention **TIME:** 2:50 minutes

This modules explains what data retention is and what guidelines employees need to follow, including the use of email and authorized data destruction.

Compliance Training Modules

MODULE: Social Security Numbers **TIME:** 3:28 minutes

A Social Security Number (SSN) is a person's unique identifier that can be used by criminals for identity theft, fraud, unauthorized access to medical records and to create general havoc for a person's overall privacy. This module covers the steps every employee should take to protect SSNs.

MODULE: Foreign Corrupt Practices Act **TIME:** 3:42 minutes

The Foreign Corrupt Practices (FCPA) applies to any organization that does business in the U.S. or that has stocks, bonds or other securities traded in U.S. markets. This module explains what FCPA is, why it's important and the rules and processes that employees are expected to follow to be in compliance with FCPA.

MODULE: Federal PII **TIME:** 3:34 minutes

Any Personally Identifiable Information (PII) that comes from federal agencies is protected by federal law. It has special and very specific policies on how that data must be protected. This module explains what Federal PII is and the steps people need to take to protect that data.

MODULE: EU Data Protection **TIME:** 2:43 minutes

The European Union's Data Protection Directive is concerned with any information, either by itself or used with other pieces of information, that could identify a living person. This module explains what EU protected data is and the EU guidelines on how it should be collected, handled, protected and disposed of.

MODULE: Client Confidentiality for Law Offices **TIME:** 2:45 minutes

This module gives an overview of how client data is at risk in law firms, why lawyers need to protect it and key steps they need to take in order to protect it. This module is unique in that it uses terminology specific to the legal industry.

MODULE: Privacy **TIME:** 1:55 minutes

This module explains what privacy is, why it's important (to include respecting the privacy of others) and steps people should take to protect privacy. This module does not apply to any specific law, regulation or standard, instead, it is an overview of privacy concepts and their importance.

“This computer-based training is truly designed for the 21st century employee. It addresses both our compliance requirements and our enhanced security needs.”

– Ahmad Alkamali, Director of Security, Etisalat

Should you require further information or wish to demo the training please contact:

SANS Institute
8120 Woodmont Avenue, Suite 205
Bethesda, Maryland 20814
info@securingthehuman.org