Global Learning Systems

CORE COURSES

Security Awareness Essentials Challenge 30 Minutes

Despite the best efforts of organizations worldwide, cybercrime is rising rapidly, and it is expected to cost organizations a stunning amount in 2019: $2 trillion. This is because human error continues to be the biggest threat to information security. This course aims to mitigate human error by teaching how to classify data, secure mobile devices, secure remote and home offices, avoid social engineering scams like pretexting and phishing, and create strong passwords. The course engages users by describing real-life security challenges and asking them to choose the best course of action for each challenge.

BEST PRACTICE MODULES

InfoSec Best Practices Module: Setting Up Secure Passwords 7 Minutes

Setting strong passwords is extremely important, for passwords are the gateway to computer systems and sensitive data. This course teaches how to distinguish between strong and weak passwords, create a strong and memorable password using a passphrase, and secure your accounts using strategies such as multiple passwords and changing passwords often.

InfoSec Best Practices Module: Avoiding Phishing Message Threats 10 Minutes

According to a Verizon report, 30 percent of phishing emails are actually opened, and 12 percent of those targeted click on the infecting link or attachment. This course teaches what

phishing is, how to recognize a phishing email or text message by looking for specific characteristics, what to do if you receive a phishing email or text message, and how to secure devices against potential phishing attempts.

SHORT SECURITY VIDEOS

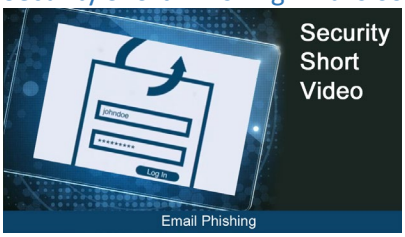
Security Short: The Human Firewall™ 6399

When it comes to information security, an organization is only as secure as its weakest link. This short video explains this using the concept of Human Firewall™ — that information security depends on the security practices of everyone. It also describes the security measures each employee should take to strengthen the organization's Human Firewall™.

Security Short: Individual Responsibility 6398

A security-minded culture within the organization is critical for information security. This short video helps communicate just that. It points out the common mistakes that employees make when handling data, and more importantly, it lists the simple actions that employees can take in their day-to-day routine to secure information at the workplace.

Security Short: Phishing Emails 6091



Organizations are regularly targeted by phishing attacks, and many employees are not aware of how to spot or properly dispose of malicious emails.
In this short video, users will learn what phishing is, how to recognize phishing emails, and what to do if they receive a phishing email.

Global Learning Systems

SHOCK & AWARENESS VIDEOS

Shock & Awareness Video: Passwords 7971

The average individual today needs to remember passwords for dozens, if not hundreds, of personal and work-related online services — and this leads to taking shortcuts when creating passwords. But a nudge in the right direction can help change employee habits related to passwords.

This video uses statistics and facts to communicate the dangers of weak passwords. It communicates the importance of using strong passwords and the best practices for protecting passwords.

Shock & Awareness Video: Phishing 8061

An unfortunate side effect of the Internet is that sensitive data is more vulnerable than ever, and every time a breach occurs, you can pretty much guess the culprit: a phishing email. Today, phishing is the biggest challenge for every organization's Information Security department.

This video describes real-life phishing attacks, presents the facts behind phishing, and drives home the dangers of interacting with unsolicited email without taking security precautions.

Shock & Awareness Video: Responsibility 8062

Global Learning Systems

Even the best laid information security plans fail when employees do not follow security policies. It's crucial to not only train employees to properly protect themselves against attack, but also to reinforce that individual responsibility plays an important role in an organization's overall security.

This video, using examples and statistics, explains the importance of individual responsibility in protecting corporate and personal data from cybercrime. Short and engaging, it works to help promote user awareness and involvement with organizational security efforts.

ANTI-PHISHING ESSENTIALS 3398

With phishing becoming the weapon of choice for cybercriminals, it's important to be vigilant and prevent attacks. This course teaches how to avoid becoming a victim of phishing attacks by explaining how phishing attacks work and how to recognize a phishing email.

Infosec Best Practice Module: Avoid Phishing Message Threats 4295

According to a Verizon report, 30 percent of phishing emails are actually opened, and 12 percent of those targeted click on the infecting link or attachment. This course teaches what phishing is, how to recognize a phishing email or text message by looking for specific characteristics, what to do if you receive a phishing email or text message, and how to secure devices against potential phishing attempts.

Global Learning Systems

Infosec Best Practice Module: Avoid Spear Phishing Threats 5869

In recent years, cyber criminals have upped their game by moving from generic largescale phishing attacks to spear phishing attacks — an attack where cyber criminals target specific high-value targets after conducting extensive research on them. This course helps doing just that. It puts the user into the shoes of two regular employees and helps them avoid spear phishing.

Infosec Best Practice Module: Safe Social Networking 3962

Social networks are a great tool for promoting business, but they make it just as easy to share sensitive or damaging information. This course teaches how to use social networks safely. Specifically, it teaches how to avoid the most common risky behaviors on social networks and which privacy settings to use on social networks.

Security Short: Phishing Emails 6091

Organizations are regularly targeted by phishing attacks, and many employees are not aware of how to spot or properly dispose of malicious emails. In this short video, users will learn what phishing is, how to recognize phishing emails, and what to do if they receive a phishing email.

Global Learning Systems

Security Short: Ransomware 6390

A common tool that cybercriminals use is ransomware, which is malicious software that infects the victim's computer, encrypts files, and demands a ransom be paid for decrypting the files. In this short ransomware prevention video, employees will learn the basics of ransomware and how to defend against it. What is it? How does it infect computers? What can you do to avoid being a victim and protecting your organization? This video answers all these questions, and helps ensure that every member of the organization is aware and equipped to deal with a potentially deadly attack.

Security Short: Smishing 6378

Phishing is not limited to emails; text message phishing — or SMiShing — is also a popular tool of choice for cyber criminals. Similar to a phishing email, a scammer will embed a bad link in a text message, taking whoever clicks to a malicious website. This short video explains to users how SMiShing works, what SMiShing text messages look like, and what they can do to avoid becoming victims.

Security Short: Voice Phishing 6391

Phishing is typically associated with malicious emails, but it's critical to know that voice phishing — also known as "vishing" — is also a strategy that cybercriminals use.

This short video aims to educate users about voice phishing. It explains what voice phishing is, how to recognize an attack, and what best practices to follow for unsolicited phone calls.

Security Short: Social Media Posts 6984

With social media, too much information can be shared inadvertently, especially when individuals confuse confidential information with public information, or mistakenly think that what they're post will be kept "private" by security settings.This short video explains the common pitfalls of using social media as a communication tool, as well as business use of social media. It explains what information should not be shared and what should be done to use social media securely.

Security Short: Social Engineering in Social Networks 6983

Because social networks are so popular, criminals often use them to learn about a user, and use that information to target him/her with a more specific and convincing scam. This short video on social media for employees educates users on the common tactics that cybercriminals use in social networks and what they can do to avoid becoming victims.

Shock & Awareness Video: Phishing Video 8061

An unfortunate side effect of the Internet is that sensitive data is more vulnerable than ever, and every time a breach occurs, you can pretty much guess the culprit: a phishing email. Today, phishing is the biggest challenge for every organization's Information Security department. This video describes real-life phishing attacks, presents the facts behind phishing, and drives home the dangers of interacting with unsolicited email without taking security precautions.

Global Learning Systems

Shock & Awareness Video: Safe Social Networking 8208

Billions of people currently use social media platforms. However, many underestimate or don't fully understand the ways in which those platforms can be used against them. This video lists important statistics and facts about the dangers of social media. It aims to alert social media users to the risks of social media, and it provides the best practices to follow when using social networks.