Security Awareness Training

The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. At the heart of SANS are the many security practitioners in various global organizations, from corporations to universities, working together to help the entire information security community.

While technical training is of paramount importance, SANS also recognizes that non-technical individuals need training on awareness and compliance if information security is to be achieved across an entire organization. Therefore, SANS Securing The Human was created to provide computer based training for the end user. The product line has since expanded to serve end users, developers, ICS engineers, utilities, and the healthcare market.

Given that emails are a primary vehicle for communication for most organizations, we began to see increasing demand to phish test employees as a means to identify and respond to vulnerabilities. To address this need, SANS Securing The Human launched a new phishing product, a perfect complement to our current portfolio of security awareness products.

To read more about these products, please refer to the pages below.

Securing The Human (STH Products):

STH.End User                      Page 3
Support Materials                      Page 4
STH.Utility                      Page 5
STH.Engineer                      Page 6
STH.Developer                      Page 7
STH.Healthcare                      Page 8
STH.Phishing                      Page 9

“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, State of West Virginia
Chief Information Security Officer

For more information, please visit: www.securingthehuman.org
Program Benefits:

- Computer based training enables employees to take training on their own schedule
- 2-3 minute videos allow employees to complete the training in multiple short sessions
- Module assignments can be tailored to address specific audiences
- Language options offer consistent training across your entire organization regardless of location
- Module quiz questions and phishing emails test learner comprehension
- Track training completion for compliance reporting purposes

Updating Content

A significant issue for any organization in developing its own security awareness solution is the need to keep the training program up-to-date with the latest threats. The level of effort needed to maintain the program is significant and often underestimated.

To ensure our security awareness training always has the greatest impact, we depend on an Advisory Board of SANS’ Senior Instructors, selected clients and industry leaders to help with the development of our content.

The Advisory Board reviews our entire training curriculum, then identifies a need for any new modules, changes to existing modules required to achieve the learning objectives or the removal of outdated modules. We go through this entire review and updating process at least once a year.

Computer Based Training Products Summary

<table>
<thead>
<tr>
<th></th>
<th>STH.End User</th>
<th>STH.Utility</th>
<th>STH.Developer</th>
<th>STH.Engineer</th>
<th>STH.Healthcare</th>
</tr>
</thead>
<tbody>
<tr>
<td># Modules</td>
<td>43</td>
<td>30</td>
<td>25</td>
<td>10</td>
<td>35</td>
</tr>
<tr>
<td>Total Duration (minutes)</td>
<td>130</td>
<td>128</td>
<td>190</td>
<td>75</td>
<td>110</td>
</tr>
<tr>
<td># CBT Languages</td>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Materials</td>
<td>✓</td>
<td>✓</td>
<td>❌</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>Host on SANS VLE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Host on SANS VLE w/ SSO</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Host on Own LMS</td>
<td>Min 2000 Users</td>
<td>Min 2000 Users</td>
<td>❌</td>
<td>❌</td>
<td>✓</td>
</tr>
<tr>
<td>SCORM Compliant</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>508 Compliant</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Brand with Logo</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tracking &amp; Reporting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

For more information, please visit: www.securingthehuman.org
Securing The Human for End Users (STH.End User)

At SANS Securing The Human, our goal is to not only ensure you are compliant, but offer computer based training that changes end user behavior and reduces risk. We do this by using a proven framework based on the Critical Security Controls. This training is available in 28 languages.

Security Awareness Modules:

- You Are the Target
- Social Engineering
- Email and Messaging
- 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
- International Travel

Compliance Modules:

- 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 Personally Identifiable Information (PII)
- European Union Protective Directive
- Client Confidentiality
- Privacy Security
- Australian Compliance

For more information, please visit: [www.securingthehuman.org](http://www.securingthehuman.org)
Support Materials

Securing The Human Support Materials provide a multi-communication channel approach, ensuring your users get the greatest possible learning impact. The computer-based videos are designed to be the primary education channel, while the newsletters, posters and screensavers can be used for reinforcement.

Support Materials share the same images, format, and topics as each STH.End User video in order to reinforce your security message in a consistent manner. They are branded with your organization’s name, logo and security team’s contact information, and are provided to you in a single digital format. You can print them out or email them for use across your entire organization for as long as you wish. In addition to English, Support Materials are also available in Spanish, Arabic, and French.

---

**Newsletter**

**Poster**

**Screensaver**

For more information, please visit: www.securingthehuman.org
Securing The Human for Utilities (STH.Utility)

Utilities have employees within their organizations who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets. Given this access and the critical role they play in our society, Utilities are subject to federally mandated North American Electric Reliability Corporation (NERC) reliability standards and are forced to undergo compliance training or potentially face stiff penalties and fines. STH.Utility is a computer based security awareness training program developed to address these requirements, specifically the NERC-CIP Reliability Standard CIP-004-3 (Personnel & Training).

NERC-CIP Modules (CIP 004-3 R2):

- Introduction
- Reliability Standards Overview
- Critical Assets
- Physical Controls
- Electronic Access Controls
- Protecting CCA Information
- Incident Response

Security Awareness Modules (CIP 004-3 R1):

- You Are the Target
- Social Engineering
- Email and Messaging
- 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
- International Travel

“Security Awareness, Training and Education are still the best return-on-investment for your security program and SANS is the strategy to meet that goal/objective.”

Stan Gatewood, University System of Georgia

Chief Information Security Officer
Securing The Human for Engineers (STH.Engineer)

SANS has developed Securing the Human for Engineers, which focuses on security behaviors for individuals who interact with, operate or support Industrial Control Systems. This computer based training consists of 10 modules and provides an ICS overview, an understanding of ICS attacks and covers basic system and network defense approaches in an ICS environment, as well as governance and policy resources. These modules were developed to not only assist your organization in meeting compliance requirements through continued training and standard reporting, but also change human behavior and reduce risk.

STH.Engineer Modules:

- Overview of ICS
- ICS Drivers and Constraints
- Overview of ICS Attacks
- ICS Attack Surfaces
- ICS Server Security
- ICS Network Security
- ICS System Maintenance
- ICS Information Assurance
- ICS Incident Handling
- Attack Scenario

For more information, please visit: www.securingthehuman.org
Securing The Human for Developers (STH.Developer)

By educating everyone involved in the software development process, including developers, architects, managers, testers, business owners and partners, you reduce the chances that your organization will become a victim of today’s data security threats and ensure that your team can properly build defensible applications from the start. STH.Developer provides the pinpoint software security awareness training that your team needs when they need it most, from the comfort of their own desks.

Fundamentals Developer Awareness Modules:

Open Web Application Security Project (OWASP) Modules:

Software Development Life Cycle (SDLC) Modules:
Securing The Human for Healthcare (STH.Healthcare)

Health data breaches involving more than 500 patients have recently risen, with laptop computer thefts as the leading cause of breached data and paper-based record thefts as the next. Additionally, electronic health records are even more valuable to the underground market than your average personally identifiable information. As a result, educating workforce members is becoming more and more crucial to healthcare companies entrusted with sensitive patient data. STH.Healthcare is a computer based security awareness program tailored for healthcare organizations.

Healthcare Modules:

- Regulations and Healthcare
- The Privacy Act
- The Security Act
- You Are the Target
- Social Engineering
- Privacy
- Health Information (PHI) Overview
- Protecting Confidential Information That Is Not PHI
- Help Desk Responsibilities to Protect PHI
- IT Staff Responsibilities to Protect PHI
- Leadership Responsibilities to Protect PHI
- Cameras in Medical Offices
- Insider Threat to PHI
- Reporting Trouble
- Passwords
- Encryption
- Physical Security of PHI
- Protecting PHI in Email
- Protecting PHI Online
- Protecting PHI in Social Media
- Corporate Mobile Devices vs. Personal Devices (BYOD)
- Physically Disposing of PHI
- Protecting PHI on Wireless Networks
- Protecting PHI While Working Remotely
- Cloud Computing and PHI
- Mobile Data Security
- International Travel
- Business Associates and PHI
- Medical Device Security
- Security Officers Overview (HIPAA)
- Privacy Officers Overview (HIPAA)
- PCI-DSS
- EU Data Protection Directive

For more information, please visit: www.securingthehuman.org
Securing The Human Phishing (STH.Phishing)

SANS STH.Phishing takes an innovative approach to advanced attack prevention. We too often focus on technical controls while ignoring the weakest link: the end user. STH.Phishing simulates phishing attacks to educate your end users on how to avoid being compromised.

Reasons to Use SANS STH.Phishing:

1. Create a Custom Campaign
   - Simulate real-world attacks.
   - Choose an existing email template or create your own.
   - Choose a prebuilt training landing page or create your own.

2. Deliver Immediate Feedback
   - Launch awareness training when it is most impactful: the moment a user clicks on a link in the simulated phishing email.
   - Educate and empower users without making them feel like they have been duped.
   - Customize campaigns to forward the user to our customizable training, your own existing material or no training at all.

For more information, please visit: [www.securingthehuman.org](http://www.securingthehuman.org)
3. Rich & Interactive Reporting

- Get comprehensive detail on who clicked or forwarded the test email link.
- Assess any user’s endpoint device security or source IP address, and check whether or not they completed the training and if they reported the phish.
- Detect vulnerable endpoints and eliminate malware by pinpointing and patching users who have vulnerable browser plug-ins like Adobe, Java, Flash and Silverlight.

4. Nothing to Install (SaaS service)

- No hardware or software to manage. Your annual subscription provides unlimited phishing.