

Information Technology ▼

General Insurance IT

Life & Retirement IT

Investments IT

Corporate Systems

Infrastructure Services

Information Security Office

Global IT Process and Metrics

## AIG Cybersecurity Awareness Campaign

Welcome to the AIG cybersecurity awareness website – your “one-stop-shop” for cybersecurity information.

As you become familiar with the resources below, you’ll learn how you are empowered to protect yourself, your family, and AIG from cyber risk.

Cybersecurity Training - “Deep Dives”	Cybersecurity Basics	Staying Safe at Home and Beyond
<a href="#">Email Security</a>	<a href="#">Supercharge Your Passwords</a>	<a href="#">How Hackable Is Your Life?</a>
<a href="#">Email Security on Mobile Devices</a>	<a href="#">Two Factor Authentication</a>	<a href="#">Holiday Shopping: Staying Safe Online</a>
<a href="#">Safe Social Networks</a>	<a href="#">Travel Cyber Safe</a>	<a href="#">Privacy Tips for Teens</a>
<a href="#">Social Engineering</a>	<a href="#">Vishing Awareness</a>	<a href="#">Securing Your Kids from Cyber Risk</a>
<a href="#">Travel Security</a>	<a href="#">Phishing, Vishing, and Smishing</a>	<a href="#">Hinder the Hackers on Social Media</a>
<a href="#">+LinkedIn Learning - Cybersecurity Courses</a>	<a href="#">How to Build the Best IT Security Defense</a>	Visit <a href="#">staysafeonline</a> for additional resources



**AIG’s cyberdefense begins with me and my pledge to:**

- Understand how to report a security incident.
- Recognize what makes an email suspicious.
- Report suspicious emails via the Report Phish button on Outlook or send them as an attachment to [phishing@aig.com](mailto:phishing@aig.com).
- Hold off on sharing information until I verify the identity of the requester.
- Not use my AIG password for any other accounts outside of AIG.
- Lock my workstation every time I step away.
- Encrypt sensitive emails to external recipients using AIGENCRYPT.
- Enable Multifactor Authentication to protect online accounts.
- Become familiar with AIG’s Acceptable Use of Technology Standard.

**Defense starts here.**  
Learn more at [contact.aig.net/cybersecurity](https://contact.aig.net/cybersecurity)





### Learn The Basics

Let’s start with [How to Report IT Security Incidents](#). And what are our expectations for acceptable use of technology at AIG?

Next, [learn how to protect yourself from phishing emails](#), which remain attackers’ favorite method for extracting money or information. (Translations: [Simplified Chinese](#), [Traditional Chinese](#), [Japanese](#), [Spanish](#), [French](#), [Portuguese](#)). AIG has a [phishing awareness program](#), which includes sending phishing simulation emails to colleagues.

Keep the momentum going with a [basic cyber safety tip sheet](#) (translated versions are [here](#)), and top it off with an understanding of how you can help AIG [build the best IT security defense](#).

[Read the Top Ten Tips to Stay](#)

- My Technology
- Technology Corner
- Computers and Software
- Email
- Help
- Cyber Security Awareness

- CSAMDates Wk1
- RRAnnouncements
- RiskRemediationInfoList
- CyberSecurityNews
- AssetLibrary
- HowHackableIsYourLife
- ReportingITSecIncidents

- Mobile Devices & Service
- Multimedia & Webcasts
- Network Connectivity
- Print
- Voice Services
- FileTaxesSafely2018
- New PCI DSS Procedures
- CyberSecurity Awareness - Stay
- Cyber Safe at Work and Home
- Reducing Cyber Risk at AIG

# REPORTING IT SECURITY INCIDENTS

Please immediately report anything unusual on your computer or device, or report if your device is lost or stolen. Prompt notification allows IT Security and the Cyber Defense team to contain incidents.

## SOMETHING UNEXPECTED

- Your mouse moves by itself and makes selections.
- People receive emails from your email account even though you did not send them.
- A window or program opens by itself repeatedly.
- You click on a link in an email and your computer freezes.
- Lost AIG laptop or device
- Unwanted browser toolbars
- Redirected Internet searches
- Frequent random popups
- Unexpected password changes or software installs.

Contact the AIG Global Service Desk at  
+1-800-435-7457 (US and Canada) or  
+1-682-831-8402 (International).

Always safeguard potential evidence and document incident details.

### 1. Safeguard potential evidence:

- Discontinue use of the computer or device
- Disconnect from AIG network when possible
- Do not shut down the computer or device
- Do not delete anything or close any application

## PRIVACY RISK INCIDENT

If you believe that AIG Company Information may be at risk, report this as a Privacy Risk Incident to your AIG Privacy Team immediately. Contact details are available [here](#).

For example, if your device is lost and may not be encrypted, or the password has been compromised, this could expose AIG Company Information to risk of unauthorized access. This may have legal compliance consequences for AIG and these should be handled immediately by your Privacy Team.

Do not discuss the incident with anybody other than your manager and others managing the incident.

### 2. Document incident details by including:

- What happened
- When it happened
- What you were doing when it happened

## PHISHING AND VISHING

If you receive a "phishing" email, please use the PhishAlarm button on Outlook or send the email as an attachment to [Phishing@aig.com](mailto:Phishing@aig.com).

Avoid opening suspicious attachments or links in the suspicious email.

If you visited websites or opened attachments contained within the phishing email, **please contact the AIG Global Service Desk at +1-800-435-7457 (US and Canada) or +1-682-831-8402 (International).**

Contact the Global Service Desk if you have received a suspicious phone call (i.e. "vishing").

- My Technology
- Technology Corner
- Computers and Software
- Email
- Help
- Cyber Security Awareness
- Mobile Devices & Service
- Multimedia & Webcasts
- Network Connectivity

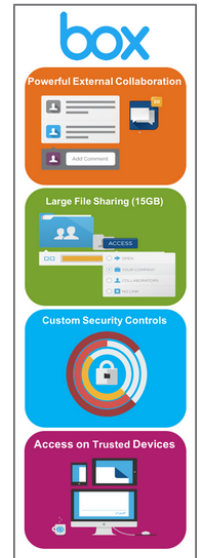
Wireless Connections  
Remote Access/VPN Pulse  
Remote Access/RSA Token

- Office 365 Info Center
- Print
- Voice Services
- Teleworker
- Wireless Connections
- Wireless Connections

## Network Connectivity

In AIG offices, users have two options for connecting AIG-managed devices securely to the AIG network – via the AIG wired (cable) network or via AIG wireless (MobileNet). Whenever you are at your desk or work area, wired access should be used. Outside AIG offices, users will need to connect via Pulse Secure remote access/VPN to connect securely to AIG network. Devices that are not AIG-managed have two options for connecting to our wireless network (GuestNet and EmployeeNet).

Learn more about setting up and using remote access/VPN or wireless access by clicking on the icons below.



**Technology Support**

**WE CAN HELP**

Have a technology issue or request? Here are a few ways to get help:

## Wireless Connections



AIG EMPLOYEES  
WITH A  
COMPANY DEVICE...

**MOBILENET**

...IS FOR YOU!

- Direct access to AIG applications
- Authentication with LANID / Password credentials
- Access to Citrix / VDI
- AIG inappropriate site restrictions
- **Currently available in APAC, EMEA and NA. Coming to Japan in Q1 2019!**

AIG **MobileNet** is the standard wireless network available at all AIG office locations globally. It is available to all AIG employees and contractors on **AIG issued and approved devices**. **MobileNet** enables AIG employees and contractors to access the AIG network and all applications/services just like they would on a wired network. **MobileNet** offers convenience, increased mobility, ease of use, and security.

You can use **MobileNet** only on corporate issued laptops, mobile phone and/or tablets- wireless access does not apply to desktops.

[Simple steps to access MobileNet](#)



AIG EMPLOYEES  
WITH A  
PERSONAL DEVICE...

**EMPLOYEEENET**

...IS FOR YOU!

- Authentication with LANID / Password credentials with a ServiceNow Request
- Bring your own mobile device (BYOD) approved
- Access to Internet e-mail, Facebook, etc.
- Access to Citrix / VDI via Internet Portal
- AIG inappropriate site restrictions
- **Currently available in the US. Coming to other regions in Q1 2019!**

**EmployeeNet** is the wireless network for AIG employees wanting to connect their **personal** wireless devices also known as **BYOD** (Bring Your Own Device) to the AIG network.

Employees can access **EmployeeNet** by selecting "EMPnet" from their wireless device after provisioning through ServiceNow.

You can use **EmployeeNet** on your personal laptops, mobile phones, or tablets. AIG policies for internet use applies.

[Simple steps to access EmployeeNet](#)



AIG GUESTS  
WITH  
ANY DEVICE...

**GUESTNET**

...IS FOR YOU!

- Bring your own mobile device (BYOD) approved
- Access to internet e-mail, Facebook, etc.
- Guest registration (up to 30 days)
- Access to Citrix / VDI
- AIG inappropriate site restrictions
- **Currently available in APAC, EMEA and NA. Coming to Japan in Q1 2019!**

**GuestNet** is the wireless access offered at all AIG office locations for the convenience of visiting AIG guests for up to 30 days on registration.

Visitors (Guests) can access **GuestNet** by selecting "GUESTNET" from their wireless device and requesting access from the host/sponsor. The AIG Employee (host/sponsor) has authority to approve guest access to the **GuestNet**. Once access is approved the guest can access the internet seamlessly.

AIG policies for internet use applies.

- My Technology
- Technology Corner
- Computers and Software
- Email
- Help
- Cyber Security Awareness
- Mobile Devices & Service
- Multimedia & Webcasts
- Network Connectivity
- Wireless Connections
- Remote Access/VPN Pulse
- Remote Access/RSA Token
- Office 365 Info Center
- Print
- Voice Services
- Teleworker
- Wireless Connections
- Wireless Connections

## Remote Access / VPN Pulse Secure (Off Network Access)

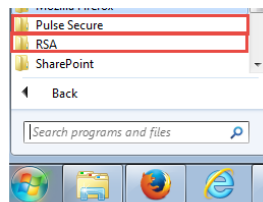
Pulse is the new AIG standard to access all of your AIG resources. Pulse has replaced Juniper/Neoteris for out of the office and flexible work arrangements (FWA). To use remote access on your AIG laptop, you will need a RSA Token & Pulse Secure already installed on your AIG laptop.

### RSA SecurID Software Token Setup

The RSA SecurID Software Token is an authentication method to securely allow access to the network. The token generates a new 6-digit random code every 60 seconds.

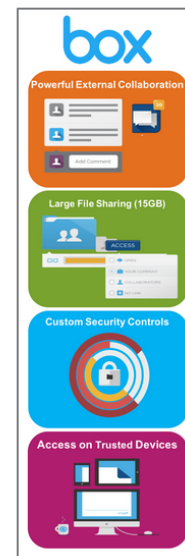
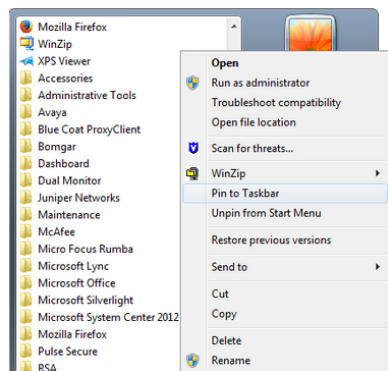
To start, check to see if you have Pulse Secure and RSA Token software installed before leaving the office.

While logged into your laptop, go to **Start** and then **All Programs**. If you have a **Pulse Secure** folder and an **RSA** folder listed, then you are ready to log into remote access. If you do not, contact your local support, Technology Bar Specialist or the AIG Global Service Desk to request access if necessary and install the needed software.



### Launching RSA SecurID Software Token

Open the RSA token by going to: **Start > All Programs > RSA > RSA SecurID Token > RSA SecurID Token** (*Pin to the Task Bar by Right-clicking RSA SecurID Token, then click Pin to Taskbar*). You could also open the icon on your Desktop.



### Technology Support



Have a technology issue or request? Here are a few ways to get help:

Call the AIG Global Service Desk at 1-800-451-6100

- My Technology ▾
- Technology Corner ▾
- Computers and Software ▾
- Email ▾
- Help ▾
- Cyber Security Awareness ▾
- Mobile Devices & Service ▾
- Multimedia & Webcasts ▾
- Network Connectivity ▾

Wireless Connections

Remote Access/VPN Pulse

Remote Access/RSA Token

- Office 365 Info Center ▾
- Print ▾
- Voice Services ▾
- Teleworker ▾
- Wireless Connections ▾
- Wireless Connections ▾

## Remote Access / RSA Token Code

### How to Use / Install the RSA Token

If you need your RSA token on another device forward the email with the attachment to the new device. Save the RSA token to your personal drive for later use. RSA tokens not used for 90 days will be deactivated.

#### Install on a Computer

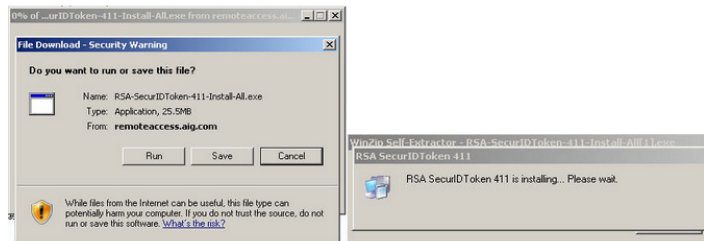
Windows (Personal):

<ftp://ftp.rsasecurity.com/pub/agents/RSA SecurIDToken411.zip>

Windows (AIG laptop):

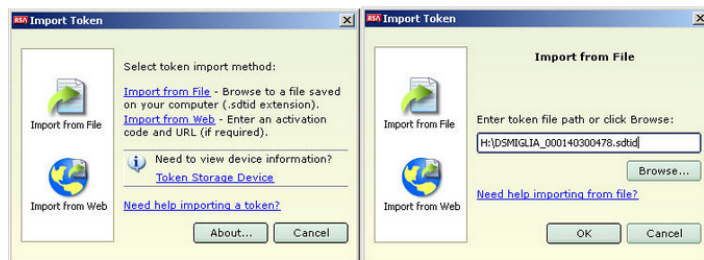
<https://remoteaccess.aig.com/RSA-SecurIDToken-411-Install-All.exe>

1. Select "RSA SecurIDToken411.msi"
2. Click save and utilize the 'Run As' feature for the .EXE file.

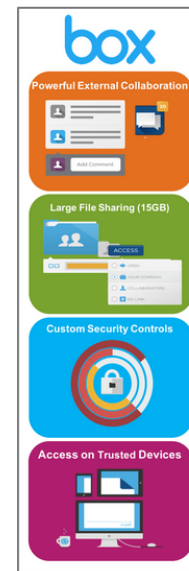


Once the installation finishes, please proceed to importing the token onto the pc.

3. Choose 'Import from File' OR Drag the File from your Email to the desktop and open it.
  - a) Browse to the location of the .sdtid file, select it, and click



4. You should receive a message stating 'Token named xxxxxxxx successfully imported'.







OWN IT. SECURE IT. PROTECT IT.

## October is National Cybersecurity Awareness Month!



LEARN HOW TO STAY SAFE ONLINE



KEEP MY BUSINESS SECURE



GET INVOLVED



LEARN MORE ABOUT NCSA

# Building the Best IT Security Defense

AIG's cybersecurity is in our hands. Along with key support from our experienced IT Security team, all of us must protect our company from technology risk. In addition to visiting our [cybersecurity awareness site](https://contact.aig.net/cybersecurity) (contact.aig.net/cybersecurity), read on for some ways you can help us to protect the company.



## Why Should We Care?








- The average cost of a data breach globally is \$3.86 million, a 6.4 percent increase from 2017.<sup>1</sup>
- Email is the most common attack vector for the delivery of malware.<sup>2</sup>
- In a survey, two-thirds of chief information security officers in the financial sector said there has been an increase in cyberattacks against their organizations in the last year, and 80 percent said the attackers are more sophisticated in how they are targeting and launching attacks on organizations.<sup>3</sup>
- The number of malware infections on mobile devices has increased by one-third since 2017.<sup>4</sup>
- One in ten URLs are malicious.<sup>4</sup>

## Guidance for General Users

Phishing	Approved Messaging Programs	Passwords
<ul style="list-style-type: none"> <li>• Report suspected phishing emails using the PhishAlarm button on Outlook or by sending them as an attachment to <a href="mailto:phishing@aig.com">phishing@aig.com</a></li> </ul>	<ul style="list-style-type: none"> <li>• Lync/Skype</li> <li>• Yammer</li> <li>• iMessage</li> </ul> <p><i>Note that messaging programs may not be used to transfer and/or transmit non-public information.</i></p>	<ul style="list-style-type: none"> <li>• When possible, create passphrases. Passphrases combine letters, numbers and symbols into an easy-to-remember phrase. For example: <i>MyHouses37*Green.</i></li> <li>• Never share your passwords with others.</li> <li>• Turn on Multi-Factor Authentication (2FA)</li> </ul>
AIG Email	Personal Email	Social Media
<ul style="list-style-type: none"> <li>• Should be used for company business; limit personal use.</li> <li>• AIG Company Information must not be forwarded to personal, non-AIG, email accounts.</li> <li>• When sending <a href="#">Sensitive Personal Information</a> outside AIG, you must add "AIGENCRYPT" to the email subject line.</li> </ul>	<ul style="list-style-type: none"> <li>• Never access personal email from the AIG network or an AIG computing device.</li> <li>• Never use personal email for business communication.</li> </ul>	<p>Be careful on social media when...</p> <ul style="list-style-type: none"> <li>• The offer is too good to be true.</li> <li>• There are misspelled words.</li> <li>• You are told that you "must" do something.</li> <li>• Someone you know is sending an unlikely invitation</li> </ul> <p><i>Remember that hackers can pose as people you know. If you are uncertain whether an invitation is legitimate, try contacting the invitee via phone or email.</i></p>
File Sharing	Network/WiFi	Managers
<ul style="list-style-type: none"> <li>• Use <a href="#">BOX</a> to share data externally. (You'll need to adhere to the terms of use.)</li> <li>• To share data internally, use SharePoint or <a href="#">OneDrive</a>.</li> </ul>	<ul style="list-style-type: none"> <li>• Only corporate-owned or BYOD-approved devices should be connected to the AIG network.</li> <li>• If you use public WiFi, immediately connect to VPN (Virtual Private Network) for protection of <a href="#">AIG Company Information</a>.</li> </ul>	<ul style="list-style-type: none"> <li>• Know who on your team has access to what applications and why.</li> <li>• Be sure to remove/review permissions appropriately (see <a href="#">IAM</a> site on Contact).</li> <li>• Make sure access is removed for workers who leave AIG or change department.</li> </ul>



# Guidance for Advanced and/or IT Technical Users

Updating Devices	Vishing/Social Engineering	
<ul style="list-style-type: none"><li>• Ensure you update all mobile devices when updates are announced and approved by AIG IT. You can check for the latest AIG-approved iOS and Android versions <a href="#">here</a>.</li><li>• Be vigilant with software updates on both your company and personal devices. Updating devices when prompted by AIG IT is one of the best ways to protect yourself from the latest threats.</li></ul> 	<ul style="list-style-type: none"><li>• Be aware of a person who calls and claims that you may have a virus or missing patches. If you are suspicious, take their number, hang up, and call the <a href="#">Global Service Desk</a>. They will investigate as necessary.</li><li>• At work, be careful with callers who are looking for non-public AIG information, especially Personal Information about our customers and employees. If you are suspicious of the caller, ask for a number listed in the AIG directory and tell them you will call them back. Once you are off the call, contact the AIG Global Service Desk if the phone number they provided is not listed.</li><li>• Never let anyone remote into your workstation/laptop unless you are certain they are a validated AIG IT resource (e.g., AIG Global Service Desk).</li><li>• Be careful when answering calls from numbers that you do not recognize.</li><li>• Be mindful that cyber scammers also send texts that link to malicious locations. This is called “smishing.”</li></ul> 	
Cloud/IoT	Phone and Conferencing	Secure Coding
<ul style="list-style-type: none"><li>• Don’t buy cloud services outside of approved channels (e.g. with your credit card.) Visit <a href="#">Service Now</a> for more information.</li><li>• Internet of Things (IoT) devices/any devices on our network must be approved; a vendor sending you a device does not qualify as approval. Hardware and software must be approved by opening a ticket via <a href="#">ServiceNow</a>.</li><li>• Change default credentials upon deployment of approved IoT devices.</li><li>• Ensure SaaS applications are incorporated into an approved CASB (Cloud Access Security Broker). This will better manage identities and access for your users.</li></ul> 	<ul style="list-style-type: none"><li>• Do not order your own Collaboration service such as Cisco WebEx. Do visit <a href="#">Order a WebEx Account and/or Status of WebEx Account order</a>.</li><li>• Do not order telephone carrier voice services outside of approved channels. Do request new services within project or service requests to ensure that calls are being delivered and can be monitored for security centrally. Visit <a href="#">Service Now</a> and link to the “Service Catalog.”</li></ul> 	<ul style="list-style-type: none"><li>• Confidential production data may not be used in—or accessed by—development or other non-production environments unless that data has been sanitized to remove, mask or hash the confidential information.</li><li>• Developers and the development community must utilize only the authorized AIG repositories to protect AIG code: <a href="https://github.aig.net/">https://github.aig.net/</a> or the AWS Code Pipeline. For guidance on utilizing the AIG Enterprise GitHub environment, please visit the <a href="#">Enterprise Devops Knowledge Base</a>.</li></ul> 
Servers	Local Admin Use	
<ul style="list-style-type: none"><li>• Do not deploy your own servers to the AIG network. Use the AIG Information Services organization to deploy any necessary servers in a secure fashion.</li><li>• Ensure that all information within the Configuration Management Database (CMDB) is populated and accurate.</li></ul> 	<ul style="list-style-type: none"><li>• If you have local administrator access on your computer, contact the Global Service Desk to have it removed.</li></ul> 	

## References

- 1 (Ponemon Cost of a Data Breach Study 2018)
- 2 (Cisco 2019 Threat Report)
- 3 (Carbon Black/Optiv Security Modern Bank Heists: The Bank Robbery Shifts to Cyberspace)
- 4 (Symantec ISTR 2019)

# Cybersecurity Courses on LinkedIn Learning

You might have heard that [LinkedIn Learning](#) is now available to AIG employees in select countries.\* However, you may not know that the platform offers a wealth of cybersecurity learning. Whether you're looking for basic knowledge or more advanced courses on cloud security and ethical hacking, LinkedIn learning will expand your skill set and sharpen your IT and cybersecurity acumen.

Please see below suggested courses. If you've taken one of the courses, we'd be interested to hear your feedback. Send all comments and inquiries to [isoinfo@aig.com](mailto:isoinfo@aig.com).

*\*Note: LinkedIn Learning is currently available in select countries pending additional legal review.*

## Courses to improve overall knowledge of *cybersecurity concepts*:

### [CISSP Cert Prep: 1 Security and Risk Management](#)

2.5 hours

Learn about information security and risk management practices needed to complete the first domain of the 2018 *Certified Information Systems Security Professional* (CISSP) exam. CISSP is the industry's gold standard certification, necessary for many mid- and senior-level positions. This course includes coverage of key exam topics from the Security and Risk Management domain: security governance, compliance and policy issues, personnel security, threat modeling, and vendor management. Author Mike Chapple also covers the trifecta of information confidentiality, integrity, and availability. He reviews business continuity and risk management strategies, and highlights the importance of ongoing security awareness and education in any organization.

### [CISSP Cert Prep: 2 Asset Security](#)

1 hour

CISSP is the industry's gold standard certification, necessary for many mid- and senior-level information security positions. Learn about best practices needed to complete the second domain of the 2018 Certified Information Systems Security Professional (CISSP) exam: Asset Security. Instructor Mike Chapple explains the importance of data governance policies and roles, and how you can develop security baselines that leverage industry standards. Learn how to avoid liability by limiting data collection, and control your exposure with file encryption, system-level file permissions, and cloud storage security options. Plus, find out how to properly retain and dispose of sensitive information.

### [Cybersecurity for IT Professionals](#)

2.5 hours

Protect your network from cyberattacks. In this course, Malcolm Shore shows how to use the latest tools to discourage and combat hackers, phishers, and snoopers attempting to infiltrate your Windows and Linux systems. Learn what forms cyberattacks can take, as well as the two most common types of protection you can build into your system: antivirus protection and firewalls. Then, learn how to scan your network for suspicious files, detect intruders with Netcat, and identify vulnerabilities at the host level with Nessus scans. Malcolm also shows how to combat application-level threats and monitor packet-level activity on your network.

### [Cybersecurity Foundations](#)

2.5 hours

Set a rock solid foundation for your network, users, and data by learning about the basics of cybersecurity. Security expert Malcolm Shore shows how to assess and mitigate risks using various cybersecurity frameworks and control standards, such as NIST, COBIT 5, ISO 27000, and the Payment Card Industry Data Security Standard (PCI DSS). He'll also show how to detect hidden and cloaked files, evaluate and avoid threats such as malware, architect security to align with business needs using SABSA, manage user access, and prepare for and respond to cybersecurity incidents when they do occur.

By the end of this course, you'll have a greater understanding of the threats that affect private, corporate, and government networks, and the knowledge to prevent attacks and defeat them.

### [Cybersecurity with Cloud Computing](#)

2.5 hours

How do you keep your organization's files, applications, and accounts safe on the cloud? It starts with a considered design approach. In these videos, Malcolm Shore outlines the major cloud security risks, some of which have resulted in service disruptions at companies like Azure, Dropbox, Google, and Amazon, and shows how to plan for and minimize risk when it comes to your own cloud deployments. He introduces concepts such as software as a service (SaaS) and infrastructure as a service, and the differences between public and private clouds. Then, after reviewing the cloud security best practices from the Cloud Security Alliance and the European Network and Information Security Agency (ENISA), Malcolm shows how to use SABSA, a popular security requirements mapping approach, to figure out the business requirements for a successful and secure cloud deployment of your own.

### [Cybersecurity Awareness: Security for Cloud Services](#)

1 hour

Many organizations are abandoning on-premises hosting in favor of cloud services—however, cloud computing is still a mystery to many. By becoming better acquainted with the various types of cloud offerings—as well as the general security risks involved with each option—companies and organizations can determine if cloud services are right for them. This course covers the different types of cloud service offerings, and presents security advantages and disadvantages as well. Plus, learn about the risks associated with using Skype and Dropbox, as well as risk mitigation strategies.

### [Implementing an Information Security Program](#)

2.5 hours

Building and operating an information security program at your organization can be challenging. The scope can be vast and complex. Thinking of all the ways an organization can fail and coming up with actionable measures you can take to prevent issues, mitigate risk, or recover from events is a large undertaking. In this course, Kip Boyle, president of Cyber Risk Opportunities, guides you through the entire process of creating an information security program, rolling it out to your organization, and maintaining it for continuous risk management.

### **IT Security Careers and Certifications: First Steps**

2.5 hours

Demand for information security professionals has never been higher—and it's only projected to grow. Interested in finding a job in this exciting new field? Or simply advancing to the next level? IT security expert Marc Menninger explains how to launch and develop a successful career in information security. Learn about the nine most common security jobs and the duties and qualifications for each role. Learn which security certifications appear in job listings and which ones will help you get the job you want. Follow example career paths to learn how others have progressed: from IT hobbyist to help-desk technician to analyst, systems architect, and more. Marc closes with career advice specific to information security, which will help you succeed in this dynamic and high-demand industry.

### **IT Security Foundations: Core Concepts**

1.5 hours

Computing and Internet security are everyone's business, but it's especially critical for information technology specialists. Learning the core concepts of operating-system and network-level security helps avoid ongoing threats and eliminate system vulnerabilities. This beginner-level course covers core security concepts and introduces risks such as social engineering, malware, and spyware. *Foundations of IT Security* series creator Lisa Bock will also go over some basic wireless security best practices, tips for beefing up browser security, and techniques for implementing encryption.

### **IT Security: Key Policies and Resources**

0.5 hours

Cybersecurity can be daunting because of its technical complexity and the ever-changing threats that professionals must grapple with. And more than ever, cybersecurity is not just an IT issue, but a core business issue for organizations of all kinds. Just like other business issues—such as finance, legal, or human resources—cybersecurity has its own set of external policies, laws, rules, established practices, and resources for getting help. Getting to know these policies and resources better across your organization—and not just within your IT department—can be hugely beneficial to your company. This course seeks to make key cybersecurity policies and resources clear and understandable—whether you work in IT, in business, or are just interested in how information security fits in with our public policies and laws.

### **Learning Cryptography and Network Security**

2 hours

Though technology changes rapidly, the need to assure the confidentiality, integrity, authenticity, and accountability of information does not. Understanding the basics of cryptography is fundamental to keeping your networks, systems, and data secure. In this course, Lisa Bock reviews the historical and present-day uses of encryption, including techniques such as symmetric and asymmetric encryption, algorithms, and hashing. She also reviews message digest and passwords and provides a demonstration of a typical SSL transaction. By the end of this course, you'll have a solid understanding of what it takes to move and store data securely.

### **Learning Mobile Device Security**

1 hour

Mobile devices have become critical to the way we work and live. That's what makes them such an attractive target to hackers and cybercriminals. This course provides a practical, hands-on approach to securing your mobile device and protecting your hardware, apps, and data from theft and intrusion. Mobile device management expert Ryan Spence provides an overview of the risks and general security best practices, such as choosing and properly disposing of a mobile device and using password protection. He then covers specifics on Android and iOS security, including enrolling in a mobile device management program such as Apple Business Manager and Android Enterprise. Finally, learn how to secure the hardware itself: the camera, microphones, sensors, and radios.

## **Courses to enhance knowledge of *cloud security*:**

### **Amazon Web Services: Data Security**

4 hours

Learn best practices, patterns, and processes for designing and implementing data security with the Amazon Web Services (AWS) cloud. This course can also help to prepare you for the AWS Certified Solutions Architect – Associate exam. Your instructor, Lynn Langit, covers how to use AWS design patterns, tools, and best practices for security, governance, and validation of data used in AWS Identity and Access Management (IAM), Virtual Private Cloud (VPC), and Route 53. She also goes over other AWS tools, such as AWS CloudWatch, CloudTrail, and Inspector; explores encryption concepts; looks at working with security scenarios; and reviews common patterns and practices for implementing disaster recovery processes.

### **Amazon Web Services: Enterprise Security**

2 hours

Cloud computing isn't just for startups. Many of the world's leading companies, including GE and Dow Jones, run on the cloud, and they choose Amazon Web Services (AWS). If you're tasked with implementing AWS at your organization, big or small, this is the course for you. Understanding security concepts is the gateway to using AWS as your enterprise solution. This course is also part of a series designed to help you prepare for the AWS Certified SysOps Administrator – Associate certification exam.

### **Amazon Web Services: Monitoring and Metrics**

2 hours

Amazon Web Services (AWS)—a global leader in cloud computing—provides a wide variety of IT services. As you're financially responsible for whichever AWS services you use, it's important to establish sound financial monitoring to ensure that you're alerted

to any changes before those changes become a financial burden. This course provides system administrators with an intermediate-level look at monitoring and metrics for the AWS platform. This course is also part of a series designed to help you prepare for the AWS Certified SysOps Administrator – Associate certification exam.

#### **AWS for DevOps: Monitoring, Metrics, and Logging**

3 hours

Enhance your development operations by learning how to work with monitoring tools from Amazon for services and applications. In this course, Lynn Langit explains how to use practical and applicable tools, techniques, and strategies for instrumenting your production AWS applications. She shows how to use product consoles, such as EC2, S3, and RDS. She also discusses and demonstrates using services—such as CloudTrail, CloudFormation, and the newly-announced X-Ray—for monitoring, gathering key metrics, and logging your application's output. Plus, she covers AWS scripting tools, such as the AWS CLI. This course maps to the Monitoring, Metrics, and Logging domain from the AWS Certified DevOps Engineer – Professional exam.

#### **AWS for DevOps: Security, Governance, and Validation**

3 hours

In this course—which was designed for DevOps professionals working with the AWS cloud—learn about AWS tools and best practices for security, governance, and validation. Instructor Lynn Langit covers different security and governance approaches, including outcome-based validation with service level agreements, outcome-based security with audits, and protecting data in-flight and at-rest. Lynn discusses using AWS tools such as CloudWatch, CloudTrail, and Inspector for security monitoring. Plus, she shows how to use third-party security and governance tools, and shares cost control approaches for AWS service billing. This course can also be used as an exam preparation resource, as it covers the topics in the third domain of the AWS Certified DevOps Engineer exam: Security, Governance, and Validation.

#### **Cert Prep: CompTIA Security+ Exam (SY0-501): The Basics**

1 hour

Are you interested in taking the CompTIA Security+ exam to become certified? Pursuing this certification requires a thorough understanding of how to secure networks and devices, participate in risk mitigation activities, and more. This overview course provides CompTIA Security+ candidates with essential information they need to register and prepare for the exam. Cybersecurity expert Mike Chapple goes over the six knowledge domains for exam SY0-501—all of which are covered in greater depth in the other courses in this series—and shares study tips that can help you feel prepared to take and pass the test on your first try. This course works in coordination with the six-course Security+ series and provides a 90-question practice exam as a post-course assessment.

#### **CompTIA Cloud+ (CV0-002) Cert Prep: 2 Security**

1.5 hours

Earning the CompTIA Cloud+ certification can help to enhance your IT career, as this certification validates an IT practitioner's skills and expertise in implementing and maintaining cloud technologies. Cloud+ accredits IT professionals with the constantly changing and advancing knowledge they need to be successful in today's cloud environment. This course can prepare you for the qualifying exam by covering the topics outlined in domain 2.0 of the CompTIA Cloud+ (CV0-002) certification exam: Security. Instructor Joseph Holbrook reviews concepts that can help both experienced IT professionals prepping for exam CV0-002, and current certification holders who need to renew their certification. Joseph reviews security and compliance best practices; security template and access control lists; how to implement the right security technologies; and security automation techniques. He also goes over how to troubleshoot security and connectivity issues.

#### **Learning Cloud Computing: Cloud Security**

1.5 hours

Understand the basics of cloud security—a core component of cloud computing. Beginning with the basics, instructor David Linthicum explains the business case for cloud security and the levels and models available, including infrastructure-, application-, and data-level security; identity and risk management; encryption; and multifactor authentication. He then dives into the services offered by the top three cloud providers: Amazon, Microsoft, and Google. He reviews the compliance issues that affect specific industries, including health care and finance, and reviews the points you need to consider when identifying your security requirements and the security tools, services, and software to best meet those needs.

#### **Microsoft Azure: Security Concepts**

2 hours

The professionals in charge of Azure administration need to know how to secure services correctly to protect the data flowing between client computers and the cloud. This course investigates security concepts related to Azure deployment and services such as Office 365 and Azure Active Directory. Find out how to work with the security portals, secure virtual machines, implement more robust multi-factor authentication, and protect your services and data, including email, documents, and user data. Plus, learn best practices for successfully securing your Azure deployment.

Courses for those professionals focused on **security assessments, security effectiveness and security testing**:

#### **CISSP Cert Prep: 6 Security Assessment and Testing**

2 hours

Learn about security assessment and testing practices needed to prepare for the Certified Information Systems Security Professional (CISSP) exam. CISSP—the industry's gold standard certification—is necessary for many top jobs. This course helps you approach the exam with confidence by providing coverage of key topics, including threat assessment, log monitoring, and software testing. It also covers disaster recovery and security process assessment. Students who complete this course will be prepared to answer questions on the sixth CISSP exam domain: Security Assessment and Testing.

#### **CISSP Cert Prep: 8 Software Development Security**

1.5 hours

Prepare for the Certified Information Systems Security Professional (CISSP) exam by bolstering your knowledge of software development security practices. In this course, follow Mike Chapple as he walks through each topic in the eighth domain of the CISSP exam—Software Development Security. He covers the software development lifecycle and common software security issues, such as cookies, session hijacking, and code execution attacks. Mike also discusses secure coding practices and software security assessment. This course prepares you for the CISSP exam and provide you with a solid foundation for a career in information security.

### **CompTIA Security+ (SY0-501) Cert Prep: 1 Threats, Attacks, and Vulnerabilities**

3.5 hours

The CompTIA Security+ exam is an excellent entry point for a career in information security. The latest version, SY0-501, expands coverage of cloud security, virtualization, and mobile security. This course prepares exam candidates for the critical Threats, Attacks, and Vulnerabilities domain of the exam. By learning about malware, networking and application security exploitations, and social engineering, you'll be prepared to answer questions from the exam—and strengthen your own organization's systems and defenses. Author Mike Chapple, an IT leader with over 15 years of experience, also covers the processes for discovering and mitigating threats and attacks, and conducting penetration testing and scanning for vulnerabilities.

### **Ethical Hacking: Introduction to Ethical Hacking**

1.5 hours

What is ethical hacking? When it comes to cybersecurity, hacking comes in many colors: white, grey, black, and shades in between. White hat hackers use their skills for good. They practice ethical hacking: involved testing to see if an organization's network is vulnerable to outside attacks. Ethical hacking is key to strengthening network security, and it's one of the most desired skills for any IT security professional. If you're interested in becoming an ethical hacker, or getting started securing your own network, this introduction is for you.

### **Ethical Hacking: Denial of Service**

1.5 hours

Ethical hacking involves testing to see if an organization's network is vulnerable to outside threats. Denial-of-service (DoS) attacks are one of the biggest threats out there. Being able to mitigate DoS attacks is one of the most desired skills for any IT security professional—and a key topic on the Certified Ethical Hacker exam. In this course, learn about the history of the major DoS attacks and the types of techniques hackers use to cripple wired and wireless networks, applications, and services on the infrastructure. Instructor Malcolm Shore covers the basic methods hackers use to flood networks and damage services, the rising threat of ransomware like Cryptolocker, mitigation techniques for detecting and defeating DoS attacks, and more.

### **Ethical Hacking: Enumeration**

2 hours

Ethical hacking is one of the most desired skills for any IT security professional. White hat hackers can detect, prevent, and mitigate network intrusions and data theft: a critical liability for any company that does business online or in the cloud. This course introduces to the concept of enumeration—identifying the resources on a host or network, including user names, ports and services, policies, and more. It covers protocol, process, and service enumeration on Windows and Linux, and maps to the Enumeration competency from the Certified Ethical Hacker (CEH) body of knowledge. Malcolm discusses host profiling, enumerating protocols (such as SMB, RPC, and SNMP), and enumerating the Internet, and concludes with demos of third-party tools organizations can use to mitigate risk, including SuperScan, NetScan Pro, and JXplorer.

### **Ethical Hacking: Exploits**

1.5 hours

In addition to damaging and disabling computers, malware (malicious software) can compromise the security of stored data and can spread to other machines. To protect the integrity of networks and systems, penetration testers benefit from learning how malware works. In this course, cybersecurity expert Malcolm Shore discusses how to avoid being hacked or attacked by explaining the mechanics of malware and other exploits—harmful software that takes advantage of flaws. Malcolm shows how to test if your organization's network is vulnerable, a crucial skill for IT security professionals. He also demonstrates how to use basic and advanced debugging tools by taking you through the uses for each.

### **Ethical Hacking: Footprinting and Reconnaissance**

1.5 hours

If you watched our *Introduction to Ethical Hacking* course, you know the basics of ethical hacking. Ethical hackers use their knowledge for good: to test if an organization's network is vulnerable to outside attacks. But where do they start? With footprinting (aka reconnaissance), the process of gathering information about computers and the people to which they belong. In this course, Lisa Bock introduces the concepts, tools, and techniques behind footprinting: finding related websites, determining OS and location information, identifying users through social media and financial services, tracking email, and more. Footprinting relies on tools as simple as a web search and dumpster diving, and as complex as DNS interrogation and traceroute analysis. Lisa shows how to put these nefarious sounding tools to work for good, and mitigate any risks an organization has to these types of attacks.

### **Ethical Hacking: Mobile Devices and Platforms**

2 hours

Mobile devices are used for our most sensitive transactions, including email, banking, and social media. But they have a unique set of vulnerabilities, which hackers are all too willing to exploit. Security professionals need to know how to close the gaps and protect devices, data, and users from attacks. Join author Malcolm Shore as he explores the two dominant mobile operating systems, Android and iOS, and shows ways to protect devices through analysis and testing. Watch this course to review the basics of mobile OS models, the toolsets you need for testing, and the techniques for detecting and preventing the majority of security flaws.

### **Ethical Hacking: Penetration Testing**

1.5 hours

You've done everything you can to logically secure your systems, along with layering in user education and providing physical security. However, the only way to *know* if your defenses will hold is to test them. This course looks at one of the most important skills of any IT security professional: penetration testing. A key competency for the Certified Ethical Hacker exam, penetration testing is the process to check if a computer, system, network, or web application has any vulnerabilities. Cybersecurity expert Lisa Bock



reviews the steps involved in performing a worthwhile penetration test, including auditing systems, listing and prioritizing vulnerabilities, and mapping out attack points a hacker might target. She also defines the various types of "pen" tests—such as black, grey, and white box; announced vs. unannounced; and automated vs. manual testing—and the techniques and blueprints a pen tester should use to test everything from Wi-Fi to VoIP. Finally, she discusses how to choose and work with an outsourced pen-testing organization, which can bring a valuable outsider's perspective to your IT security efforts.

#### **Ethical Hacking: Perimeter Defenses**

1.5 hours

Ethical hacking—testing to see if an organization's network is vulnerable to outside attacks—is a desired skill for many IT security professionals. In this course, cybersecurity expert Malcolm Shore prepares you to take your first steps into testing client defenses. Malcolm provides you with an overview of firewall technology, and demonstrates the two main operating system firewalls. Next, he goes into web application firewalls and API gateway threat mitigation solutions. Learn about the Cowrie honeypot, how to use Security Onion to detect intrusions, and more.

#### **Ethical Hacking: Scanning Networks**

2 hours

After footprinting and reconnaissance, scanning is the second phase of information gathering that hackers use to size up a network. Scanning is where they dive deeper into the system to look for valuable data and services in a specific IP address range. Network scans are also a key tool in the arsenal of ethical hackers, who work to prevent attacks on an organization's infrastructure and data. This course investigates the scanning tools and techniques used to obtain information from a target system, including specially crafted packets, TCP flags, UDP scans, and ping sweeps. Lisa Bock discusses how hackers can identify live systems via protocols, blueprint a network, and perform a vulnerability scan to find weaknesses. She also introduces some of the tools and techniques that hackers use to counter detection via evasion, concealment, and spoofing. In addition, learn how to reduce the threat of tunneling, a method hackers use to circumvent network security.

#### **Ethical Hacking: Session Hijacking**

1.5 hours

One of the most sophisticated forms of cyberattacks is session hijacking. Hackers take over network, web, or service sessions—the valid interactions of unsuspecting users—in order to gain unauthorized access to data and systems and attack an organization from the inside. The root failure is weaknesses in common protocols. To prevent these attacks, IT security professionals need to know which protocols are vulnerable and how to test their systems for exposure. This course teaches you what session hijacking is, and how black-hat hackers use it to attack an organization. Learn how TCP, web, and wireless protocols work and how hackers exploit them. Find out how to use built-in Windows and Linux tools, as well as specialized third-party solutions such as Zed Attack Proxy (ZAP) and Cain, to detect and shore up vulnerabilities.

#### **Ethical Hacking: Sniffers**

1.5 hours

Ethical hackers: Get an inside look into the tools the black hat hackers use to "sniff" network traffic, and discover how to countermeasure such attacks. Security ambassador Lisa Bock explains what a sniffer is, and how hackers use it to intercept network traffic. She reviews the seven-layer OSI model, active vs. passive attacks, and the different types of protocol attacks, including MAC and macof attacks, DNS caching and forgery, DHCP denial-of-service attacks, and ARP cache poisoning. Learn how ethical hackers have an arsenal of tools to emulate these attacks and techniques, from examining headers and URLs to capturing images.

#### **Ethical Hacking: Social Engineering**

1.5 hours

Social engineering is a technique hackers use to manipulate end users and obtain information about an organization or computer systems. In order to protect their networks, IT security professionals need to understand social engineering, who is targeted, and how social engineering attacks are orchestrated.

#### **Ethical Hacking: System Hacking**

1.5 hours

System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. This course explains the main methods of system hacking—password cracking, privilege escalation, spyware installation, and keylogging—and the countermeasures IT security professionals can take to fight these attacks.

#### **Ethical Hacking: Trojans and Backdoors**

1.5 hours

It is crucial to maintain a network secure enough to prevent sophisticated attacks, especially if you are part of an enterprise organization. Some of the more dangerous threats to your systems are Trojans and backdoors, which get into computers and compromise the integrity of the system. Data leaks, dissemination, and destruction are just some of the unfortunate outcomes caused by such attacks.

#### **Ethical Hacking: Viruses and Worms**

1 hour

Malware is often one of the first ways hackers will target a system or network. Ethical hackers can combat malware such as viruses and worms by understanding exactly how they are created, dispersed, detected, and neutralized. This course is part of our *Ethical Hacking* series, designed to give security professionals the tools to defend against attacks and prepare for the Certified Ethical Hacking exam. Join security ambassador Lisa Bock for an overview of malware, the differences between viruses and worms, and current virus trends and types, including macro, boot, shell, and cluster viruses. She also reviews the threat of polymorphism, techniques for overriding parasitic viruses, and the growing threat of ransomware. By the end of the course, you'll have the skills to detect and defend against malware on your own computer or your company's network.

#### **Ethical Hacking: Website and Web Application Testing**

1.5 hours

Websites and web applications are—by their very nature—accessible remotely, which puts them at high risk of cyber-attacks. Knowing how to detect and prevent web attacks is a critical skill for developers and information security professionals alike. Find out how to test your sites and applications for weaknesses in this course with cybersecurity expert Malcolm Shore. Malcolm examines the

various parts of a web application (focusing on the most vulnerable components), and introduces the Open Web Application Security Project (OWASP), which provides documentation, tools, and forums for web developers and testers.

### **Ethical Hacking: Wireless Networks**

1.5 hours

Wireless networks are convenient and popular, but poor configuration and encryption leave them open to attack. Hackers can use Wi-Fi vulnerabilities to infiltrate your entire network. Security professionals need to know how to detect, prevent, and counter these kinds of attacks using the latest tools and techniques—the subject of this course with cybersecurity expert Malcolm Shore. Malcolm covers everything from configuring basic security to understanding how hackers extract passwords, harvest connections at rogue access point, and attack networks via Bluetooth. He also explains how to select the right antennae for testing and introduces some sophisticated Windows and Linux tools to scan for vulnerabilities, including Acrylic, Ekahau, and Wireshark. By the end of the course, you should be able to shore up your wireless connections and gain confidence that your local network is safe to use.

### **IT Security Foundations: Operating System Security**

1.5 hours

The operating system is where many attacks are targeted, which makes OS-level security just as important to your organization as network security. OS security is also a key component of the Microsoft Technology Associate (MTA) Security Fundamentals exam (98-367). In this course, instructor Lisa Bock details what's actually involved in securing an operating system. Lisa reviews user authentication, the structure of Active Directory, and how to assign permissions and create audit policies. In addition, she covers various cryptographic techniques, as well as how to protect servers and email.

### **Oracle Database 12c: Security**

4 hours

Database security is one of the hottest topics for Oracle DBAs, and one of the most important aspects of their role. With the increasing risks of cyberattacks, database hacks, and data leaks, knowing how to fully enable and leverage all of the Oracle 12c security features is essential. In this course, Oracle instructor and consultant David Yahalom covers this vitally important and in-demand skill. Learn how to identify the major risks and security threats, and review general best practices for properly protecting and "hardening" any production database.

### **Performing a Technical Security Audit and Assessment**

2.5 hours

This course follows a proven methodology for conducting thorough and effective technical security audits and assessments based on guidelines from NIST. Learn how to develop the testing methodology essential for technical security reviews. Discover how to identify and analyze targets, use key technical testing tools, identify and mitigate findings, and more. Performing technical information security audits and assessments is essential to protecting information assets. By the end of this course, you'll know how to determine if your network is secure.

### **Securing Android Apps**

2 hours

Securing or "hardening" Android apps is an important final step to ensure code, keys, and credentials, as well as the developer's intellectual property, are well protected. This course provides an introduction to the key features of the Android security model: from the Android operating system to the hardware it runs on. Instructor Malcolm Shore demonstrates the weaknesses in some sample commercial Android apps, and shows the default output from existing development environments, including Android Studio, PhoneGap, and RAD Studio. He then explains a range of tools and techniques to increasingly harden an Android app, secure known vulnerabilities, and test your work. Malcolm also reviews advanced techniques for securing enterprise apps and leveraging the security enhancements in Android O. Using these tutorials, you'll be able to develop more secure and more robust mobile applications.

### **Securing SQL Server 2012**

1.5 hours

Make sure your network's SQL Servers are secure, using best practices for physical, instance, network, and file system security. Gerry O'Brien introduces basics like SQL Server securables, principals, logins, users, and roles. Then learn how SQL Server checks permissions and use that information to create accounts and assign logins and roles. Last, Gerry explains common network security risks and steps you can take to secure network protocols.

### **Securing the IoT: Designing and Testing**

3 hours

It is estimated that by 2020, there will be 20 billion IoT devices worldwide. Designing security around these devices is crucial. In this course, Malcolm discusses what some of the security concerns are, and then shows you how to design with these concerns in mind. He covers IoT development and he explains how to test an IoT gateway and IoT devices.

### **Securing the IoT: Privacy**

2 hours

The rapid expansion of IoT technology brings with it an array of exciting and imaginative ways to make our products smarter and our lives easier. But the growth of this emerging technology also brings with it huge gaps in security. The IoT is plagued with vulnerabilities, malware, DDoS attacks, and the potential to disrupt infrastructure. In this course, join Lisa Bock as she explores the relationship between security, privacy, and the IoT. Lisa discusses how the vulnerabilities in IoT devices have the potential to compromise user privacy and make them more susceptible to attacks and glitches. In addition, she discusses IoT privacy concerns; existing standards, regulations, and guidelines, such as HIPAA and Sarbanes-Oxley; and proposed standards and legislation that are currently in the works to ensure the privacy of the data collected on the IoT.

### **Securing Windows Server 2016: Server Hardening Solutions**

1.5 hours

Maintaining a secure server environment is one of the most crucial tasks for professionals charged with administering enterprise networks. In this course, learn about server hardening solutions for Windows Server 2016. Ed Liberman explains how to configure file and disk encryption, as well as how to configure patches and updates. Plus, he covers implementing antimalware.

## Courses for those professionals focused on *security architecture, engineering & operations*:

### **CISSP Cert Prep: 7 Security Operations**

2 hours

Prepare for the Certified Information Systems Security Professional (CISSP) exam and gain crucial knowledge about best practices in security operations. Mike Chapple walks through each topic in the seventh domain of the CISSP exam. He explains how to conduct and support investigations, find evidence using forensics, and report and document security incidents. In addition, Mike goes into logging and monitoring activities, resource security, and security principles, as well as the importance of incident response and emergency management programs. This course—along with the others in this nine-part series—prepare you for the CISSP exam and provide you with a solid foundation for a career in information security.

### **Exchange 2016: Infrastructure, Recipients, and Security**

2.5 hours

Bolster your understanding of the infrastructure, recipients, and security features in Exchange Server 2016, to help ensure that your Exchange installation goes to plan. This course maps to the Designing and Deploying Microsoft Exchange Server 2016 (70-345) exam, specifically the following domain: Plan, deploy, and manage an Exchange infrastructure, recipients, and security. In this course, Scott Burrell helps you get a clear understanding of key features, to prepare you to create your own Exchange organization. Scott covers how to plan and configure Active Directory, create mailboxes, and configure security features that can help you keep your Exchange content safe.

### **Microsoft Cybersecurity Stack: Securing Enterprise Infrastructure**

1.5 hours

The rise of the hybrid cloud has rendered traditional data center infrastructure security approaches insufficient. The modern IT professional must be equipped with the knowledge and skills to defend against an array of threats, such as threat actors trying to penetrate IaaS and PaaS resources hosted in public clouds. In this installment of the *Microsoft Cybersecurity Stack* series, instructor Pete Zerger demonstrates how to design and implement an approach to securing your data center and cloud infrastructure from a variety of internal and external threats. Pete goes over the features and benefits of Hyper-V guarded fabric, explores shielding data in VMs on guarded fabric, explains how to manage and respond to security threats, and discusses encrypting data in Azure virtual machines.

### **Microsoft Cybersecurity Stack: Advanced Identity and Endpoint Protection**

2 hours

With the rise of the cloud, the traditional model of the network perimeter is dead—identity is the new control plane. This course offers advanced techniques for identity and endpoint security with the Microsoft cybersecurity stack: Enterprise Mobility + Security (EMS) and Azure Active Directory Premium. Instructor Peter Zerger shows how to set up secure access to resources in any app, on any cloud, and from any device. Learn how to configure virtual-based security with Windows Defender Device Guard and Credential Guard, secure email with Exchange Online ATP, control what happens after a breach with Advanced Threat Analytics, and protect the cloud with Azure Active Directory. Plus, find out how to use Windows Defender ATP and manage access to secure Azure resources using privileged access.

### **Microsoft Cybersecurity Stack: Identity and Endpoint Protection Basics**

2 hours

The traditional model of the network perimeter is dead. The perimeter—where access and authorization are enforced—can be anywhere, on any device. With the evolution of Microsoft Enterprise Mobility + Security (EMS) and Azure, the Microsoft enterprise cybersecurity story is growing increasingly more exciting. The *Microsoft Cybersecurity Stack* series of courses provides IT pros with a holistic view of the Microsoft cybersecurity stack, and how to configure those components to strengthen an organization's security posture. These hands-on courses demonstrate how to configure EMS and Azure features, and how to combine them for greatest effect.

### **Microsoft Cybersecurity Stack: Securing Enterprise Information**

2 hours

Today's users expect to be productive wherever they are. IT pros must look beyond the traditional network perimeter model, and discover how to design and implement a comprehensive strategy for protecting corporate information. The *Microsoft Cybersecurity Stack* series shows how to use the Microsoft cybersecurity stack to strengthen your organization's security posture.

### **Microsoft Enterprise Mobility Suite: Management and Security**

2.5 hours

Microsoft Enterprise Mobility + Security (EMS) provides a comprehensive solution for managing and protecting users, data, devices, and apps. In this intermediate-level course, instructor takes a deep dive into EMS, showing you how to work with the management and security tools in this service. Sharon covers Azure Active Directory services—including the Premium services in EMS—and goes into using Azure Information Protection to secure information and protect data. She also covers using Intune to manage mobile devices and apps.

### **Securing the IoT: Secure Architectures**

2 hours

IoT is one of the biggest new developments in IT, with growth expected to reach billions of devices in the short term. There is, however, a major gap in understanding of security for IoT. Many first-wave IoT systems are showing significant security weaknesses, and security is often recognized as one of the key blockers to successful IoT deployments. In this course, Malcolm Shore provides guidance for businesses intending to deploy IoT solutions on the end-to-end security architecture required to ensure the comprehensive security of their deployment. He provides an introduction to security architecture and discusses emerging IoT reference architecture, domain specific architecture, proximity network services, and more.

### **SSCP Cert Prep: 2 Security Operations and Administration**

3 hours

The (ISC)2 Systems Security Certified Practitioner (SSCP) certification is an excellent entry point to a career in IT security. To help you prepare for the SSCP exam, instructor Mike Chapple has designed a series of courses covering each domain. In this installment, Mike covers the objectives of Security Operations and Administration, the second domain, which comprises 17% of the questions on the exam. Topics include the security triad, data security, security controls, and compliance training. Learn about core concepts and the security code of ethics, and find out how to document controls, start asset and change management programs, conduct security awareness and training, implement physical controls, and assess the compliance of your organization.

#### **VMware NSX: Security**

1.5 hours

Making sure an organization's software-defined network (SDN) is secure is the main concern for any organization looking to move to the cloud. This course illustrates how NSX, VMware's SDN solution, provides not just a virtual network environment but also a microsegmentation of security in a business context, down to the level of each application for each tenant. This security aspect of NSX can be an eye-opener for many people. Here Bill Ferguson covers edge firewalls and distributed firewalls, role-based security administration, and security control with Service Composer, a tool that allows you to inspect all the data your network sends and receives.

#### **VMware vSphere: Configure and Administer Security**

1 hours

VMware is the market leader in virtualization. Their cloud-based virtualization platform, vSphere, is the software of choice for organizations looking to go virtual. This course, by VMware Certified Instructor Rick Crisci, shows what it takes to configure and manage security in a VMware vSphere environment—a key skill for any systems administrator or virtualization pro. Rick covers managing vCenter roles and permissions, as well as local ESXi permissions and authentication. Plus, learn how to secure and harden the vSphere environment, including virtual machines, switches, services, and firewalls, and enable single sign-on for your users.

### **Courses on *incident response*:**

#### **Learning Computer Security Investigation and Response**

2 hours

Cybersecurity is a growing area of IT. Qualified computer forensics techs are in demand. But even if you aren't a forensics specialist, it can be useful to know how to collect evidence of harassment, hacking, and identity theft on your own computer or mobile phone. This course covers the basics of computer forensics and cyber crime investigation. Author Sandra Toner provides an overview of forensic science, and discusses best practices in the field and the frameworks professionals use to conduct investigations. Then, after showing how to set up a simple lab, Sandra describes how to respond to a cyber incident without disturbing the crime scene. She dives deep into evidence collection and recovery, explaining the differences between collecting evidence from Windows, Mac, and Linux machines. The course wraps up with a look at some of the more commonly used computer forensics software tools.

### **Courses covering *network security concepts*:**

#### **CCNA Security (210-260) Cert Prep: 1 Security Concepts**

1.5 hours

Earning a Cisco Certified Network Associate (CCNA) Security certification demonstrates that you have the specialized knowledge needed to secure Cisco networks. Join Lisa Bock as she prepares you to tackle the Security Concepts portion of the CCNA Security exam 210-260, Implementing Cisco Network Security. In this course Lisa covers essential security terms, and discusses common security threats such as active and passive attacks, social engineering, and malware. She reviews cryptographic techniques such as encryption and digital signatures, and describes various network topologies such as campus area networks, wide area networks, and data centers.

#### **CCNA Security (210-260) Cert Prep: 2 Secure Access**

1.5 hours

Administering a network means controlling access to network resources: granting, limiting, preventing, and revoking permissions as necessary. This course covers the topic of secure access, including in-band and out-of-band management, secure device access, and protocols such as NTP, SCP, and SNMP, as they relate to the Secure Access domain of Cisco Certified Network Associate (CCNA) Security exam 210-260. Security ambassador Lisa Bock introduces the three *a*'s of triple-A security: authentication, authorization, and accounting. She compares RADIUS and TACACS+ authentication, and BYOD or bring your own device architecture. Plus, learn about mobile device management and security as it applies to the Internet of Things. These lessons will help you configure and manage Cisco devices, prepare for the CCNA Security exam, and properly secure your organization's infrastructure.

#### **CCNA Security (210-260) Cert Prep: 3 VPN**

1.5 hours

Boost your technical skill set by earning a Cisco Certified Network Associate (CCNA) Security certification. By passing the CCNA Security exam, you demonstrate to potential employers that you have the specialized knowledge needed to secure Cisco networks. In this course, join Lisa Bock as she prepares you to tackle the VPN portion of the CCNA Security exam 210-260, Implementing Cisco Network Security. Lisa covers essential VPN concepts—including the different types of VPNs, topologies, and working with the Cisco Adaptive Security Appliance—which offers many functions to help secure networks. She also dives into the IPsec framework, VPN configuration, and how to prepare your site for an IPsec VPN.

#### **CCNA Security (210-260) Cert Prep: 4 Secure Routing and Switching**

1.5 hours

A malicious person that gains access to a switch or router can modify system integrity to steal information or disrupt communications. Cisco Certified Network Associates (CCNAs)-and other qualified network administrators-should know how to

prevent attacks by securing networking devices. This course covers secure routing and switching, including mitigation procedures and VLAN switching, as covered by CCNA Security certification exam 210-260. Lisa Bock, a security ambassador, explains the difference between the control, data, and management planes in networking, and provides to an overview of Layer 3 attacks and techniques for securing Cisco routers. Next, she addresses Layer 2 attacks and techniques to secure Cisco switches. She includes mitigation procedures such as dynamic ARP inspection and BPDU guard, and wraps up with a discussion of VLAN security.

#### **CCNP Routing (300-101) Cert Prep: Router and Routing Security**

1 hour

Earning a Cisco CCNP Routing and Switching certification can accelerate your career by demonstrating to potential employers that you have the skills needed to work on complex networking solutions. In this course, Greg Sowell prepares you for exam 300-101 ROUTE, Implementing Cisco IP Routing—a qualifying exam for the CCNP Routing and Switching certification—by reviewing key router and routing security concepts. Greg explores how to use time-based and infrastructure ACLs, protect passwords, and prevent spoofing on a network using Unicast Reverse Path Forwarding (uRPF). He also covers Simple Network Management Protocol (SNMP), OSPF and BGP authentication, and more.

#### **CCNP Switching (300-115) Cert Prep: 2 Infrastructure Security and Services**

1 hour

Validate your enterprise networking knowledge and expertise by earning a CCNP Routing and Switching certification. In this course, Greg Sowell prepares you for the Infrastructure Security and Infrastructure Services portions of exam 300-115 SWITCH, Implementing Cisco IP Switched Networks—one of three required exams for the CCNP Routing and Switching certification. Here, Greg covers how to use Hot Standby Routing Protocol (HSRP) to provide fault-tolerant gateways for hosts. He also discusses how the Gateway Load Balancing Protocol (GLBP) can be used to both provide gateway redundancy and natively load balance connections across multiple gateways simultaneously. Plus, learn about VLAN security, spoofing prevention, centralizing user management, and more.

#### **CISSP Cert Prep: 4 Communication and Network Security**

4 hours

The Certified Information System Security Professional (CISSP) certification is an important component of any security professional's resume, and is a requirement for many top jobs. In this course, prepare for the fourth domain of the exam: Communications and Network Security. Instructor and cybersecurity expert Mike Chapple goes over TCP/IP networking, network security devices, and secure network design. Mike also includes coverage of specialized networking, network attacks, wireless networking, and more.

#### **CompTIA Security+ (SY0-501) Cert Prep: 2 Technologies and Tools**

5.5 hours

Earning the CompTIA Security+ certification can help kick-start your career in information security. This course—the second installment in a series readying you for version SY0-501 of the CompTIA Security+ exam—prepares you to tackle the Technologies and Tools domain. Instructor Mike Chapple—an IT leader with over 15 years of experience—covers key topics, including how to install network components that can help support enterprise security, leverage security and monitoring technologies, troubleshoot security issues, improve the security of mobile devices, and secure common protocols. Visit [certmike.com](http://certmike.com) to join one of his free study groups.

#### **CompTIA Security+ (SY0-501) Cert Prep: 3 Architecture and Design**

4 hours

CompTIA Security+ certification is an excellent entry point for a career in information security. This course prepares candidates for the third domain of the qualifying exam: Architecture and Design. The emphasis of this domain is building security into every aspect of your organization—using security standards, user training, secure systems design, smart development practices, cloud computing and virtualization, automation, and physical security controls.

#### **CompTIA Security+ (SY0-501) Cert Prep: 4 Identity and Access Management**

2 hours

Pass the CompTIA Security+ exam with our certification prep training. This installment prepares candidates for the fourth domain of the CompTIA Security+ exam: Identity and Access Management. This domain covers everything you need to know to identify your users, verify their identities, limit their access, and manage their accounts on an ongoing basis. The skills taught in this course are vendor-neutral, core principles that any IT security pro should master, regardless of company size or industry.

#### **CompTIA Security+ (SY0-501) Cert Prep: 5 Risk Management**

3.5 hours

Earning the CompTIA Security+ certification demonstrates to potential employers that you have a foundational understanding of network security and risk management concepts. This course—the fifth installment in a series readying you for version SY0-501 of the CompTIA Security+ exam—prepares you to tackle the Risk Management domain of the exam. Instructor Mike Chapple—an IT leader with over 15 years of experience—covers key topics, including risk assessment; business impact analysis concepts; personnel management; security education and compliance training; disaster recovery; and preparing for incident response. Visit [certmike.com](http://certmike.com) to join one of his free study groups.

#### **CompTIA Security+ (SY0-501) Cert Prep: 6 Cryptography**

2.5 hours

Prepare to take and pass the CompTIA Security+ exam. This installment of the *CompTIA Security+ (SY0-501) Cert Prep* series prepares candidates to confidently approach the Cryptography domain of the exam. Topics include encryption, symmetric and asymmetric cryptography, and key management. Plus, instructor Mike Chapple—an experienced IT leader—dives into hash functions, digital signatures, cryptanalytic attacks, and cryptographic applications.

#### **CompTIA Server+ (SK0-004) Cert Prep: 4 Security**

2 hours

Earning the CompTIA Server+ certification signals to potential employers that you have a robust understanding of server management. It's a vendor-neutral certification that ensures administrators can manage a variety of systems, including web servers, virtual servers, mail servers, and more. Our series, *CompTIA Server+ Cert Prep*, is designed to help you prepare for and pass the exam. In this course, Ed Liberman helps you study for the security objectives. Review the three major layers of security—server, network, and data—as well as concepts such as multifactor authentication, logical access control, and environmental security.



### **Data-Driven Network Security Essentials**

1 hour

Explore essential concepts, skills, and techniques for managing network security and forensics. In this course, Jungwoo Ryoo explains how to improve network security and forensics by leveraging data. He begins by reviewing essentials such as firewalls, VPNs, and vulnerability management systems. Next, he explores different data sources, and explains how the data from diverse sources can be a powerful tool to enhance your network security. Jungwoo also covers network data collection techniques and tools, and machine learning and visualization to process network data and detect anomalies.

### **IT Security Foundations: Network Security**

1.5 hours

Network security is the keystone of IT security, and an important component of the Microsoft Technology Associate (MTA) Security Fundamentals exam (98-367). In this installment of *Foundations of IT Security*, series creator Lisa Bock will cover one of the main topics of the exam: securing an organization's network to keep interconnected systems and data safe. The course introduces security devices such as firewalls and packet inspectors, network isolation, and common security protocols. She also provides an overview of how to protect clients with antivirus software, encrypt offline files, and implement software restriction policies. Finally, she looks at the often-overlooked topics of mobile device and physical security, which includes securing a building's perimeter and the hardware within.

### **Securing Windows Server 2016: Implementing Workload Specific Security**

1 hour

Discover how to implement workload specific security in Windows Server 2016. In this concise training course, instructor Ed Liberman discusses secure application development, including how to install Security Compliance Manager (SCM) and configure and deploy a security baseline. He also covers secure file services, discussing quota management, file screening, and storage reports. Upon completing this course, you'll be equipped with strategies that can help you maintain a secure server environment.

### **Securing Windows Server 2016: Securing Network Infrastructure**

1.5 hours

Learn how to secure network infrastructure in Windows Server 2016. In this short training course, instructor Ed Liberman shows how to configure Windows Firewall and Datacenter Firewall, secure communications protocols like IPsec and DNSSEC, and shielding a guarded fabric for virtual machines. These simple, practical steps will enable you to secure your network data, traffic, and virtual resources.

### **Windows 10: Security**

2 hours

Whether you are upgrading or starting afresh with a new operating system out of the box, having the peace of mind that your system will be secure is possible by taking a few necessary actions. Protecting your Windows 10 system includes updating authentication and authorization settings, reviewing encryption options, selecting an anti-virus solution, and configuring network settings. Activating native solutions or adding compatible third-party solutions can improve your system's defenses. Completing a few crucial steps and configuring settings according to your needs is the focus of this course, *Windows 10: Security*.

### **Windows 7: Networking and Security**

5 hours

Explore Windows 7 networking and security. Join Steve Fullmer for an exploration of the Open Systems Interconnection (OSI) model, IPv4 and IPv6, Domain Name System (DNS) resolution, and the Dynamic Host Configuration Protocol (DHCP). Learn how to configure Automatic Private IP Addressing (APIPA) and firewalls, and encrypt file systems. Plus, get insights on the Windows 7 security model, User Account Control (UAC), AppLocker, BitLocker, and Windows Defender.

### **Windows 8: Networking and Security**

4.5 hours

Learn about Windows 8 networking and security. Author Steve Fullmer explores the Open Systems Interconnection (OSI) model, IPv4 and IPv6 networking, Domain Name System (DNS) resolution, and wireless networking. Additional topics include public key infrastructure, Windows 8 Defender, the defense-in-depth approach, and User Account Control (UAC).

## **Courses to improve user cybersecurity awareness:**

### **Cybersecurity Awareness: Breaking Down Cloud Security**

2 hours

Cloud computing has made the sharing of information and resources significantly easier—but it has also brought about some unique security concerns. In this entry-level course, instructor Scott Hogg provides an introduction to cloud security, including common terminology and vocabulary. Throughout the course, Scott covers the topic of cloud security in a down-to-earth manner, and provides realistic security measures you can put into practice right away. He reviews the current industry-standard guidelines for cloud security. He also goes into several popular cloud service provider (CSP) security models and security controls.

### **Cybersecurity Awareness: Building Your Cybersecurity Vocabulary**

1.5 hours

Cybersecurity can be an intimidating world to navigate. To speak intelligently on the subject, one must have a basic understanding of certain acronyms and terminology—much of which isn't immediately easy to decode. This practical course was designed to help beginners build their cybersecurity vocabulary, and give them the foundational knowledge they need to approach this subject with confidence. Here, instructor Serge Borso breaks down the vocabulary heard in the cybersecurity industry, and presents scenarios where those words, phrases, and acronyms are used. Upon wrapping up this course, you should have a solid foundation of what cybersecurity is, and what it entails.

### **Cybersecurity Awareness: Cybersecurity While Traveling**

1 hour

Tightly controlled security is a lot tougher when you are on the road. Learn about the various cybersecurity situations you will run into while traveling, and the technology that can be used to help keep you safe. This course reviews the triangle of security, as well as wireless and wired threats and countermeasures. Instructor Jordan Scott designed the training primarily to raise awareness of travel situations commonly encountered while trying to maintain connectivity. This includes accessing open Wi-Fi networks securely, using SSL, setting up VPNs, and more.

#### **Cybersecurity Awareness: Digital Data Protection**

1 hour

Businesses, government agencies, and private citizens are losing the digital data war. Every day brings reports of new breaches, identity theft, stolen intellectual property, military and diplomatic secrets divulged, financial fraud, or humiliating disclosures made by a hacktivist collective. Losses are projected to cost the world economy 2 trillion dollars by 2019. By any measure, this problem has reached crisis proportions. This course examines digital data theft and proposes solutions to protect your privacy and your intellectual property. Join David Kruger to learn about email protection, securing files by default, and controlling files by design. By the end of this course, you should feel more confident in your ability to protect your own data.

#### **Cybersecurity Awareness: Identifying Personally Identifiable Information**

1.5 hours

As we use our computers to play games, pay for goods and services, and apply for jobs, our online identity is constructed from bits of information that we may or may not be conscious of revealing or sharing. This course discusses different information sources about who we are, what we do, where we are, and with whom we are associated—and how we can protect that information from misuse or corruption. Instructor Jennifer Kurtz explains how personally identifiable information (PII) is formed, and how it is valued and used in the marketplace by legitimate and criminal actors. She also covers the formal and informal capture of PII; goes into the legal and regulatory properties of PII; dives into breach case studies in the medical, financial, educational, government, and commercial sectors; and offers PII protection practices for both individuals and organizations.

#### **Cybersecurity Awareness: Malware Explained**

1 hour

Malware poses a threat to anyone who uses a computer. Malware is malicious software that "infects" your machine, giving control to hackers who may delete your files, access your credentials, or even drain your bank account. This course arms learners with the knowledge to avoid and defend against malware. Find out about the history of malware and how it works, and learn about the precautions you should take to protect yourself and your devices. Learn cybersecurity techniques to combat malware, including the most effective antimalware tools for dealing with viruses, ransomware, adware, and spyware.

#### **Cybersecurity Awareness: Mobile Device Security**

1 hour

Mobile devices have become critical to the way we work and live. That's what makes them such an attractive target to hackers and cybercriminals. This course provides a practical, hands-on approach to securing your mobile device and protecting your hardware, apps, and data from theft and intrusion. Mobile device management expert Ryan Spence provides an overview of the risks and general security best practices, such as choosing and properly disposing of a mobile device and using password protection. He then covers specifics on Android and iOS security, including enrolling in a mobile device management program such as Apple Business Manager and Android Enterprise. Finally, learn how to secure the hardware itself: the camera, microphones, sensors, and radios.

#### **Cybersecurity Awareness: Phishing and Whaling**

1 hour

Phishing and whaling are types of cybercrime used to defraud people and organizations. The average 10,000-employee company spends \$3.7 million dollars a year dealing with phishing and whaling attacks alone. It's imperative that all employees of an organization are educated on how to avoid these attacks. Phishing is successful when an email message persuades a person to take an action or reveal information which should not be disclosed. Whaling focuses on high-profile targets such as executives, politicians, and celebrities. Learn about the tactics used in phishing and whaling, and view some examples so that you can identify suspicious emails and network intrusions. Then learn how to reduce your risk and put protections in place to help mitigate these threats.

#### **Cybersecurity Awareness: Safer Digital Communications**

1 hour

The internet is extremely useful and powerful, but it comes with risks. Learn to identify and avoid dangerous situations online and improve the security of your computers and your network. This course is intended to increase your knowledge of internet safety and give you safer digital communication habits. Tom Tobiassen reviews some of the tricks and techniques used by unsavory characters, hackers, and bullies on the internet, and provides tips for protecting your identity, encrypting data, securing your network, and using social media responsibly.

#### **Cybersecurity Awareness: Security Overview**

0.5 hours

Get acquainted with today's cybersecurity reality. In this course—which is part of a series of cybersecurity awareness courses—familiarize yourself with the current state of cybersecurity. Steve Maciejewski identifies, categorizes, and discusses cyber threats, covering the types that would concern a CIO, as well as ones that could endanger any user. Steve also defines the responsibilities of the cyber citizen. Throughout the course, he focuses on risks, threats, and root cause analysis.

#### **Cybersecurity Awareness: Social Engineering**

1 hour

Social engineers—by playing into their target's desire to be helpful and do their job—can trick their victims into casually revealing sensitive internal information. As a result, social engineering is a key concern for all employees of an organization. In this course—which is part of a series of cybersecurity awareness courses—explore some common techniques used by hackers, and learn what end users can do to protect themselves from these attacks. Tom Tobiassen provides some background on social engineering, and covers tactics such as shoulder surfing, RFID theft, scareware, and more.

#### **Cybersecurity Awareness: Social Networking at Work**

1 hour

People and companies leverage the capabilities of social networking sites to stay connected and share information—but there are risks to this technology. Scams on Facebook are a highly common form of malware distribution, and millions of fake Facebook accounts exist. In this course—which is part of a series of cybersecurity awareness courses—join Todd Edmands as he reviews different types of social media and expectations of privacy, and explains the risks of using social media. Plus, he provides ideas on how to protect yourself when using this technology.

**Cybersecurity Awareness: *The Internet of Things (IoT)***

*1 hour*

The Internet of Things (IoT) will change our personal and professional lives forever. By 2020, there are expected to be over 50 billion devices communicating through the internet, ranging from doorbells and thermostats, to cars and washing machines. These devices can make our lives easier and more efficient, but the technology may put our safety and privacy at risk. Knowing about the how the Internet of Things works and what we can do to be safe is important. In this course, Tom Tobiassen provides a basic understanding of IoT, including robots, wearable tech, smart cars, and drones. He discusses the security and privacy implications as well as protective countermeasures that even casual IoT users should know.