EPRI

GRIDED

The Center for Grid Engineering Education

Cybersecurity 101 – Practical Survival Tips for Navigating the Cyber Threat Landscape

Course Description

Critical infrastructure, governments, public institutions and utility providers are under constant attack. New and emerging cyber threats have increased exponentially during the last decade and exploded during the COVID-19 pandemic as more industries became reliant on internet-based applications and remote workers. Currently, anyone who uses technology is at risk due to online fraudsters and hackers, targeting them at work, home, and on the road.

Employees who understand cyber threats and can help safeguard their organizations from these risks, making themselves more valuable and in great demand.

This course is designed to introduce anyone who uses technology to the basic concepts of Cybersecurity. The goals of the course are to:

1. Increase participants' overall security awareness and ability to identify cyber-threats.
2. Provide practical tips and tricks to reduce cyber-threat exposure and to reduce the risk of attacks both in the workplace and at home.
3. Encourage participants to step into the role of a cyber-champion to promote cybersecurity best practices to others.

Key topics include:

- Outsmarting social engineering attacks
- Malicious software identification and defense
- Cyber self-defense strategies for email, computers, and mobile devices
- Digital forensics preparedness and incident response planning
- Privacy awareness and open source intelligence gathering
- Defenses while working remotely
- Security controls and operational technology defenses
- Incident response planning and management
- Industrial internet of things - attacks and defenses

Who Should Attend

This practical, hands-on, fun and informative course is ideal for any utility employee who uses basic technology such as email, phones, computers and tablets. This course is intended for utility employees encompassing a variety of positions, including field technicians, operation engineers, upper level administration, and clerical support staff.

(This course is introductory level, and is not recommended for those already highly specialized in cybersecurity, information assurance or information security.)

PDH Available: Participants who attend the full course will receive a Certificate of Attendance for 12 Professional Development Hours. Participants who attend the full course and pass an optional exam will be provided a Certificate of Completion.

Registration:

- $1,200 per person
- 20% discount for organizations with three or more attendees
- 25% discount for government employees (non-utility)
- 25% discount for university professors*
- 75% discount for graduate students*

*University IDs required to qualify for professor or graduate student discounts.

Location: Online - Live sessions will be recorded and available following the live web conference for four weeks.

EPRI Contacts

William Webb, wwebb@epri.com

Amy Feser, afeser@epri.com

Participants will need access to an internet connection from a standard desktop/laptop computer equipped with speakers, microphone and common web browser, i.e. Internet Explorer, FireFox, Google Chrome, etc. Students will join live, synchronous web conference sessions via WebEx, with two-way voice capability through a telephone bridge.

Meet the Instructors

Daryl Pfeif is the Founding Partner of Digital Forensics Solutions (GotDFS.com) and CEO of Digital Security Associates (GotDSA.com). Since 2004, she has been actively engaged in digital forensics and cyber security, supervising forensic and data breach investigations, security audits and analysis, training, research, and software development.

DFS has made significant contributions to the field of digital forensics and cybersecurity, advancing the state of the art in Live Memory Analysis, File Carving, Forensic Analysis of Embedded File Systems, and Windows Registry Analysis. Federal projects include training, research and development for the National Science Foundation, The National Institute for Standards in Technology, DARPA, NASA, and the National Institute of Justice.

Daryl is also a founding Board Member and the COO of DFRWS.org, a volunteer-driven non-profit organization that coordinates international knowledge sharing and collaborative activities for leaders in education, government, and industry to address emerging challenges and to advance the science in DFIR research and practice. Daryl's most recent endeavor is the Cyber Sleuth Science Lab, (CyberSleuthLab.org), an initiative of Go Learn Labs, founded in 2016 to introduce DFIR in High School to encourage the next generation to pursue careers in DFIR and related fields. Daryl is a member of HTCIA (High Technology Crime Investigators Association) ISACA and the WiCys (Women in Cyber Security).

Christopher Loomis brings over 20 years of experience in information security - with an emphasis on secure programming, web application testing, project management, policy creation, vulnerability assessment, digital forensics, and incident response. Christopher is familiar with the assessment and implementation of methodologies in accordance with regulatory and internal audit guidelines and is well versed in all major operating systems and a suite of modern security testing platforms and tools.

Christopher wrote the award-winning CAL9000 application security testing tool for OWASP. He has served as a GSEC and GCIH Advisory Board Member for the SANS Institute where he worked with other security professionals to support and guide the GIAC program, also updating and authoring SANS course materials. He has created and implemented a secure software development program for a Fortune 250 company, as well as written and taught security best-practices classes. He is currently exploring hardware security, so don't plug anything into your computer that he may give you.

Course Outline

Session 1 - Social Engineering

- Course Intro and Scale of Problem
- Social Engineering Attack Case Studies
- Malware (Smishing, Vishing and Phishing)
- How to Prevent and Defend Against These Attacks

Session 2 - Cyber Self-Defense Strategies

- Identifying Cyber-Threats
- Email Account Compromise
- Practical Computer Safety
- Password Management and Privacy Awareness

Session 3 – Safety Tips for Working Remotely

- Defenses for Working Remotely
- Backups and Encryption
- Safety Tips for Home Routers, Public Wi-Fi and Mobile Phones

Session 4 - Industrial & Cyber-Physical Security

- Cyber-Physical / Physical Case Studies
- Securing IIoT - Industrial Internet of Things
- Common Threats to OT / ICS / SCADA systems

Session 5 - Digital Detectives (DFIR & OSINT)

- Defining your Digital Footprint
- Digital Forensics Preparedness
- Incident Recovery - Response Planning and Management
- OSINT – Open Source Intelligence

Session 6 - Practice and Review

- Password Cracking and Password Strength Testing
- Personal Incident Response Plans
- Course Review

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com