

Entertaining & Effective Security Awareness Training



securED



DIGITAL
DEFENSE[®]
INCORPORATED

www.DigitalDefense.com

Technology Isn't Enough

Improve Security with a Fun Training Program that Works!

Social engineering, system issues and employee and third-party negligence are all contributing factors to security breaches. While most organizations place a high focus on employing safeguards for their networks, technology is only one piece of the equation. Organizations must effectively educate employees to fend off attacks which target human vulnerabilities. One way to help educate and fight cybercrime is to leverage the Digital Defense, Inc. security awareness training program, SecurED®.

SecurED has blended security expertise, award-winning comedy sketch writers and a cast of Hollywood talent to bring to life security training that is innovative, fun and impactful.

- ✓ **It Works!** A Ponemon institute study revealed that SecurED outperforms the alternative training intervention by 300% in long term gains.
- ✓ **Fun and Entertaining!** Training developed in collaboration with award winning comedy writers.
- ✓ **Underpinned by Security Expertise!** Training includes courses on information security hot topics to improve security intelligence and best practices.
- ✓ **Easily Measure Success!** Each training module includes test questions to help you track the “stickiness factor” required for effective retention.
- ✓ **Meet Your Global Needs!** Training available in ADA-compliant and multi-language versions.

“Absolutely excellent!”

“This made learning security fun!”



YOUR ORGANIZATION CAN BENEFIT FROM A FUN SECURITY AWARENESS EXPERIENCE THAT MAKES AN IMPACT!

Say, “No,” to boring training and leverage a program that features fun, engaging characters and optimizes employee retention of serious security intelligence and best practices.

Employees can receive memorable information and access anytime, anywhere from virtually any device.

SecurED

Are your employees creating **secure** passwords?

What is the likelihood that your employees could fall victim to a **phishing** attack?

How **confident** are you that one of your employees wouldn't be the **root cause** of a **ransomware** attack?

One way to help educate employees is to introduce Security Spotlight animations. Security Spotlights are 90 second fun and entertaining animations that will effectively raise awareness.

SECURITY SPOTLIGHTS:

- Password Security
- Phishing Protection
- Ransomware Prevention

Security Spotlight Topics



Password Security



Phishing Protection



Ransomware Prevention

3 Ways to Use Security Spotlights to Improve Information Security

1. Build a powerful defense against cybercrime

Arm employees with the required knowledge to thwart information security intrusions. Designed to help train, educate and reinforce a security aware employee base.

2. Use all tools available to fight hackers

Kick off a new way of training and create maximum excitement and support by leveraging a fun and enjoyable security awareness training program.

3. Improve Your Teams' Security IQ

Easily deploy fun and engaging animated videos to all employees regardless of their security training level. Easy and convenient, these videos will be accessible from multiple platforms (PC, laptop, iPad/tablet or mobile device).

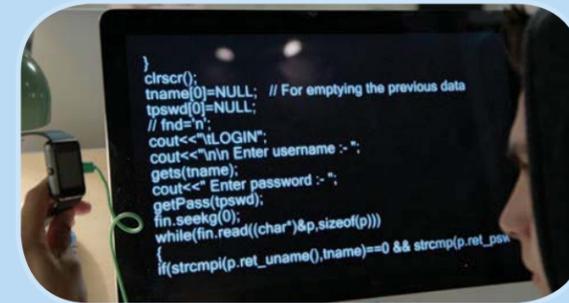


SecurED Expanded: Security Awareness

The industry recognized security awareness training program that so many know and value has become even better with the SecurED Expanded series. The new training courses take a fresh approach and deliver training content on today's most relevant information security topics. Build on SecurED Core with the latest videos for a robust library of security education courses that will bolster your defenses by creating a vigilant workforce.

Training videos are approximately 10 minutes each and deliver educational background, real world examples and best practices that employees can easily understand and quickly apply. Each course includes comedic elements, training content and test questions to help measure the success of the program and the organization's understanding of information security topics.

Training Gets Even Better



CORE COURSES AVAILABLE

✓ Acceptable Use of Computer Systems

Go beyond common sense and outline the importance of the company computer use policy in this entertaining security training video.

✓ Installing Software from Unknown Sources

New software is enticing but can also wreak havoc in the office. Learn how to properly use software and how to avoid unknown or unsolicited programs or files that could lead to a breach.

✓ Mobile Device Security

Employees utilizing personal iPhones, iPads and other devices to conduct business are no longer the exception but now the rule. However, convenience can come at a price. Train your employees on proper security on the go.

✓ Onsite Social Engineering

Train your employees not to be taken advantage of by scammers who are using human nature to get their foot in the door and their hands on sensitive information.

✓ Password Development & Security

The recent security breaches making headlines in the news and security flaws being announced underscore the need for employees to understand the importance of secure passwords.

✓ Physical Security

Does your organization have the wrong kind of 'open door policy'? Are social engineers getting access to sensitive information? From piggy backing to dumpster diving, train your employees on what to be looking for to help defend against an attack.

✓ Preventing Virus & Malware Outbreaks

The complexity of virus attacks demonstrates the need for training and ongoing education. In this training video learn about anti-virus technologies and ways to detect malware.

✓ Remote Social Engineering

One opened email; One clicked link. Simple acts that could lead to devastating consequences. Train your employees how to spot easily deployed attacks that are highly effective at gaining access to corporate data.

✓ Safe Web Browsing

Online pop-ups, deceptive links and clickable graphics can all lead to spyware and other potentially dangerous traps. Train your employees on common tactics used by cyber criminals and how to avoid scams.

✓ Securing Protected Data

Protecting sensitive information is the objective for all security measures. Learn the fundamentals of ways employees can work together to protect personal and customer data.

✓ Social Media Dangers

Friending, following, tweeting, checking in and linking up... In today's ever connected world, people all over the globe are utilizing social media. Train your employees how to socialize more safely.

✓ Using Cloud Services Safely

A security storm could be brewing. Train your employees how to be responsible for selecting a secure cloud provider.

NEW COURSES AVAILABLE

✓ Compliant & Secure: HIPAA

Over the past several years, there has been a significant rise in criminal attacks against organizations with access to patient data as a result of the underground value of protected health information (PHI) and personal identifiable information (PII). In this training video, employees will learn the security protocols surrounding the Health Insurance Portability and Accountability Act (HIPAA) and gain insight into regulations and information security best practices for complying with HIPAA to defend against a breach and to bolster the security of patient data.

✓ Compliant & Secure: PCI

Credit card fraud resulting from data breaches caused by internet attacks against merchants and banks is on the rise. In this video, employees will learn the importance of the Payment Card Industry (PCI) standards to prevent cyber theft, and how to go beyond compliance to ensure your organization is proactively adhering to standards and mitigating the risk of a data breach.

✓ Defending Against Cyber Fraud

Cyber Fraud is the use of Internet services or software to deceive and defraud victims, both individuals and organizations, with a motivation of financial gain. This training video will discuss ways to prevent cyber criminals from accessing your workplace to commit cyber fraud. From ransomware to wire fraud, employees will be educated on schemes and tactics used by cyber criminals and learn best practices for defending against these types of attacks.

✓ Defending the Security Landscape

Cyber security breaches are happening at an alarming rate. Consumers and businesses alike are faced with the challenge of ensuring they are investing in safe technologies and keeping apprised of the

various ways in which they may be compromised. In this training video, the state of security is addressed by presenting consequences of a breach, common motivations of hackers and methods of attacks utilized to gain access to sensitive data. From phishing to physical security, this training presents an introduction to the various tactics used to infiltrate organizations and helps educate employees on how to fight the ongoing battle to protect your organization's most valuable assets.

✓ Executive Cyber Defense

We believe that hacker success rates will increase and organization leadership must keep their guards up at all times to reduce the risk of a security breach that can result in a devastating outcome. Research has proven that executive level support is essential to building a culture of security. This training video, specifically designed for executive management, presents best practice recommendations on how to defend against an attack aimed at executives and their families, as well as approaches to reduce risk by creating a high level of security awareness across the organization.

✓ The Internet of Things: Secure Practices

The Internet of Things is the set of physical devices that are connected to the internet. They collect and exchange data with each other as well as with humans, all with the goal of rendering our lives more efficient and more productive. Along with technological advancements comes the potential for increased security risks. In this module, employees will be trained to better understand the environment, infrastructure and IoT security risks and privacy concerns. Through best practices and tips for improved security, employees will learn the effective ways to apply the same security protection protocols on IoT devices as they would any other network attached equipment.

ASK ABOUT CONTENT OWNERSHIP AND HOSTED OPTIONS.

**“Very
informative.”**

**“I found
myself
taking notes
not just for
work, but also
for my
personal
use.”**

**“The training
was on basic topics
but seemed to be
more in-depth than
what we have seen
in the past.”**



9000 Tesoro Drive, Suite 100
San Antonio, Texas 78217
888.273.1412
www.DigitalDefense.com