livingsecurity

CONTENT CATALOG

Latest Update: March 2025

Living Security is dedicated to diversity

50%
of actors in Living Security content are WOMEN.

85%
of Living Security content includes BIPOC actors.

We use actors that look like *your* end users.

Living Security is available across the globe

Training content is translated in 29 unique languages to serve our worldwide audience.

AVAILABLE LANGUAGES

1. Arabic
   **Arabic is the only language on this list that only has video translations. Assessments and puzzles remain untranslated.*
2. Bulgarian
3. Chinese (Traditional)
4. Chinese (Simplified)
5. Czech
6. Danish
7. Dutch
8. English
9. Finnish
10. French (Canadian)
11. French
12. German
13. Hungarian
14. Indonesian
15. Italian
16. Japanese
17. Korean
18. Norwegian (Bokmål)
19. Polish
20. Portuguese (Brazil)
21. Portuguese (Portugal)
22. Romanian
23. Russian
24. Spanish (Mexico)
25. Spanish (Spain)
26. Swedish
27. Thai
28. Turkish
29. Vietnamese

Ways to view our content

BY TYPE

- Courses
- CyberEscape Online
- Series
- Modules
- Assessments
- Puzzles
- Campaign in a Box
- Mini Boxes

BY CATEGORY

- Authentication & Access
- Data Security & Privacy
- Device Security
- Phishing & Social Engineering
- Physical Security
- Policy & Compliance
- Reporting & Personal Responsibiltiy
- Web Security

BY AUDIENCE

- Vertical-Based
- Department-Based
- Employee Class-Based
- Role-Based

Table of Contents

See also: *different ways to view content.*

Table of Contents

See also: *different ways to view content.*

Table of Contents

See also: *different ways to view content.*

Table of Contents

See also: *different ways to view content.*

Table of Contents

See also: *different ways to view content.*

Table of Contents

See also: *different ways to view content.*

Table of Contents

See also: *different ways to view content.*

Table of Contents

Please note, Campaign in a Box offerings grow on a monthly basis. Support Garden should be referenced for the most up to date offerings.

This section is intentionally left blank due to frequent new content releases throughout the year. Please continue to the next page for details about the content in our catalog.

See also: *different ways to view content.*

Staying Cybersafe: Annual Training Course

General End Users | 45 min
TRAILER HERE.

DESCRIPTION

This comprehensive annual cybersecurity training uses a mix of videos, puzzles, and text-based learning to keep the end user engaged.

LEARNING OBJECTIVES

- Web Security
- Device Security
- Passwords & Authentication
- Data Privacy
- Social Engineering & Phishing

INTEGRATED VIDEOS

- Born Secure Quick Tips: Staying Safe Online
- Case in Point: Synthetic Identity Theft
- Security Basics: Device Security
- Cybersecurity Tonight: Passwords & Authentication
- Cybersecurity Tonight Quick Tips: Stolen Passwords
- Brick Wall: Data Privacy
- Cybersecurity Tonight: Social Engineering & Physical Security
- Security Basics: Phishing
- Cybersecurity Tonight Quick Tips: Themed Phishing
- Vantage Point: Alternative Forms of Phishing

INTEGRATED PUZZLES

- Cyber Criminal Mapping Puzzle
- Mobile Device Safety Puzzle
- Identifying & Protecting PII Puzzle
- Mapping Online Threats Puzzle

Role-Based Annual Training Courses

Role-Basd | 15-20 min
TRAILER HERE.

DESCRIPTION

These pre-built annual training courses make it easy to provide your end users everything they need to know in one go. Each course is built for a specific role at your organization and uses a mix of videos and text based learning to keep end users engaged with material relevant to their positions.

CUSTOMER SUPPORT PROFESSIONALS

Integrated Videos

- Introduction to the course
- Why?: Customer Support
- Day in the Life: Support Professionals
- Compliance Basics: PII
- Vantage Point: Alternative Forms of Phishing
- Compliance Basics: PCI
- Brick Wall: Data Privacy
- Conclusion

DEVELOPERS

Integrated Videos

- Introduction to the course
- Secure Coding: Introduction
- Secure Coding: OWASP
- Secure Coding: Vulnerable Dependencies
- Secure Coding: Threat Modeling
- Secure Coding: Static Analysis
- Secure Coding: Source Code Secrets
- Secure Coding: Patching
- Secure Coding: Least Privilege
- Secure Coding: Injection
- Secure Coding: Authorization & Authentication
- Conclusion

Courses

Role-Based Annual Training Courses (cont'd)

EXECUTIVES
Integrated Videos
- Introduction to the course
- LS Talk: Execs - The Ultimate Target
- Case in Point: Travel Secure
- Vantage Point: Cyber Harassment for Public Figures
- Big Ideas: Privileged Users/Permissions
- Security Basics: Whaling
- Conclusion

EXECUTIVE ASSISTANTS
Integrated Videos
- Introduction to the course
- Why?: Executive Assistants
- LS Talk: Execs - Executive Assistants
- Cybersecurity Tonight Quick Tips: Themes Phishing
- Security Basics: Device Security
- Security Basics: Spearphishing
- Securitiy Basics: Whaling
- Conclusion

FINANCE PROFESSIONALS
Integrated Videos
- Introduction to the course
- Why?: Finance
- Day in the Life: Finance Professionals
- Case in Point: Vendor Email Compromise
- Security Basics: Spearphishing
- Case in Point: Advanced Financial Social Engineering
- Security Basics: Policy Violations
- Conclusion

HIGHLY VISIBLE EMPLOYEES
Integrated Videos
- Introduction to the course
- Why?: Highly Visible Employees
- Vantage Point: Cyber Harassment for

HIGHLY VISIBLE EMPLOYEES (cont'd)
- LS Talk: Executives - Privacy for Executives
- Case in Point: Advanced Financial Social Engineering
- Security Made Simple: Multifactor Authentication
- Vantage Point: Alternative Forms of Phishing
- Security Basics: Spearphising
- Conclusion

HR PROFESSIONALS
Integrated Videos
- Introduction to the course
- Why?: HR
- Day in the Life: HR Professionals
- Compliance Basics: PII
- Security Basics: Insider Threat
- Vantage Point: Alternative Forms of Phishing
- Security Basics: Policy Violations
- Brick Wall: Data Privacy
- Conclusion

IT PROFESSIONALS
Integrated Videos
- Introduction to the course
- Why?: IT
- Big Ideas: Privileged Users/Permissions
- Security Basics: Device Security
- Security Basics: MFA
- Security Basics: Insider Threat
- Security Basics: Shadow IT
- Conclusion

LEGAL PROFESSIONALS
Integrated Videos
- Introduction to the course
- Why?: Legal Department
- Compliance Basics: PII
- Security Basics: Data Classification
- Security Basics: Insider Threat
- Brick Wall: Data Privacy
- Conclusion

Courses

Role-Based Annual Training Courses (cont'd)

MANUFACTURING PROFESSIONALS

Integrated Videos

- Introduction to the course
- Why?: Manufacturing
- Security Made Simple: Social Engineering
- Vantage Point: Alternative Forms of Phishing
- Vantage Point: Lock Your Computer
- Security Made Simple: Insider Threat
- Conclusion

MARKETING PROFESSIONALS

Integrated Videos

- Introduction to the course
- Why?: Marketing
- Brick Wall: GDPR
- Compliance Basics: PII
- Security Basics: Spearphishing
- Vantage Point: Cyber Harassment for Social Media Managers
- Brick Wall: Data Privacy
- Conclusion

PEOPLE MANAGERS

Integrated Videos

- Introduction to the course
- Why?: People Managers
- Case in Point: Reporting Suspicious Activity
- Security Basics: Policy Violations
- Security Basics: Physical Security
- Compliance Basics: PII
- Security Basics: Insider Threat
- Security Basics: Shadow IT
- Conclusion

PEOPLE MANAGERS

Integrated Videos

- Introduction to the course

PRIVILEGED USERS (cont'd)

- Why?: Privileged Users
- Day in the Life: Privileged Users
- Big Ideas: Privileged Users
- Security Made Simple: Data Classification
- Security Basics: Encryption
- Compliance Basics: PII
- Brick Wall: Data Privacy
- Conclusion

PRODUCT DEVELOPMENT PROFESSIONALS

Integrated Videos

- Introduction to the course
- Why?: Product Development
- Data Privacy for Product Development Professionals
- Big Ideas: General Cybersecurity
- Conclusion

SALES PROFESSIONALS

Integrated Videos

- Introduction to the course
- Why?: Sales
- Vantage Point: Alternative Forms of Phishing
- Security Basics: Data Classification
- Case in Point: Travel Secure
- Security Basics: Working Remotely
- Cybersecurity Tonight Quick Tips: Social Media Phishing
- Conclusion

VENDOR MANAGEMENT & PURCHASING PROFESSIONALS

Integrated Videos

- Introduction to the course
- Why?: Vendor/Contractor
- Case in Point: Vendor Email Compromise
- Vantage Point: Pretexting
- Security Basics: Spearphishing
- Vantage Point: Gift Card Scams
- Brick Wall: Data Privacy
- Conclusion

Teams / CyberEscape Online

Critical Mass

General End Users | 45-60 min
TRAILER HERE.

DESCRIPTION
Suspicious behavior at Gizmo Corp. leads one team of remote investigators on a heart-pounding pursuit of a cybercriminal heist which could leak $millions...You are that team!

LEARNING OBJECTIVES
- **Combat Phishing, Spear-phishing, Voice Phishing (Vishing) and SMS-Phishing (Smishing) by identifying red flags that social engineers leave behind**
- **Secure a WFH Workspace (7 Deadly Sins of Work From Home)**
- **Learn Proper Data Classification**
- **Change Default Credentials and Protect IoT Devices**
- **Discover evidence of Insider Threats & Cyber Criminals**
- **Learn 10 Fundamentals of Security Awareness**

INTEGRATED PUZZLES
- *Arrest Warrant*
- *Olivia's Phishy Emails*
- *Data Classification at Gizmo*
- *Avoiding Accidental Insider Threats*
- *Investigate Olivia's Apartment*
- *Cracking the Code*
- *Olivia's Vishing Calls*
- *Camera Feed*

Born Secure: Entrance Exam

General End Users | 8 puzzles: 60 min | 5 puzzles: 45 min | 4 puzzles: 30 min | 3 puzzles: 20 min | 2 puzzles: 15 min
TRAILER HERE.

DESCRIPTION
Jacob Webb has been selected for a top-secret Program that trains new recruits on how to become the world's best cybersecurity operatives. However, first he must pass a test known by the community as the "Entrance Exam."

LEARNING OBJECTIVES
- **Identifying Suspicious Activity & Physical Security**
- **Social Engineering & Spear Vishing**
- **Phishing & Business Email Compromise (BEC)**
- **Identifying Cyber threats**
- **Passwords & Passphrases**
- **Incident Response/Reporting/Escalation**
- **Attack Mapping & Critical Thinking**
- **Communication & Ethics**

INTEGRATED PUZZLES
- *Correct the Security Violations**
- *Go Vish**
- *Building Business Email Compromise**
- *The Weakest Link**
- *Emoji Passphrase**
- *Online Presence Protection**
- *Attack Mapping*
- *Incident Response Management*

**Puzzles also available as Puzzle Modules.*

Teams / CyberEscape Online

Born Secure: Entrance Exam (Retail)

Retail Store Employees | 45-60 min

DESCRIPTION

This variation of Living Security's highly popular Born Secure: Entrance Exam focuses on cybersecurity training most relevant to retail employees. Jacob Webb has been selected for a top-secret program that trains new recruits on how to become the world's best cybersecurity operatives. However, first he must pass a test known by the community as the "Entrance Exam."

LEARNING OBJECTIVES

- Physical security
- Vishing and phishing
- Malicious insider threats
- Secure passphrases
- Sensitive customer information

INTEGRATED PUZZLES

- *Secure the Store*
- *Vishing the Best Depot*
- *Phishing Wall-E-World*
- *Insider Threat Interview*
- *Passphrase Riddles*
- *Retail Store Incident Responder*

Born Secure: Webb of Lies

General End Users
4 puzzles: 45 min | 3 puzzles: 30 min
TRAILER HERE.

DESCRIPTION

Jacob "xGhost" Webb has escaped a life he never asked for as an operative in a morally dubious, underground organization called The Group...but his quiet days living off the grid may be numbered. The arrival of his ex-girlfriend Hannah and two agents from The Group throw his freedom into jeopardy. Even Webb can't take down The Group alone; is Hannah just the partner he needs, or is she working with the enemy?

LEARNING OBJECTIVES

- OSINT
- Social media privacy
- Strong passwords
- Secure payments using e-wallets
- Public Wi-Fi
- Phishing
- Application security
- Physical Security - removable media, clean desk policy, ID badges, tailgating

INTEGRATED PUZZLES

- *Secure Webb's Cabin*
- *Webb of Lies: Mobile Security*
- *Securing Hannah's Social Media*
- *Webb of Lies: Physical Security*

Teams / CyberEscape Online

Legacy Code

General End User | 30 or 45 min
TRAILER HERE.

DESCRIPTION
In order to save her father's company, Cryptik's new CEO Emilia Evans must solve a series of puzzles and uncover the code to a revolutionary new product left behind just for her. Can she do it before the board forces her to sign away her father's legacy forever?

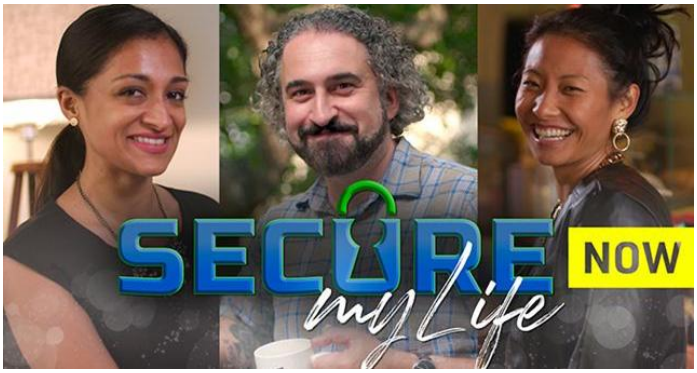
LEARNING OBJECTIVES
- **Strong Passwords & Passphrases**
- **Remote & Home Security**
- **Removeable Media**
- **Sensitive Information**
- **Privacy**

INTEGRATED PUZZLES
- *Henry's Wifi Puzzle*
- *Henry's Shadow IT Puzzle*
- *Henry's AI Privacy Puzzle*
- *Henry's Phishing Hotspot Puzzle*
- *Henry's Password Puzzle*

**Puzzles also available as Puzzle Modules in the Training Platform*

This content is also available on the Training Platform as a series.

Secure My Life Now!



General End User | 45-60 min
TRAILER HERE.

DESCRIPTION
Freelance writer Johan's discovered ransomware on his computer! Will he lose the book he's been working on for years and all of his family photos and videos? Join three cybersecurity experts to help Johan figure out what his options are.

LEARNING OBJECTIVES
- **Ransomware, including what it is, how it infects a computer, and the ethics of paying a ransom**
- **Backing up important data**
- **Social media security, including phishing**
- **Bitcoin security**
- **Backing up important data**

INTEGRATED PUZZLES
- *Johan's Ransomware Message*
- *How'd the Ransomware Spread?*
- *News Feed Red Flags*
- *Profile Page Red Flags*
- *Private Message Red Flags*
- *Consult an Expert: Ransomware*
- *To Pay or Note to Pay?*
- *Bitcoin and Botnets*
- *Work Device vs Personal Device**

**Puzzles also available as Puzzle Modules in the Training Platform*

Teams / CyberEscape Online

Cybersecurity Tonight

General End User | 15-85 min
TRAILER **HERE**.

DESCRIPTION

Welcome to Late Night Tonight with Andre Oliver, LSTV's hit late night talk show! We have a great show for you tonight, jam-packed with guests ready to share their cybersecurity expertise.

LEARNING OBJECTIVES

- **Cybersecurity is part of your job, including reporting suspicious activity**
- **Passphrases, password managers and MFA**
- **Ransomware, including how a device is infected with malware**
- **Phishing, including alternative forms or phishing and red flags**
- **Device updates and mobile device security**
- **Physical security, including removable device policies**
- **Social engineering**

INTEGRATED PUZZLES

- *Rings of Privacy*
- *Password Management Mastery*
- *Panicking Pal: Ransomware**
- *Phishing from a Cybercriminal's Perspective**
- *Most Secure Mobile Device*
- *Secure the Office!*

**Puzzles also available as Puzzle Modules in the Training Platform*

This content is also available on the Training Platform as a series and independent modules.

The Cyber Race

General End User | 60-85 min
TRAILER **HERE**.

DESCRIPTION

With $1 million in crypto on the line, teams of two put their cybersecurity knowledge to the test in this race around the world. This is...The Cyber Race.

LEARNING OBJECTIVES

- Protecting your digital identity
- Cryptocurrency and NFT, defining and exploring associated risks and scams associated
- Deep fakes and how to identify them
- Security in the Metaverse and personal data collected
- Protecting your crypto wallet

INTEGRATED PUZZLES

- *Exploring Biometric Data*
- *Hot & Cold: Your Crypto Wallet*
- *Deepening Your Deepfake Knowledge*
- *Who's the Crypto Master?*
- *Getting Meta: What's the Metaverse?*

This content is also available on the Training Platform as a series and independent modules.

Virtual Tabletop Experience (VTX)

War Room

Leadership | 45-60 min
TRAILER HERE.

DESCRIPTION

When cybersecurity attacks happen to responsible organizations, how do good leaders respond? They call a War Room. They get the right players together to take positive control over a situation and take meaningful action. They get a bridge-call full of the right stakeholders who can mitigate damage and probably save a lot of money.

LEARNING OBJECTIVES

This modern take on traditional tabletop exercises incorporates ten scenario-based puzzles designed to simulate real-life cyber incidents. Participants will use a fictitious company's plans, policies, and procedures to respond to a data breach.

INTEGRATED TRAINING

- Gathering intel to determine whether a incident may be a breach
- Using BCDR to open communication with the correct responders
- IR Plans
- Containing threats and gathering evidence
- Complying with legal regulations
- Communicating internally to prevent information leaks
- Addressing an incident with the public to limit reputational damage
- Implementing security precautions in response to an incident

INTEGRATED EXERCISES

- Gathering intel
- Calling in the right people
- Laying out the IR plan
- Investigation
- Phone tree, legal requirements
- Internal communications
- Email tree, public communications
- Takeaways, executive summary

Training Series

T.G.I.S

General End User | 26:31
TRAILER HERE.

DESCRIPTION
Thank Goodness It's Secure is an episodic sitcom set in a local coffee shop, The Ground Truth. Follow the life of charming new barista, Allie Button, as she helps the shop's lovable regulars learn to lead more secure lifestyles.

INTEGRATED TRAINING
Retention modules per episode (4)

LEARNING OBJECTIVES
- Multi-factor authentication
- Remote access/authentication
- Mobile phishing
- Incident reporting
- Biometric authentication
- Safety online
- Smishing
- Healthy suspicion

True Eye

General End User | 18:02
TRAILER HERE.

DESCRIPTION
True Eye is a Hollywood-style thriller that follows new-hire, Adrian Bridges, through his first day at a global AI-technology firm. Adrian's policy orientation and security training quickly spin into suspense and intrigue as his personal AI device, Guide, starts asking him to do unethical and even dangerous things with sensitive data. His adventure offers a glimpse into proper operational security, how technology affects people, and what we can do about it.

INTEGRATED TRAINING
Retention modules per episode (4)

LEARNING OBJECTIVES
- Password hygiene
- Secure data storage
- Phishing awareness
- Physical security
- Social media privacy
- Safety online
- Device security
- Default credentials

INTEGRATED PUZZLES
- *In-Office Policy Violations*- **Identify the security vulnerabilities**
- *Public or Private?*- **Determine the security level of assets**
- *Calling Co-Worker Together*- **Follow a vishing attack scenario**
- *Jennifer's Hidden Message* - **Create sentences describing security best practices**

Training Series

Phishing IRL

General End User, Phishing Remediation Training | 9:08
TRAILER HERE.

DESCRIPTION
This engaging, training-driven series debunks myths about cyber criminals and better informs end users about what phishing looks like in real life.

INTEGRATED TRAINING
Retention modules per episode (3)

LEARNING OBJECTIVES
- Origination of phishing emails
- Cyber criminal organization
- Phishing email analysis
- Effects of phishing emails

INTEGRATED PUZZLES
- Catching the Big Phish - Determine the best phishing email.
- Spoil the Vish*: Data Dojo** - Stop the vishing attempts.
- Phishing Red Flags - Detect the red flags in phishing emails.

**Puzzles also available as Puzzle Modules in the Training Platform*

The Squad

General End User | 21:00
TRAILER HERE.

DESCRIPTION
It's the year 2027, and the Squad is on the verge of launching their biggest project to date: taking 7G to the moon! However, just before their big day, the Squad's biggest rival, Copy Dat, announces they're doing the same thing! How is this possible?! Did Orson overshare on social media? Did Caleb get phished!? It's a race against the clock to reclaim the Squad's beloved project from being defunded, replace the competitor's project with a better one, and restore glory to its rightful place. Squad up! This one's going to be fun.

INTEGRATED TRAINING
Retention modules per episode (3)

LEARNING OBJECTIVES
- Oversharing on social media
- Privacy settings and cleaning up digital footprint
- Spear-phishing and spear-vishing
- Business email compromise (BEC) & vendor email compromise (VEC)
- Incident response
- Policy & compliance

Training Series

Born Secure: Training Grounds

General End User | 24:00
TRAILER HERE.

DESCRIPTION
This training experience follows Jacob Webb, code-named xGhost, who never considered a life as a cyber-operative until he was hand-picked for a government-funded training program. As xGhost and the other candidates enter Phase 3 of their training, their anticipation of real-world operations grows. But the veil of secrecy leads xGhost into doing someone else's bidding.

INTEGRATED TRAINING
Retention modules per episode (4)

LEARNING OBJECTIVES
- Phishing
- Password hygiene
- Physical security
- Attack mapping
- Asset protection

INTEGRATED PUZZLES
- *Crafting Convincing Phish*
- *7 Violations*
- *Cyber Criminal Mapping**
- *The Biggest Target*

**Puzzles also available as Puzzle Modules in the Training Platform*

Born Secure: Webb of Lies

General End Users
4 puzzles: 45 min | 3 puzzles: 30 min
TRAILER HERE.

DESCRIPTION
Jacob "xGhost" Webb has escaped a life he never asked for as an operative in a morally dubious, underground organization called The Group...but his quiet days living off the grid may be numbered. The arrival of his ex-girlfriend Hannah and two agents from The Group throw his freedom into jeopardy. Even Webb can't take down The Group alone; is Hannah just the partner he needs, or is she working with the enemy?

LEARNING OBJECTIVES
- OSINT
- Social media privacy
- Strong passwords
- Secure payments using e-wallets
- Public Wi-Fi
- Phishing
- Application security
- Physical Security - removable media, clean desk policy, ID badges, tailgating

INTEGRATED PUZZLES
- *Secure Webb's Cabin*
- *Webb of Lies: Mobile Security*
- *Securing Hannah's Social Media*
- *Webb of Lies: Physical Security*

Training Series

Secure My Life

General End User | 30:19
TRAILER HERE.

DESCRIPTION
Working mom, Fiona, has been selected as the latest participant on the hit cybersecurity makeover show Secure My Life! Three experts will transform the security hygiene of Fiona and her family at home, at the office, and on the go. In the end, Fiona will need to prove to the experts just how much she's grown. This 4-part series explores security concerns and best practices in a variety of different environments—in the office, in public, and at home.

INTEGRATED TRAINING
Retention modules per episode (4)

LEARNING OBJECTIVES
- Cybersecurity at home, including internet of things, home Wi-Fi security, and internet safety for children
- Passphrases and password managers
- Travel security, such as malware-loaded USB ports
- Physical security concerns, such as tailgating and shoulder-surfing
- VPNs and the dangers of public Wi-Fi
- Oversharing on social media
- Protecting sensitive information

Healthcare Cyber Checkup

Healthcare Professionals | 15 or 30 min Versions
TRAILER HERE.

DESCRIPTION
Join the staff of a hospital or private clinic as they navigate cybersecurity for healthcare workers in a series of slice-of-life vignettes.

LEARNING OBJECTIVES
- Physical security in a hospital or private clinic environment
- Phishing, specifically for PHI
- Strong passwords/passphrases (Long versions only)
- HIPAA and protected vs unprotected information (Long versions only)

INTEGRATED PUZZLES
- *Physical Security in the Hospital or Physical Security in the Clinic*
- *Phishing for PHI**
- *Password Protecting PHI** **(Long versions only)**
- *What's Protected by HIPAA** **(Long versions only)**

**Puzzles also available as Puzzle Modules in the Training Platform*

This content is also available on the CyberEscape Online Platform.

Training Series

Cybersecurity Tonight

General End User | 22:09 Video
TRAILER HERE.

DESCRIPTION
Welcome to Late Night Tonight with Andre Oliver, LSTV's hit late night talk show! We've got a great show for you tonight, jam-packed with guests ready to share their cybersecurity expertise.

INTEGRATED TRAINING
Retention modules at completion of episode (10)

LEARNING OBJECTIVES
- Cybersecurity is part of your job
- Passwords and authentication including passphrases, password managers and multi-factor authentication
- Malware and ransomware
- Phishing including alternative forms of phishing (smishing, vishing, social media phishing), red-flags and dangers of links and attachments
- Mobile device security and device updates
- Physical security like tailgating and removable media policies
- Social engineering

This content is also available on the CyberEscape Online Platform.

Legacy Code

General End User | 22:09 Video
TRAILER HERE.

DESCRIPTION
In order to save her father's company, Cryptik's new CEO Emilia Evans must solve a series of puzzles and uncover the code to a revolutionary new product left behind just for her. Can she do it before the board forces her to sign away her father's legacy forever?

INTEGRATED TRAINING
Retention modules at completion of episode (5)

LEARNING OBJECTIVES
- MFA
- Strong Passwords & Passphrases
- Phishing
- Remote & Home Security
- Removable Media
- Malware
- Backup
- Sensitive Information
- Privacy
- Artificial Intelligence

This content is also available on the CyberEscape Online Platform.

Training Modules

Day in the Life (2 min)

SAMPLE VIDEO HERE.

TRAINING STYLE

Sometimes the best way to understand something is to see it in action. These role-based training modules will contextualize security policies for your end users by showing them how cybercriminals use violations to their advantage.

See *'Variations'* | 2:00 Videos | 10 questions

DESCRIPTION

An antagonist character highlights how poor security behavior hygiene within an office can open up that organization to an increased risk of a security incident. Users will gain a better understanding of how physical security relates to cybersecurity and why basic security protocols are so important for keeping data (and people) safe.

VARIATIONS

This module is role-based and available for a variety of end users:

- General End Users
- HR Professionals
- Finance Professionals
- Privileged Users
- Support Professionals

LEARNING OBJECTIVES

- Tailgating
- Social engineering, such as taking advantage of people's desire to be helpful
- Shoulder-surfing
- Sharing of sensitive information
- Badge security, including wearing badges outside of the workplace
- Phishing
- Malicious attachments
- Dangers of public Wi-Fi
- Unauthorized visitors

Training Modules

Big Ideas (3-5 min)

SAMPLE VIDEO HERE.

TRAINING STYLE
Each module features an expert-driven conversation, where a single security concept is explained at three levels of difficulty. The conversations begin with a foundational level explanation accessible to all people, followed by an intermediate discussion accessible to most people, building upon the foundation laid in the first discussion. The modules conclude with an advanced discussion between an expert and an active professional to flesh out the concept for more advanced and ambitious learners.

Data Classification
General End Users | 3:59 Video | 10 questions
DESCRIPTION
In this module, users will learn about basic distinctions between public and private data, nuances in classification, and why protecting data is everyone's responsibility.

General Cybersecurity
General End Users | 3:46 Video | 10 questions
DESCRIPTION
In this module, users will learn about basic cybersecurity practices, common violations in the workplace, and how to secure their digital lives.

Password Management
General End Users | 4:03 Video | 10 questions
DESCRIPTION
In this module, users will learn about secure password storage, password management across multiple devices, and the risks of auto-filling credentials in web browsers.

Phishing
General End Users | 3:58 Video | 10 questions
DESCRIPTION
In this module, users will learn about phishing, alternative types of phishing, and how to protect against it.

PII
General End Users | 3:57 Video | 10 questions
DESCRIPTION
In this module, users will learn about personally identifiable information (PII), data protection, and why it's important to prevent breach.

Privacy
General End Users | 4:11 Video | 10 questions
DESCRIPTION
Privacy: In this module, users will learn the benefits and drawbacks of technology, including the reality that it is far too easy to overshare online (e.g. geolocation).

Privileged User/Permissions
General End Users | 4:04 Video | 10 questions
DESCRIPTION
In this module, users will learn what it means to have privileged access, the difference between 'want to know' and 'need to know,' and why privileged users are larger targets for cyber attack.

Vishing
General End Users | 3:30 Video | 10 questions
DESCRIPTION
In this module, users will learn about voice phishing (vishing), the benefits of being suspicious in combating scams, and red flags to look out for.

Training Modules

Security Basics (1-2 min)

TRAILER HERE.

TRAINING STYLE

For the end-user starting at square one, jumping into the deep end of cybersecurity training can be overwhelming. Help them get their feet wet first with these awareness-oriented, introductory training modules.

Data Classification

End Users | 0:58 Video | 3 questions

DESCRIPTION

Users will learn about the types of data, why data needs to be classified, and how they can do so.

Device Security

End Users | 1:00 Video | 3 questions

DESCRIPTION

Users will learn about the physical threats their devices face, why it's important to secure them, and how they can do so.

Encryption

End Users | 1:13 Video | 3 questions

DESCRIPTION

Users will come to understand how encryption hides private information from prying eyes.

Insider Threat

End Users | 1:03 Video | 3 questions

DESCRIPTION

Users will learn what insider threats are, both accidental and malicious.

Internet of Things (IoT)

End Users | 1:03 Video | 3 questions

DESCRIPTION

Users will learn what makes up the IoT, the security threats these devices pose, and how they can better protect their IoT device.

Malware

End Users | 0:58 Video | 3 questions

DESCRIPTION

Users will learn what malware is, why updates are important in defending against it, and how they can protect their devices.

MFA

End Users | 1:15 Video | 3 questions

DESCRIPTION

Users will learn what multi-factor authentication is and discover types of MFA among the three categories (something you know, something you are, and something you have).

Mobile Security

End Users | 1:00 Video | 3 questions

DESCRIPTION

Users will come to understand why mobile device security is important and how they can keep their devices secured.

Password Managers

End Users | 1:05 Video | 3 questions

DESCRIPTION

Users will learn what password managers are, how they work, and why they're an important tool for good cyber hygiene.

Phishing

End Users | 1:14 Video | 3 questions

DESCRIPTION

Users will learn about phishing, including the most common type and how to identify an attack. Understand the concept of phishing

Training Modules

Security Basics (cont'd)

Physical Security
End Users | 1:08 Video | 3 questions
DESCRIPTION
Users will come to understand how physical security is intertwined with cybersecurity and how they can do their part in protecting their organization's physical security.

Policy Violations
End Users | 0:58 Video | 3 questions
DESCRIPTION
Users will come to understand the importance of policy, how policies protect data, and how they protect individuals.

Reusing Passwords
End Users | 1:04 Video | 3 questions
DESCRIPTION
Users will come to understand why reusing their passwords is a security concern, how they can avoid doing so, and how a password manager can improve their password hygiene.

Securing Your Apps
End Users | 0:55 Video | 3 questions
DESCRIPTION
Users will learn about the dangers of unsecured application software and how cybercriminals can use apps against them.

Shadow IT
End Users | 1:24 Video | 3 questions
DESCRIPTION
Users will come to understand the danger of downloading apps without approval and how requesting downloads through the proper channel can prevent breaches and data loss.

Sharing Passwords
End Users | 0:57 Video | 3 questions
DESCRIPTION
Users will learn why sharing passwords is a security concern.

Smishing
End Users | 1:00 Video | 3 questions
DESCRIPTION
Users will learn about smishing, including why it's a threat and how an attack can be spotted.

Spearphishing
End Users | 1:02 Video | 3 questions
DESCRIPTION
Users will learn about spear-phishing, including the difference in tactics between spear-phishing and other types of phishing.

Tailgating
End Users | 0:54 Video | 3 questions
DESCRIPTION
Users will learn what tailgating is, what it's used for, and how to prevent it.

Vishing
End Users | 1:33 Video | 3 questions
DESCRIPTION
Users will learn what vishing is, what it's used for, and how to foil a vishing attack.

Whaling
End Users | 0:58 Video | 3 questions
DESCRIPTION
Users will learn the difference between whaling and spear-phishing, who's targeted in a whaling attempt, and how to identify an attack.

Working Remotely
End Users | 1:14 Video | 3 questions
DESCRIPTION
Users will learn about the risks of remote work and how they can minimize those risks.

Training Modules

Compliance Basics
(1-2 min)

SAMPLE VIDEO HERE.

TRAINING STYLE
Compliance with legal regulations can seem complicated, but it doesn't have to be. Introduce common compliance and regulation topics with these short, easy to understand training modules.

CCPA
End Users | 1:12 Video | 3 questions
DESCRIPTION
Users will learn the basics of the California Consumer Privacy Act.

Data Privacy
End Users | 1:35 Video | 3 questions
DESCRIPTION
Users will learn how to identify suspicious applications and agreements and how to properly adjust their privacy settings.

GDPR
End Users | 1:51 Video | 3 questions
DESCRIPTION
Users will learn the basics of the General Data Protection Regulation, including rights surrounding data storage and the consequences of noncompliance.

HIPAA
End Users | 1:22 Video | 3 questions
DESCRIPTION
Users will learn the basics of the Health Insurance Portability and Accountability Act and how they can safely share and collect patient health information.

PCI
End Users | 1:30 Video | 3 questions
DESCRIPTION
Users will learn about regulations related to Payment Card Information and how they can safely share and collect PCI.

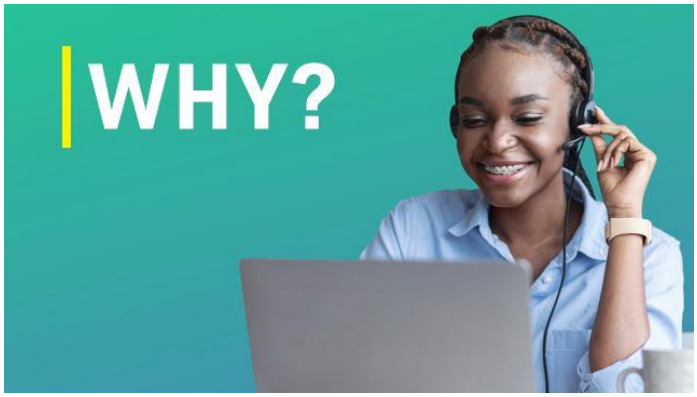
PHI
End Users | 1:41 Video | 3 questions
DESCRIPTION
Users will learn about protected health information, how they can safely collect and share PHI, and why reporting breaches in a timely manner is important.

PII
End Users | 1:49 Video | 3 questions
DESCRIPTION
Users will learn about personally identifiable information and how they can safely share and collect it.

PIPEDA
End Users | 1:09 Video | 3 questions
DESCRIPTION
Users will learn the basics of the Personal Information Protection and Electronic Documents Act.

Training Modules

Role-Based ‘Why?’
(1-2 min)



TRAILER HERE.

TRAINING STYLE

When security awareness material feels relevant and personal, good habits stick. Help your team understand why cybersecurity is important to their role at your organization with these short training modules.

See *‘Variations’* | 0:55-1:30 Videos | 3 questions per Module

DESCRIPTION

Each module of the Role-based ‘Why?’ collection is unique to the role it covers. All modules are accompanied by 3 assessment questions.

VARIATIONS

- Why? Customer Support
- Why? Executive Assistants
- Why? Finance
- Why? Help Desk
- Why? Highly Visible Users
- Why? HR
- Why? IT
- Why? Legal
- Why? Manufacturing Professionals
- Why? Marketing
- Why? People Managers
- Why? Privileged Users
- Why? Product Development
- Why? Sales
- Why? Service Desk
- Why? Vendor / Supply Chain

Training Modules

Case in Point (1-3 min)

SAMPLE VIDEO HERE.

TRAINING STYLE

Because people understand in story and metaphors, Case in Point modules use powerful analogies to educate users on seemingly inaccessible concepts.

Advanced Financial Social Engineering

General End Users | 3:30 Video | 5 questions

DESCRIPTION

In this module, users will experience how convincing advanced financial social engineering can be and learn tactics to avoid becoming a victim of it.

Cloud Security

General End Users | 2:36 Video | 5 questions

DESCRIPTION

In this module, users will learn how to define 'the cloud,' its vital role in storing and transporting data securely, and how to protect that data.

Internet of Things (IoT)

General End Users | 2:39 Video | 5 questions

DESCRIPTION

In this module, users will learn about internet-connected things, their default settings, and how to secure them.

Mobile Security

General End Users | 1:40 Video | 5 questions

DESCRIPTION

In this module, users will learn about mobile device security, how to discern between legitimate and illegitimate applications, and lessons learned from true stories of compromise.

Password Management

General End Users | 1:32 Video | 5 questions

DESCRIPTION

In this module, users will learn about the significant drawbacks of password reuse, the practice of credential stuffing, and the necessity of using a password manager.

Physical Security

General End Users | 1:37 Video | 5 questions

DESCRIPTION

In this module, users will learn about best practices for guarding against inside and outside threats to the company and personal property by keeping a clean desk, minimizing tailgating into secure facilities, and securely disposing of physical material.

Point of Sale Security

General End Users | 3:56 Video | 5 questions

DESCRIPTION

In this module, users will learn the importance of correctly securing PoS locations and the risk associated with locations left unsecure.

Ransomware

General End Users | 2:25 Video | 5 questions

DESCRIPTION

In this module, users will learn about ransomware, backup plans, and how to proactively combat malicious software.

Case in Point (cont'd)

Reporting Suspicious Activity

General End Users | 2:52 Video | 5 questions

DESCRIPTION

In this module, users will learn the importance of reporting suspicious activity and key indicators of when it should be done.

Synthetic Identity Theft

General End Users | 2:37 Video | 5 questions

DESCRIPTION

In this module, users will learn the value of personal data to a cybercriminal, including how small pieces of stolen identification can become a full compromise.

Themed Phishing

General End Users | 2:30 Video | 5 questions

DESCRIPTION

In this module, users will learn about themed emails that are designed to convince people to take action. Here's how to spot them!

Travel Secure

General End Users | 1:42 Video | 5 questions

DESCRIPTION

In this module, users will learn how to secure and stow devices properly while traveling.

Vendor Email Compromise (VEC)

General End Users | 2:39 Video | 5 questions

DESCRIPTION

In this module, users will learn about BEC's cousin, vendor email compromise (VEC), including how to prevent it from impacting their lives, their organizations, and the bottom line.

Work From Home (WFH)

General End Users | 2:29 Video | 5 questions

DESCRIPTION

In this module, users will learn about remote work security, including VPNs, safety online and remote meeting security.

Training Modules

Secure Coding (1-5 min)

TRAILER HERE.

TRAINING STYLE

Technical employees need introductory training, too. These short training modules will introduce your developers and other technical employees to various secure coding concepts. For end users who are already familiar with these concepts, Secure Coding is a great reminder of their importance.

Introduction

Developers | 0:59 Video | 3 questions

DESCRIPTION

Users will be introduced to secure coding training for development teams and come to understand why secure coding is important.

Note: This module acts as an introduction and should be assigned first

Authentication and Authorization

Developers | 1:34 Video | 3 questions

DESCRIPTION

Users will come to understand the difference between authentication and authorization, why both are important, and how they can be tested.

Injection

Developers | 1:40 Video | 3 questions

DESCRIPTION

Users will learn two types of injection (SQL and command) and how to protect against them before publishing.

Least Privilege

Developers | 1:16 Video | 3 questions

DESCRIPTION

Users will learn about the principle of least privilege, including how to uphold it through regular auditing.

OWASP Introduction

Developers | 1:18 Video | 3 questions

DESCRIPTION

Users will learn what the OWASP Top 10 is used for, including the tools and references available to them.

OWASP Update

Developers | 5:00 Video | 3 questions

DESCRIPTION

Review of 2021 OWASP Top 10 categories update.

Patching

Developers | 1:42 Video | 3 questions

DESCRIPTION

Users will come to understand why patching frequently is important, including the consequences of not patching security vulnerabilities.

Source Code Secrets

Developers | 1:41 Video | 3 questions

DESCRIPTION

Users will learn the different forms of source code secrets and come to understand the real-world consequences of sharing them.

Static Analysis

Developers | 1:08 Video | 3 questions

DESCRIPTION

Users will learn what static analysis is used for and what tools they can use to help find bugs before they're in production.

Threat Modeling

Developers | 1:18 Video | 3 questions

DESCRIPTION

Users will learn what threat modeling is used for and the basic steps of the process.

Vulnerable Dependencies

Developers | 1:20 Video | 3 questions

DESCRIPTION

Users will come to understand the risks of using libraries written by others and what tools they have available for detecting vulnerabilities.

Training Modules

Secure My Life Quick Tips (1-2 min)

TRAINING STYLE

The cybersecurity experts from Secure My Life! are back with extra tips and tricks for staying secure at home, at the office, and in public spaces. These training modules work as supplementary material to the Secure My Life! series or Secure My Life Now! CyberEscape Online Experience, or as independently assigned training.

Home Wi-Fi

General End Users | 1:16 Video | 3 questions

DESCRIPTION

Users will come to understand why it's important to secure their home Wi-Fi network and how to do so, including router updates and secure passwords.

Social Media

General End User | 1:29 Video | 3 questions

DESCRIPTION

Users will come to understand why security is relevant to social media, the importance of privacy online, and how to spot a spoofed account.

Updates

General End User | 1:14 Video | 3 questions

DESCRIPTION

Users will come to understand why it's important to promptly install device updates and how they can remember to do so.

Training Modules

Cyber Kitchen (5-7 min)

TRAILER HERE.

TRAINING STYLE

Modeled after instructional cooking shows, Cyber Kitchen pulls end users in with real-life stories from the cybersecurity front lines. Users can copy the recipes to cook at home, driving engagement with the content learned outside of the office.

Cloud Security

General End Users | 7:26 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers least privilege, the importance of staying organized in the cloud, and cloud security concerns such as insider threats.

Cybersecurity at Home

General End Users | 6:36 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers home Wi-Fi and internet of things security, updating devices, and keeping kids safe online.

Mobile Security

General End Users | 7:41 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers public Wi-Fi, USB ports, bluetooth security, strong passcodes, app security, shoulder-surfing, and staying updated.

Passwords & Authentication

General End Users | 7:19 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers strong passwords, passphrases, multifactor authentication, and keeping passwords a secret.

Phishing

General End Users | 7:44 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers staying safe from phishing, vishing, smishing, and social media phishing.

Ransomware

General End Users | 6:21 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers covers what ransomware is, how a device can become infected, the ethical issues with paying a ransom, and the importance of having a backup.

Social Engineering

General End Users | 7:12 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers the various tactics employed by social engineers (priming, framing, loss aversion, familiarity bias, and baiting).

Take Ownership: Cybersecurity is Everyone's Responsibility

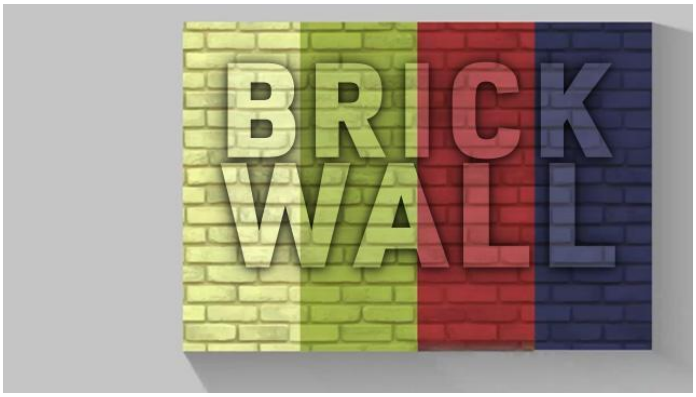
General End Users | 5:34 Video | 5 questions

DESCRIPTION

This episode of Cyber Kitchen covers individual responsibility to learn and practice good cybersecurity hygiene.

Training Modules

Brick Wall (3-7 min)



TRAILER HERE.

TRAINING STYLE

Policies and regulations can be complicated—but that doesn't mean their explanation has to be. These training modules will cover concepts relevant to your company's compliance of legal regulations in a way that's digestible for the average end user. Perhaps most importantly, your end user will understand why they need to know about these topics and what they can do in their own work to maintain compliance.

CCPA

General End Users | 5:00 Video | 5 questions

DESCRIPTION

Users will learn about the rights afforded to Californian consumers under the California Consumer Privacy act (CCPA) and the responsibilities they have in upholding these rights.

Data Privacy in the Workplace

General End Users | 3:24 Video | 5 questions

DESCRIPTION

Users will gain an understanding of data privacy and why it's crucial when handling customer or employee data. They'll be given suggestions for the practical implementation of data privacy in their workplace and for what to do if they suspect data may have been mishandled.

FERPA

General End Users | 2:48 Video | 5 questions

DESCRIPTION

Users will learn about the rights afforded to parents and students under the Family Educational Rights and Protection Act (FERPA).

GDPR Compliance

General End Users | 7:03 Video | 5 questions

DESCRIPTION

Users will gain a basic understanding of the General Data Protection Regulation and what is expected of them to remain compliant. Major learning objectives include the 8 rights of data subjects, the 7 overarching principles of GDPR, special category data, consequences of noncompliance, and when personal data may be processed.

Training Modules

Vantage Point (1-2 min)

TRAILER HERE.

TRAINING STYLE

As much as we rely on it, using technology is inherently risky. Cybercriminals are always looking for ways to take what's yours. They're counting on one thing...that you won't know it's them. Unfortunately for cybercriminals, you only need one thing to see a threat for what it is: a new vantage point.

Alternative Forms of Phishing

General End Users | 1:18 Video | 3 questions

DESCRIPTION

In this module, users will learn about forms of phishing other than email phishing, such as smishing, vishing, and social media phishing.

Creating Strong Passphrases

General End Users | 1:32 Video | 3 questions

DESCRIPTION

In this module, users will learn what makes a password strong and how they can create their own strong passwords using passphrases.

Cyber Harassment for Public Figures

General End Users | 1:17 Video | 3 questions

DESCRIPTION

In this module, users will learn how to manage the harassment those in the public spotlight may face online.

Cyber Harassment for Social Media Managers

General End Users | 1:35 Video | 3 questions

DESCRIPTION

In this module, users will learn the basics of moderating harassment on company social media accounts.

Cyberbullying for Parents and Teens

General End Users | 2:08 Video | 3 questions

DESCRIPTION

In this module, users will learn about the cyberbullying as it relates to kids and teens, including how to recognize warning signs in their own children.

Gift Card Scams

General End Users | 1:23 Video | 3 questions

DESCRIPTION

In this module, users will learn about popular BEC scams involving gift cards.

Lock Your Computer

General End Users | 1:09 Video | 3 questions

DESCRIPTION

In this module, users will learn the importance of locking unattended devices.

Pretexting

General End Users | 1:12 Video | 3 questions

DESCRIPTION

In this module, users will learn how to recognize pretexting, a tactic in which a social engineer will invent a story to make a victim more likely to share information.

Training Modules

Cybersecurity Tonight
(3-4 min)

TRAILER HERE.

TRAINING STYLE
Cybersecurity Tonight covers seven unique cybersecurity concepts all in one place, making it a great fit for your annual training needs. Concepts can also be assigned individually as separate modules and include cybersecurity as a responsibility, physical security, social engineering, phishing, passwords and authentication, mobile device security and device updates, and malware with an emphasis on ransomware.

This content is also available on the CyberEscape Online Platform.

Cybersecurity is Part of Your Job
General End Users | 2:46 Video | 5 questions
DESCRIPTION
In this module, users will learn why cybersecurity is important to their job.

Passwords & Authentication
General End Users | 3:18 Video | 5 questions
DESCRIPTION
In this module, users will learn about passphrases, password managers, good password hygiene, and multifactor authentication

Malware & Ransomware
General End Users | 3:21 Video | 5 questions
DESCRIPTION
In this module, users will learn about ransomware, how devices are infected with malware, and how to stay safe.

Phishing
General End Users | 3:49 Video | 5 questions
DESCRIPTION
In this module, users will learn how to recognize phishing, how to stay safe, and alternative forms of phishing to look out for (smishing, vishing, and social media phishing).

Mobile Device Security & Device Updates
General End Users | 4:07 Video | 5 questions
DESCRIPTION
In this module, users will learn how to keep their mobile devices secure, the importance of reporting a lost or stolen device, and how regular updates protect a device.

Physical Security
General End Users | 3:35 Video | 5 questions
DESCRIPTION
In this module, users will learn about physical security, including tailgating, locking unattended devices, clean desks, and removable media. This module discusses why physical security is a cybersecurity issue.

Social Engineering
General End Users | 1:47 Video | 5 questions
DESCRIPTION
In this module, users will learn what social engineering is and how they can recognize when they're being manipulated.

Training Modules

Cybersecurity Tonight Quick Tips (1-2 min)

TRAINING STYLE

Cybersecurity Tonight Quick Tips feature the cast of Cybersecurity Tonight. Each guest, as well as host Andre Oliver and co-host Antonia Rivera, covers a unique cybersecurity concept. Quick Tips can be used to supplement the content of Cybersecurity Tonight or as independently-assigned modules.

HTTPS & Web Access

General End Users | 1:26 video | 3 questions

DESCRIPTION

In this module, users will learn why the "s" in "https" doesn't guarantee a website is safe.

Removable Media

General End Users | 1:01 Video | 3 questions

DESCRIPTION

In this module, users will learn about the dangers of removable media and why so many companies have policies against them.

Social Media Phishing

General End Users | 1:15 Video | 3 questions

DESCRIPTION

In this module, users will learn how cybercriminals use social media to carry out phishing attacks.

Spear-Phishing and Whaling

General End Users | 1:11 Video | 3 questions

DESCRIPTION

In this module, users will learn why having privileged access increases their risk of being targeted by phishing attacks.

Stolen Passwords

General End Users | 1:20 Video | 3 questions

DESCRIPTION

In this module, users will learn what happens to their passwords when cybercriminals get a hold of them and why it's so important to use a unique password for every account.

Themed Phishing

General End Users | 1:07 Video | 3 questions

DESCRIPTION

In this module, users will learn how cybercriminals use topical or otherwise engaging themes to get their attention.

Training Modules

LS Talk: Executives

(4-5 min)

TRAILER HERE.

TRAINING STYLE

Six expert speakers share what they've learned about cybersecurity as high-level leaders in powerful organizations.

Executive Assistants

Executive Assistants | 4:11 Video | 5 questions

DESCRIPTION

Executive assistants will learn why they are common targets for cyber attacks and why they have an elevated responsibility to be cybersecure.

Executives, the Ultimate Target

Executives | 4:07 Video | 5 questions

DESCRIPTION

Executives will understand why they are valuable targets to cybercriminals and what they can do to strengthen their organization's cybersecurity culture.

Incidents & Preparing for Breach for Executives

Executives | 4:08 Video | 5 questions

DESCRIPTION

Executives will learn the difference between an incident and a breach, the repercussions of a data breach, and the importance of having an incident response plan.

Privacy for Executives

Executives | 5:51 Video | 5 questions

DESCRIPTION

Executives will explore how to protect their privacy while being the most visible members of their organization.

Threat Landscape & Common Attacks for Executives

Executives | 4:13 Video | 5 questions

DESCRIPTION

Executives will learn the most common ways they are targeted by cybercriminals and how to defend against these attacks.

Working Outside of the Office for Executives

Executives | 4:48 Video | 5 questions

DESCRIPTION

Executives will learn the unique risks of working remotely, whether at home or while traveling.

Training Modules

The Cyber Race (3-6 min)

TRAILER HERE.

TRAINING STYLE

With $1 million in crypto on the line, teams of two put their cybersecurity knowledge to the test in a race around the world. This is...The Cyber Race. The Cyber Race consists of one foundational module introducing the concept of digital identity and four modules covering specific aspects of digital identity in more detail.

This content is also available on the CyberEscape Online Platform.

Protecting Your Digital Identity

General End Users | 3:20 Video | 5 questions

DESCRIPTION

In this module, users will learn what their digital identity is and how it crosses over into the real world.

Note: This module acts as an introduction and should be assigned first if assigning multiple modules.

Cryptocurrency & NFTs

General End Users | 5:04 Video | 5 questions

DESCRIPTION

In this module, users will learn about digital assets such as cryptocurrency and NFTs, including risks, related scams, basic security, and the role of the blockchain.

Deep Fakes

General End Users | 3:50 Video | 5 questions

DESCRIPTION

In this module, users will learn what deep fakes are, how they're made, and how they can be debunked.

Security in the Metaverse

General End Users | 6:07 Video | 5 questions

DESCRIPTION

In this module, users will learn about the rising cybersecurity concerns experts are discussing as the metaverse develops.

Protecting Your Crypto Wallet

General End Users | 5:52 Video | 5 questions

DESCRIPTION

In this module, users will about the different types of crypto wallets and how to secure their digital assets.

Training Modules

Investigate: Insider Threat

General End Users | 6:20 Video | 5 questions
TRAILER HERE.

DESCRIPTION
In the aftermath of a data breach caused by a disgruntled employee, a member of the security team tries to piece together the whole story. What exactly caused an employee so well-liked by both his manager and his teammates to become an insider threat?

90 Seconds: Cybercare

Healthcare Professionals | 2:18 Video | 3 questions

DESCRIPTION
This two-minute mockumentary shows end users in the healthcare industry the importance of reporting suspicious activity. It also demonstrates the dangers of removable devices such as USB drives.

Training Modules

Security Snaps (:30-1 min)

TRAINING STYLE

These short remediatory videos cover specific actions taken by end users.

This content is also available as downloadable MP4s on the Training Platform.

Clean Desk Policy

General End Users | 0:28 Video

DESCRIPTION

Turns out cleaning up a messy desk isn't just a chore...it's also company policy! Sensitive info is more likely to accidentally be left out on a cluttered desk, so it's important to stay organized.

Complete Your Security Training

General End Users | 0:29 Video

DESCRIPTION

Someone got a little behind on their assigned security training, but today they found the time to get caught up. Not only are they more secure at both work and home, they also can't wait to share their new knowledge with loved ones to keep them safe, too!

Complete Your Security Training (II)

General End Users | 0:39 Video

DESCRIPTION

Someone failed their security training today. When they retake it, they'll be paying full attention to the module - no distractions!

Credentials Online

General End Users | 0:53 Video

DESCRIPTION

You'd be shocked at what you can find on the internet...If you use the same password across all your accounts, it's pretty likely a data breach has caused it to be available on the dark web. Set some time aside today to give all of your accounts unique passwords!

Deleting Data in Bulk

General End Users | 0:43 Video

DESCRIPTION

A bulk deletion of data raised some red flags. Luckily there was no malicious activity - just a great opportunity to learn more about our organization's data management policies!

Downloading Data in Bulk

General End Users | 0:41 Video

DESCRIPTION

A member of the circle has some advice for you. Before you go downloading data in bulk, make sure you're up to date on our organization's policies on data downloads and backups.

Identity Provider

General End Users | 0:36 Video

DESCRIPTION

Someone was alerted to suspicious activity on their IDP account. Seems it's time to contact the security team!

Least Privilege Data Access

General End Users | 0:33 Video

DESCRIPTION

An intern's account was flagged for suspicious data access. Luckily he was just a little too curious, and it was a great opportunity to learn more about our company policy!

Security Snaps (cont'd)

Least Privilege Data Sharing
General End Users | 0:40 Video
DESCRIPTION
Sharing data with someone who isn't authorized can be an easy mistake, but it can lead to big consequences! Be sure to double-check that the person you're sharing data with is authorized to handle it.

Malware
General End Users | 0:42 Video
DESCRIPTION
Someone's computer is acting a little strange....It could be malware, so they'll be reaching out to the security team for help!

Multifactor Authentication (MFA) Updates
General End Users | 0:46 Video
DESCRIPTION
Someone got a new phone, and it's making logging into their account a bit tough. If you run into trouble with your multifactor authentication, reach out for help!

Password Manager
General End Users | 0:29 Video
DESCRIPTION
The company password manager is causing quite the buzz...If you haven't downloaded it yet, be sure to do so today so you can remain in line with our organization's security practices!

Password Manager (II)
General End Users | 0:37 Video
DESCRIPTION
For some, using a password manager takes a little getting used to...but before you know it you might be wondering how you ever lived without one!

Password Manager (III)
General End Users | 0:34 Video
DESCRIPTION
Forgetting your passwords all the time can be really frustrating...but a password manager can save the day! If you're not using the company password

Phishing
General End Users | 0:36 Video
DESCRIPTION
Looks like someone's having a bad day... Remember to slow down when catching up on unread emails and closely scrutinize links before you click them. If you're unsure if the link is trustworthy, you can find the website you're attempting to visit using a search engine!

Phishing (II)
General End Users | 0:44 Video
DESCRIPTION
The security filters may have caught it before delivery, but a targeted phishing email has left someone a little shaken up. If you have access to sensitive data, stay vigilant and don't over-rely on security software!

Phish Clicked
General End Users | 0:44 Video
DESCRIPTION
Unfortunately, someone was fooled by a phishing email. Keep on the lookout for red flags, and don't assume all phish will be obvious to identify!

Phish Clicked Multiple Times
General End Users | 0:44 Video
DESCRIPTION
Though it may have seemed intimidating at first, someone's chat with their manager about their repeated phishing clicks turned out to be very helpful. In fact, they wish they'd asked their manager for help sooner!

Phish Landing Pages
General End Users | 0:28 Video
DESCRIPTION
Someone's had their first encounter with a phishing landing page. They can look pretty convincing, so be sure to double-check website URLs before entering sensitive data or opening links/files!

Security Snaps (cont'd)

Phish Opened
General End Users | 0:33 Video
DESCRIPTION
Someone opened a phishing email! Luckily they realized it was a phish before it was too late, but it was a good reminder to stay vigilant.

Phish Opened (Simulation)
General End Users | 0:29 Video
DESCRIPTION
Luckily no harm was done, but someone opened an attachment from a phishing email. It's best to avoid opening attachments you weren't expecting to receive!

Protecting Personal Information
General End Users | 0:45 Video
DESCRIPTION
Apparently personal data is bought and sold on the dark web. Be careful what personal information you choose to share online!

Safe Surfing on Company Devices
General End Users | 0:34 Video
DESCRIPTION
Surfing the web can be fun, but it can also be risky! Be careful what sites you visit, and use your work devices for work-related activities only.

Safe Surfing on Company Devices (II)
General End Users | 0:32 Video
DESCRIPTION
Someone's learned the hard way that security software is helpful but not invincible. When using the internet on a work device, don't assume that malicious websites will be blocked. Be careful which webpages you choose to visit!

Safe Surfing on Company Devices (III)
General End Users | 0:33 Video
DESCRIPTION
Someone had a chat with their manager about their frequent website access warnings. Frequent access warnings can be a sign of risky behavior, so be sure you're surfing the web safely!

Sensitive Information Online
General End Users | 0:31 Video
DESCRIPTION
Not all data should be uploaded to the internet. Do you know what company policy has to say about that?

Sharing Passwords
General End Users | 0:34 Video
DESCRIPTION
Someone's learned the hard way the risks of sharing a password, even with people that are trustworthy. Keep those passwords top secret!

Single Sign-On (SSO) Troubles
General End Users | 0:37 Video
DESCRIPTION
Someone's having trouble with their single sign-on account, but they're looking forward to the convenience it offers once they can log in. If you're having issues with your SSO, reach out to the security team for assistance!

Security Snaps (cont'd)

Smishing (SMS Phishing)

General End Users | 0:36 Video

DESCRIPTION

Apparently phishing attacks aren't just sent to people's email inboxes; they can be delivered over text message, too! Look out for red flags and avoid unexpected links and attachments in your text messages, just like you do your emails.

Strong Passwords & Passphrases

General End Users | 0:37 Video

DESCRIPTION

Someone thought they were unlucky...but in reality they were using really weak passwords. Passwords that are long, utilize numbers and special characters, and avoid cliches are harder to crack.

Threat Protection Basics

General End Users | 0:39 Video

DESCRIPTION

Apparently malicious data was found on someone's computer. The security team was able to help, and they had some helpful tips for staying safe in the future!

Updating Passwords

General End Users | 0:32 Video

DESCRIPTION

Someone learned something interesting today and wants to share. Apparently, updating your account credentials periodically can help keep your accounts secure!

Updating Data in Bulk

General End Users | 0:51 Video

DESCRIPTION

A mass data upload raised some questions, but it was a great learning moment! Reach out to your manager if you're unfamiliar with our organization's data management policies.

Training Modules

Security Snaps Celebrations (:15-1 min)

TRAINING STYLE

These short, congratulatory videos recognize end users for vigilant actions and emphasize how their behavior is keeping them secure. Alternative versions with celebratory GIFs rather than training videos are also available.

This content is also available as downloadable MP4s on the Training Platform.

Browser Update

General End Users | 0:23 Video

DESCRIPTION

Great work updating your browser! It's easy to snooze update reminders forever, but you know better. Now you're surfing the web more securely than ever! Let's celebrate!

Completed Security Training

General End Users | 0:15 Video

DESCRIPTION

Nice job completing your security training! Now you're all the more prepared to defend our organization - and yourself - from cybercrime. That's certainly worth celebrating, don't you think?

Multifactor Authentication (MFA)

General End Users | 0:20 Video

DESCRIPTION

Looks like someone is using multifactor authentication to protect their accounts...and that someone is you! This calls for some celebration. Great job!

Operating System Update

General End Users | 0:23 Video

DESCRIPTION

You recently updated your operating system! Great work! Now you're defending against the most recently discovered cyber threats. Let's take a second to celebrate your awesome cybersecurity skills!

Password Manager

General End Users | 0:27 Video

DESCRIPTION

You're staying at the top of your security game by utilizing our organization's password manager! Awesome job! Let's take a second to celebrate all that extra security and convenience - and you for being a cybersecurity superstar.

Reported Phish (Simulation)

General End Users | 0:20 Video

DESCRIPTION

You recently reported a simulated phishing email to the security team. Nice job...now let's take a second to celebrate your cybersecurity know-how!

Reported Phish

General End Users | 0:22 Video

DESCRIPTION

The security team recently got a report of suspected phishing from a cybersecurity rockstar...you! Great work. Let's take a moment to celebrate your top-tier phishing skills.

Reset Credentials

General End Users | 0:24 Video

DESCRIPTION

Looks like you recently reset your credentials! Nice job staying secure with cybersecurity best practices. Keep up the good work!

Training Modules

Cyber Socials (<:30 sec)

TRAINING STYLE

These short, remediatory videos cover specific actions taken by end users.

This content is also available as downloadable MP4s on the Training Platform.

Location Sharing

General End Users | 0:10 Video

DESCRIPTION

Tagging your location on social media without asking everyone else included in the post? Think again!

Multifactor Authentication (MFA)

General End Users | 0:11 Video

DESCRIPTION

Enabling multifactor authentication (MFA) keeps you smooth and the hackers guessing.

Secure Device

General End Users | 0:11 Video

DESCRIPTION

Want to be popular in the workspace? Lock your devices when they're not in use.

Reporting Phish

General End Users | 0:11 Video

DESCRIPTION

Smash that report button when you spot a phish!

Training Modules

Security Made Simple
(1-2 min)

TRAILER HERE.

TRAINING STYLE
For the end users starting at square one, jumping into the deep end of cybersecurity training can be overwhelming. Help them get their feet wet first with these awareness-oriented, introductory training modules.

Alternative Forms of Phishing
General End Users | 1:15 Video | 3 questions
DESCRIPTION
Introduce users to the basics of alternative forms of phishing.

Cybersecurity for the Family
General End Users | 1:07 Video | 3 questions
DESCRIPTION
Introduce users to the importance of discussing security with their children.

Data Classification
General End Users | 1:29 Video | 3 questions
DESCRIPTION
Introduce users to the basics of data classification.

Email Compromise
General End Users | 1:13 Video | 3 questions
DESCRIPTION
Introduce users to the basics of business and vendor email compromise.

Insider Threat Behavior
General End Users | 1:08 Video | 3 questions
DESCRIPTION
Teach end users early warning signs of insider threats so they can be reported before damage is done.

Least Privilege
General End Users | 0:57 Video | 3 questions
DESCRIPTION
Introduce users to the basics of the principle of least privilege.

Malware
General End Users | 1:27 Video | 3 questions
DESCRIPTION
Introduce users to the basics of malware.

MFA Fatigue
General End Users | 1:05 Video | 3 questions
DESCRIPTION
Introduce users to the basics of MFA fatigue attacks.

Multifactor Authentication (MFA)
General End Users | 1:01 Video | 3 questions
DESCRIPTION
Introduce users to the basics of multifactor authentication.

Oversharing on Social Media
General End Users | 1:01 Video | 3 questions
DESCRIPTION
Introduce users to the dangers of sharing too much personal information on social media.

Training Modules

Security Made Simple (cont'd)

Password Best Practices
General End Users | 1:15 Video | 3 questions
DESCRIPTION
Introduce users to the basics of strong passwords.

Password Manager
General End Users | 0:59 Video | 3 questions
DESCRIPTION
Introduce users to the basics of password managers.

Phishing
General End Users | 1:01 Video | 3 questions
DESCRIPTION
Introduce users to the basics of phishing.

Ransomware
General End Users | 1:16 Video | 3 questions
DESCRIPTION
Introduce users to the basics of ransomware.

Removable Media
General End Users | 0:53 Video | 3 questions
DESCRIPTION
Introduce users to the risks presented by removable media.

Reusing Passwords
General End Users | 1:08 Video | 3 questions
DESCRIPTION
Introduce users to the importance of using a unique password for every one of their accounts.

Security Culture for People Managers
General End Users | 1:13 Video | 3 questions
DESCRIPTION
Help users understand the responsibility they hold to create a strong cybersecurity culture within the teams they manage.

Social Engineering
General End Users | 1:12 Video | 3 questions
DESCRIPTION
Introduce users to the basics of social engineering.

Targeted Phishing
General End Users | 0:56 Video | 3 questions
DESCRIPTION
Introduce users to the basics of targeted phishing attacks, including spearphishing and whaling.

Travel Security
General End Users | 1:04 Video | 3 questions
DESCRIPTION
Introduce users to the basics of travel security.

Unapproved Software
General End Users | 1:05 Video | 3 questions
DESCRIPTION
Introduce users to the risks of downloading unapproved software.

Updates
General End Users | 1:03 Video | 3 questions
DESCRIPTION
Help end users understand why updating their devices and software is so important.

Virtual Private Networks
General End Users | 0:59 Video | 3 questions
DESCRIPTION
Introduce users to the basics of virtual private networks.

Why Security Matters
General End Users | 1:16 Video | 3 questions
DESCRIPTION
Help end users understand the personal responsibility they hold to contribute to your organization's security culture.

Wi-Fi Security
General End Users | 1:17 Video | 3 questions
DESCRIPTION
Introduce users to the basics of Wi-Fi security.

Working from Home
General End Users | 1:10 Video | 3 questions
DESCRIPTION
Introduce users to the basics of staying secure while working from home.

Training Modules

Born Secure: Quick Tips (:30-1 min)

TRAINING STYLE

The characters of Born Secure: Webb of Lies are back with some quick tips for staying cybersecure!

AI Chatbots

General End Users | 0:49 Video | 3 questions

DESCRIPTION

Introduce end users to the basics of phony AI chatbots owned by threat actors.

AI Privacy

General End Users | 0:51 Video | 3 questions

DESCRIPTION

Introduce end users to the basics of protecting their privacy while using AI chatbots.

QR Code Security

General End Users | 0:42 Video | 3 questions

DESCRIPTION

Introduce end users to the basics of malicious QR codes.

Reporting Suspicious Activity

General End Users | 0:39 Video | 3 questions

DESCRIPTION

Introduce end users to the importance of reporting suspicious activity.

Saving Passwords to Your Browser

General End Users | 0:41 Video | 3 questions

DESCRIPTION

Introduce end users to the use of URL shorteners to disguise malicious links.

Staying Safe Online

General End Users | 1:01 Video | 3 questions

DESCRIPTION

Introduce end users to the basics of staying safe while surfing the web, including avoiding online downloads, staying vigilant, and looking out for misinformation.

URL Shorteners

General End Users | 0:47 Video | 3 questions

DESCRIPTION

Introduce end users to the use of URL shorteners to disguise malicious links.

Work Devices vs Personal Devices

General End Users | 0:35 Video | 3 questions

DESCRIPTION

Introduce end users to the importance of keeping work data off of their personal devices.

Training Modules

Legacy Code Quick Tips(1-2 min)

TRAINING STYLE

Legacy Code Quick Tips feature the cast of Legacy Code. Each character covers a behind-the-scenes cybersecurity concept. Quick Tips can be used to supplement the content of Legacy Code or as independently-assigned modules.

AI & Misinformation

General End Users | 0:56 Video | 3 questions

DESCRIPTION

Artificial intelligence can be super useful, but it can also lead to the spread of misinformation. Let's take a look at what to do if something you find online is less than credible!

AI Regulation & Policy Change

General End Users | 0:49 Video | 3 questions

DESCRIPTION

Artificial intelligence is evolving quickly, which means policy changes may occur more frequently than you're used to. Don't forget to stay up-to-date with your company's current AI policies!

Deepfake Detection Techniques

General End Users | 1:16 Video | 3 questions

DESCRIPTION

With the rise of deepfake technology, how do you know if what you're seeing is real? Let's explore how to identify a deepfake!

Multifactor Authentication (MFA) Push Notifications

General End Users | 1:01 Video | 3 questions

DESCRIPTION

Multifactor authentication is a great way to add extra security to your accounts, but what do you do if you receive an authentication request you weren't responsible for? Let's find out!

Privileged Access

General End Users | 1:04 Video | 3 questions

DESCRIPTION

Your access to sensitive data is a big responsibility! Let's take a look at how you can fulfill that responsibility by following security best practices.

Safe Word Strategy for Family Cybersecurity

General End Users |):54 Video | 3 questions

DESCRIPTION

Unfortunately, threat actors may use real or fake emergencies to lower your guard. Help your family stay safe from cyber threats during an emergency with the safeword strategy!

Work Emails and Private Accounts

General End Users | 1:01 Video | 3 questions

DESCRIPTION

Work email addresses shouldn't be used to open personal accounts, but why? Let's find out!

Working Remotely

General End Users | 1:16 Video | 3 questions

DESCRIPTION

Working remotely has its perks, but it presents some unique security challenges as well. Let's explore how to stay safe when working outside the office!

Training Modules

Defensive Design (3-5 min)

TRAINING STYLE

Defensive Design, tailored for technical employees from software engineers to IT professionals, offers an introductory approach to cybersecurity from an engineering & development viewpoint.

Application Portfolio Management

General End Users | 3:42 Video | 5 questions

DESCRIPTION

Discover how effective application portfolio management not only streamlines operations but crucially strengthens your organization's cybersecurity.

GRC (Governance, Risk, and Compliance) for Technical Employees

General End Users | 1:54 Video | 5 questions

DESCRIPTION

If you're not familiar with your organization's Governance, Risk, and Compliance policies, you may be putting your systems and your organization at risk.

Open Source Code

General End Users | 3:36 Video | 5 questions

DESCRIPTION

Open source libraries are a powerful tool, but they must be utilized properly. Otherwise, they become a security risk.

OWASP

General End Users | 2:24 Video | 5 questions

DESCRIPTION

The Open Worldwide Application Security Project, or OWASP, may be best known for their OWASP Top 10, but they offer a wide array of valuable tools and resources. Let's take a look at what you can find on their website.

Phishing for Technical Employees

General End Users | 2:37 Video | 5 questions

DESCRIPTION

Phishing attacks on technical employees are often more targeted than phishing attacks on other employees. Let's explore what to look out for so you can stay safe.

Social Engineering for Technical Employees

General End Users | 3:36 Video | 5 questions

DESCRIPTION

As a technical employee, you likely have stronger security habits than others at your organization. However, that's no reason to let your guard down. Cybercriminals may craft social engineering attacks that target you, specifically.

Threat Modeling

General End Users | 3:12 Video | 5 questions

DESCRIPTION

Dive into the world of threat modeling and learn how to enhance your application's security by identifying and mitigating risks through a strategic, attacker's perspective!

User Permissions & Access Management

General End Users | 3:10 Video | 5 questions

DESCRIPTION

Discover the power of managing user permissions to strengthen your organization's security and compliance.

Surveys & Assessments

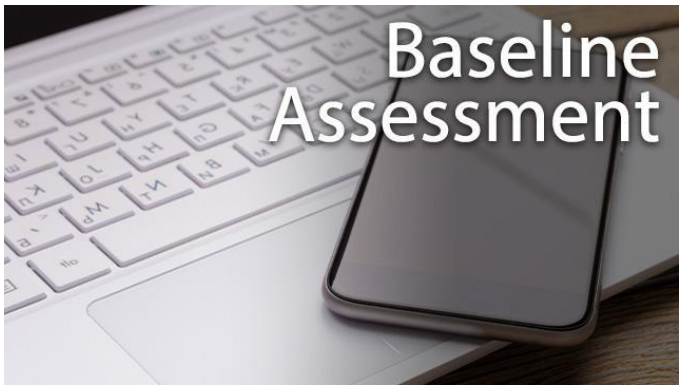
Authentication & Access Assessment

General End User | 10 Questions

DESCRIPTION

This assessment can be assigned at the beginning and end of training modules to gauge your team's understanding of key cybersecurity principles before and after training completion.

Baseline Assessments



General End User | 20 Questions

DESCRIPTION

This long-form survey is designed to accurately assess the cybersecurity knowledge of a group of general end users, both before and after participating in training.

Am I Secure? (101 & 102)

General End User | 20 Questions

DESCRIPTION

This long-form survey is designed to accurately assess the cybersecurity knowledge of a group of general end users, both before and after participating in training.

Culture Assessment

General End User | 10 Questions

DESCRIPTION

This survey measures perceived cultural dynamics (e.g. process-, compliance-, autonomy- or trust-oriented) and loosely maps end users to a security personality profile.

Surveys & Assessments

Data Security & Privacy Assessment

General End User | 10 Questions

DESCRIPTION

This assessment can be assigned before and after training modules to gauge your team's understanding of key cybersecurity principles before and after training completion.

Phishing & Social Engineering

General End User | 10 Questions

DESCRIPTION

This assessment can be assigned before and after training modules to gauge your team's understanding of key cybersecurity principles before and after training completion.

Device Security Assessment

General End User | 10 Questions

DESCRIPTION

This assessment can be assigned before and after training modules to gauge your team's understanding of key cybersecurity principles before and after training completion.

Security Policy Trivia

General End User | LS content catalog contains over 300 questions that can be leveraged in the Security Policy Trivia training module

DESCRIPTION

Multiple choice security trivia centering on the fundamentals!

Surveys & Assessments

Threat Insight (101 & 102)

General End User | 10 Questions

DESCRIPTION

This survey measures perceived risk perception of cyber threats and perceived susceptibility to phishing scams.

Web Security Assessment

General End User | 10 Questions

DESCRIPTION

This assessment can be assigned before and after training modules to gauge your team's understanding of key cybersecurity principles before and after training completion.

Puzzle Modules

Hotspot: WFH
General End Users | ~3 min
DESCRIPTION
Users will search and secure a physical environment by clicking on violations to fix them within the allotted time. They will learn to avoid the following common security mishaps: misinterpreting email legitimacy, reacting impulsively to scams, over-trusting security controls, oversharing on social media, mishandling devices, neglecting suspicious activity and surrendering to security fatigue.

Passwords Tips & Tricks
General End Users | ~1 min
DESCRIPTION
In this exercise, users will learn a few tricks to keep their passwords stronger and their accounts secure!

Emoji Pass
General End Users | ~1 min
DESCRIPTION
Users will solve cybersecurity riddles by piecing together creative passphrases. In the process users will learn what makes a strong, creative passphrases that will keep their accounts secure.

High Value Phishing Targets
General End Users | ~2 min
DESCRIPTION
Users will identify the individual who is most likely to be targeted with a phishing attack by a criminal nation or state. Users will better understand what makes someone a high-value target for phishing attacks—power, access, influence, and poor security hygiene.

Staying Safe Online
General End Users | ~5 min
DESCRIPTION
In this exercise, users will learn about ways to stay safe online like online privacy, how to safely make online purchases, how to save data, and more!

How Cybercriminals Trick Users
General End Users | ~5 min
DESCRIPTION
In this exercise, users learn how cybercriminals trick their victims, what red flags to watch out for, and how to defend against phish in real life.

Mobile Device Safety
General End Users | ~5 min
DESCRIPTION
This exercise measures your employee's security knowledge of mobile devices concerning features like MFA , passwords, data storage, and more!

Puzzle Modules

Catching the Big Phish

General End Users | ~2 min

DESCRIPTION

In this exercise, users will practice identifying phishing emails and what to look out for in real life.

This content is also available in Phishing IRL.

Flag Phishery

General End Users | ~3 min

DESCRIPTION

Users will examine emails and determine if they are real or phishing by clicking on the areas they find suspicious. Users will learn to recognize phishing identifiers within emails, such as urgency, malicious links, malicious attachments, and spoofing.

Decoding the Ransomware Message

General End Users | ~5 min

DESCRIPTION

In this exercise, users will learn important messaging used in ransomware messages and what to watch out for when dealing with this threat.

Social Media Flags

General End Users | ~2 min

DESCRIPTION

Users will learn what tricks social engineers use in their social media schemes by identifying red flags in a social media message.

Phishing Email Flags

General End Users | ~2 min

DESCRIPTION

Users will learn what tricks social engineers use in their phishing email schemes by identifying red flags in a phishing email.

Secure Coding Basics

Developers & Other Technical Employees | ~5 min

DESCRIPTION

Users will refresh their knowledge of secure coding basics by identifying best practices.

Preventing Digital Identity Theft

General End Users | ~5 min

DESCRIPTION

Users will learn basic skills to keep their online identities safe from theft by identifying which of their fictional friends is most at-risk based on their cyber hygiene.

Identifying & Protecting PII

General End Users | ~5 min

DESCRIPTION

Users will determine what personal data should remain private and what is safe to share publicly.

Password Safety & Account Security

General End Users | ~4 min

DESCRIPTION

Users will learn what makes a password strong and how to best protect their online accounts by asking questions to discover which fictional friend has the riskiest password hygiene.

Cyber Criminal Mapping

General End Users | ~5 min

DESCRIPTION

In this exercise, users must determine the WHO, WHAT, HOW, and WHY of a cyber crime. They will then link the information together on an attack map.

This content is also available in Born Secure: Training Ground series.

Puzzle Modules

Spoil the Vish: Data Dojo

General End Users | ~3 min

DESCRIPTION

In this exercise, users play through multiple vishing calls and choose how to best respond. Users must deny the caller remote access to their computer and question the Vish on their identity to succeed.

This content is also available in Phishing: IRL series.

Go Vish

General End Users | ~3 min

DESCRIPTION

In this exercise, users will be playing the role of a social engineer extracting small pieces of information from multiple targets to expose the victim's financial information.

This content is also available in Born Secure: Entrance Exam series.

Device Security - Work vs Personal Puzzle

General End Users | ~3 min

DESCRIPTION

In this exercise, users will sort files into personal vs. work to help them understand what data should be kept on which devices.

This content is also available in Secure My Life in CyberEscape Online.

Bitcoin & Botnets

General End Users | ~5 min

DESCRIPTION

In this exercise, users will learn about bitcoin, botnets, and the risks associated with these concepts.

This content is also available in Secure My Life Now! on CyberEscape Online.

Physical Security During a Data Breach

General End Users | ~4 min

DESCRIPTION

In this exercise, users will learn about physical security best practices and protocols in the event of a data breach or data incident.

This content is also available in VTX War Room on CyberEscape Online.

Rings of Privacy

General End Users | ~5 min

DESCRIPTION

In this exercise, users will organize personally identifiable information (PII) to better understand what data needs to be protected.

This content is also available in Cybersecurity Tonight on CyberEscape Online.

Detecting the Source of a Data Incident

General End Users | ~4 min

DESCRIPTION

In this exercise, users will be tasked with interviewing employees of an organization where a data incident occurred to find where the threat may have originated.

This content is also available in VTX War Room on CyberEscape Online.

What's Protected by HIPAA?

General End Users | ~4 min

DESCRIPTION

In this exercise, users will sort PHI and non-PHI information to better understand what is protected under HIPAA policies.

This content is also available in Healthcare Cyber Check-Up on CyberEscape Online.

Puzzle Modules

Phishing for PHI

General End Users | ~4 min

DESCRIPTION

In this exercise, users will practice identifying red flags in phishing emails and what to look out for in real life

This content is also available in Healthcare Cyber Check-Up on CyberEscape Online.

Password Protecting PHI

General End Users | ~4 min

DESCRIPTION

In this exercise, users will learn good password management practices to keep their accounts secure!

This content is also available in Healthcare Cyber Check-Up on CyberEscape Online.

Emoji Passphrase Decoder Puzzle

General End Users | ~4 min

DESCRIPTION

This exercise helps users brainstorm unique passphrases that will help keep their accounts secure.

This content is also available in Born Secure: Entrance Exam series.

Panicking Pal: Ransomware

General End Users | ~4 min

DESCRIPTION

In this exercise, users will engage in a simulated phone call with a friend who has been infected with ransomware and talk about the possible next steps in order to deal with the threat.

This content is also available in Cybersecurity Tonight on CyberEscape Online.

Phishing from a Cybercriminal's Perspective

General End Users | ~4 min

DESCRIPTION

In this exercise users will phish for information in two emails; one demonstrates how cybercriminals gather data and the other puts that data to use.

This content is also available in Cybersecurity Tonight on CyberEscape Online.

Correct the Security Violations

General End Users | ~3 min

DESCRIPTION

In this exercise, users will practice identifying physical security threats in the workplace.

This content is also available in Born Secure: Entrance Exam series.

Sorting and Protecting PII Puzzle

General End Users | ~4 min

DESCRIPTION

In this exercise, users will practice identifying PII.

This content is also available in Born Secure: Entrance Exam series.

The Weakest Link

General End Users | ~4 min

DESCRIPTION

This exercise introduces users to basic good cyber hygiene practices that will protect them at work and at home.

This content is also available in Born Secure: Entrance Exam series.

Building Business Email Compromise

General End Users | ~4 min

DESCRIPTION

In this exercise, users will be impersonating cybercriminals phishing for financial gain using Business Email Compromise. Users will learn what red flags to watch out for in real life and the importance of verification.

This content is also available in Born Secure: Entrance Exam series.

Campaign in a Box

Program Communications Made Easy

Each box contains 4 weeks worth of blogs, chat messages, and emails surrounding a key cybersecurity concept. Your end users will love this witty, attention-grabbing content. Program owners are encouraged to edit and/or customize Campaign in a Box content to suit their program.

SAMPLE BOX HERE.

1 blog | 4 emails | 4 chat messages
May include phishing simulation emails and/or infographics.
Boxes can be found in the Support Garden.

- **Cybersecurity at Home**
- **Digital Identity**
- **Family First**
- **GDPR**
- **Generative AI**
- **Governance & Compliance**
- **Historical Breaches**
- **Holiday Fraud**
- **Holiday Scams**
- **Internet of Things (IoT) & Online Shopping**
- **Malware***
- **Mobile Security***
- **Passwords***
- **Phishing***
- **Privacy**
- **Ransomware**
- **Secure Browsing & Incident Reporting**
- **Social Engineering***
- **Social Media Security**
- **State of the Scam**
- **Staying Safe from Identity Theft Online**
- **Travel Safety**
- **The Dark Web**
- **Updates**

* - Multiple Campaign in a Boxes available on this topic.

Campaign in a Box

Mini Boxes

Program Communications Made Easy
The Mini Box is designed to supplement your program's monthly Campaign in a Box.

Note: News-related and other time sensitive mini boxes are not listed in the content catalog

1 email | 1-2 chat messages
Mini boxes can be found in the support garden

- Cookies & Data Collection
- Cybercrime as a Service
- Cybersecurity & Customer Support
- Cybersecurity & HR
- Cybersecurity & IT
- Cybersecurity & Finance
- Cybersecurity & Marketing
- Cybersecurity & Sales
- Cybersecurity for Executives
- Cybersecurity is Everyone's Responsibility
- Encryption
- Family First: Cybersecurity is a Family Activity
- Insider Threats
- International Fraud Awareness Week
- Internet Safety
- Location Sharing
- Our Best Defense
- Passwordless Authentication
- Patching
- Physical Security
- Privileged Users
- Putting the 'U' in Cybersecurity
- Romance Scams
- Safe Surfing for the Family
- Sharing Security with Family
- SIM Swapping
- Smishing
- Student Debt Relief Scams
- Tax Day
- Web 3.0
- Wire Fraud
- & More

Content by Category

AUTHENTICATION & ACCESS

- Campaign in a Box: Passwords
- Mini Box: Passwordless Authentication
- Mini Box: Privileged Users
- Mini Box: SIM Swapping
- T.G.I.S.
- True Eye
- Born Secure: Training Grounds
- Born Secure: Webb of Lies
- Secure My Life
- Cybersecurity Tonight
- Big Ideas: Password Management
- Born Secure Quick Tips: Saving Passwords to Your Browser
- Security Basics: MFA
- Security Basics: Password Managers
- Security Basics: Reusing Passwords
- Security Basics: Sharing Passwords
- Case in Point: Password Reuse
- Secure Coding: Authentication and Authorization
- Cyber Kitchen: Mobile Security
- Cyber Kitchen: Passwords & Authentication
- Vantage Point: Creating Strong Passphrases
- Cybersecurity Tonight: Passwords & Authentication
- Cybersecurity Tonight Quick Tips: Stolen Passwords
- Hotspot: WFH *(Puzzle Module)*
- Passwords Tips & Tricks *(Puzzle Module)*
- Emoji Pass *(Puzzle Module)*
- Mobile Device Safety (Puzzle Module)
- Password Safety & Account Security *(Puzzle Module)*
- Critical Mass *(CyberEscape Online)*
- Born Secure: Entrance Exam *(CyberEscape Online)*
- Healthcare Cyber Checkup *(CyberEscape Online)*
- Security Snap: Credentials Online
- Security Snap: Password Managers

DATA SECURITY & PRIVACY

- Campaign in a Box: Privacy
- Mini Box: Cookies & Data Collection

DATA SECURITY & PRIVACY (cont'd)

- Mini Box: Encryption
- True Eye
- The Squad
- Secure My Life
- Born Secure: Webb of Lies
- Day in the Life
- Big Ideas: Data Classification
- Big Ideas: General Cybersecurity
- Big Ideas: PII
- Big Ideas: Privacy
- Born Secure Quick Tips: AI Privacy
- Born Secure Quick Tips: AI Chatbots
- Security Basics: Data Classification
- Security Basics: Encryption
- Security Basics: Insider Threat
- Compliance Basics: PII
- Case in Point: Cloud Security Threats
- Case in Point: Mobile Security
- Case in Point: Point of Sale (PoS) Security
- Case in Point: Synthetic Identity Theft
- Secure Coding: Least Privilege
- Secure Coding: Source Code Secrets
- Cyber Kitchen: Cloud Security
- Cyber Kitchen: Mobile Security
- Brick Wall: Data Privacy
- LS Talk: Executive Assistants
- LS Talk: Executives, the Ultimate Target
- LS Talk: Privacy for Executives
- LS Talk: Working Outside the Office for Executives
- The Cyber Race: Protecting Your Digital Identity
- The Cyber Race: Cryptocurrency & NFTs
- The Cyber Race: Deep Fakes
- The Cyber Race: Security in the Metaverse
- The Cyber Race: Protecting Your Crypto Wallet
- Mobile Device Safety (Puzzle Module)
- Identifying & Protecting PII *(Puzzle Module)*
- Critical Mass *(CyberEscape Online)*
- Healthcare Cyber Checkup *(CyberEscape Online)*
- Secure My Life Now! *(CyberEscape Online)*
- War Room *(Virtual Tabletop Experience)*

See also: *different ways to view content.*

Content by Category

DEVICE SECURITY

- Campaign in a Box: Internet of Things
- Campaign in a Box: Malware
- Campaign in a Box: Mobile Security
- Campaign in a Box: Ransomware
- Campaign in a Box: Secure Browsing & Incident Reporting
- Campaign in a Box: Updates
- Mini Box: SIM Swapping
- True Eye
- Born Secure: Training Grounds
- Secure My Life
- Born Secure: Webb of Lies
- Cybersecurity Tonight
- Day in the Life
- Big Ideas: General Cybersecurity
- Born Secure Quick Tips: Work Devices vs Personal Devices
- Security Basics: Device Security
- Security Basics: Internet of Things (IoT)
- Security Basics: Malware
- Security Basics: Mobile Security
- Security Basics: Remote Work
- Security Basics: Secure Your Apps
- Security Basics: Shadow IT
- Case in Point: Internet of Things (IoT)
- Case in Point: Mobile Security
- Case in Point: Point of Sale (PoS) Security
- Case in Point: Ransomware
- Case in Point: Work From Home (WFH)
- Secure My Life Quick Tips: Home Wi-Fi
- Secure My Life Quick Tips: Updates
- Cyber Kitchen: Mobile Security
- Cyber Kitchen: Ransomware
- Cybersecurity Tonight: Malware & Ransomware
- Cybersecurity Tonight: Mobile Device Security & Device Updates
- Cybersecurity Tonight Quick Tips: Removable Media
- LS Talk: Working Outside the Office for Executives
- Hotspot: WFH *(Puzzle Module)*
- Mobile Device Safety (Puzzle Module)

DEVICE SECURITY (cont'd)

- Decoding the Ransomware Message *(Puzzle Module)*
- **Critical Mass** *(CyberEscape Online)*
- **Secure My Life Now!** *(CyberEscape Online)*
- **War Room** *(Virtual Tabletop Experience)*

PHISHING & SOCIAL ENGINEERING

- Campaign in a Box: Holiday Fraud
- Campaign in a Box: Holiday Scams
- Campaign in a Box: Phishing
- Campaign in a Box: Social Engineering
- Campaign in a Box: State of the Scam
- Mini Box: Romance Scams
- Mini Box: Smishing
- T.G.I.S.
- Phishing IRL
- The Squad
- Born Secure: Training Grounds
- Born Secure: Webb of Lies
- Secure My Life
- Cybersecurity Tonight
- Day in the Life
- Big Ideas: Phishing
- Big Ideas: Vishing
- Born Secure Quick Tips: QR Code Security
- Born Secure Quick Tips: URL Shorteners
- Security Basics: Phishing
- Security Basics: Smishing
- Security Basics: Spear-Phishing
- Security Basics: Vishing
- Security Basics: Whaling
- Case in Point: Advanced Financial Social Engineering
- Case in Point: Themed Phishing
- Case in Point: Vendor Email Compromise (VEC)
- Cyber Kitchen: Phishing
- Cyber Kitchen: Social Engineering
- Vantage Point: Alternative Forms of Phishing
- Vantage Point: Gift Card Scams
- Vantage Point: Pretexting

See also: *different ways to view content.*

Content by Category

PHISHING & SOCIAL ENGINEERING (cont'd)

- Cybersecurity Tonight: Phishing
- Cybersecurity Tonight: Social Engineering
- LS Talk: Executive Assistants
- LS Talk: Executives, the Ultimate Target
- Hotspot: WFH *(Puzzle Module)*
- High-Value Phishing *(Puzzle Module)*
- How Cybercriminals Trick Users *(Puzzle Module)*
- Craft-a-Phish *(Puzzle Module)*
- Flag Phishery *(Puzzle Module)*
- Social Media Flags *(Puzzle Module)*
- Phishing Email Flags (Puzzle Module)
- Preventing Digital Identity Theft *(Puzzle Module)*
- Critical Mass *(CyberEscape Online)*
- Born Secure: Entrance Exam *(CyberEscape Online)*
- Healthcare Cyber Checkup *(CyberEscape Online)*
- Secure My Life Now! *(CyberEscape Online)*
- Security Snap: Phishing

PHYSICAL SECURITY

- Campaign in a Box: Travel Safety
- Mini Box: Physical Security
- True Eye
- Born Secure: Training Grounds
- Born Secure: Webb of Lies
- Secure My Life
- Cybersecurity Tonight
- Day in the Life
- Big Ideas: General Cybersecurity
- Security Basics: Physical Security
- Security Basics: Remote Work
- Security Basics: Tailgating
- Case in Point: Physical Security
- Case in Point: Point of Sale (PoS) Security
- Case in Point: Travel Secure
- Cyber Kitchen: Mobile Security
- Vantage Point: Lock Your Computer
- Cybersecurity Tonight: Physical Security
- LS Talk: Working Outside the Office for Executives
- Born Secure: Entrance Exam (CyberEscape Online)

PHYSICAL SECURITY (cont'd)

- Healthcare Cyber Checkup (CyberEscape Online)

POLICY & COMPLIANCE

- Campaign in a Box: Governance & Compliance
- The Squad
- Security Basics: Policy Violations
- Security Basics: Shadow IT
- Compliance Basics: CCPA
- Compliance Basics: Data Privacy
- Compliance Basics: GDPR
- Compliance Basics: HIPAA
- Compliance Basics: PCI
- Compliance Basics: PHI
- Compliance Basics: PII
- Compliance Basics: PIPEDA
- Brick Wall: CCPA
- Brick Wall: Data Privacy
- Brick Wall: GDPR Compliance
- Cybersecurity Tonight Quick Tips: Removable Media
- LS Talk: Incidents & Preparing for Breach for Executives
- Healthcare Cyber Checkup *(CyberEscape Online)*
- War Room *(Virtual Tabletop Experience)*

REPORTING & PERSONAL RESPONSIBILITY

- Campaign in a Box: Secure Browsing & Incident Reporting
- Mini Box: Cybersecurity is Everyone's Responsibility
- Mini Box: Our Best Defense
- Mini Box: Putting the "U" in Cybersecurity
- T.G.I.S.
- The Squad
- Secure My Life
- Cybersecurity Tonight
- Day in the Life
- Big Ideas: General Cybersecurity

See also: *different ways to view content.*

Content by Category

REPORTING & PERSONAL RESPONSIBILITY (cont'd)

- Born Secure Quick Tips: Reporting Suspicious Activity
- Why? Customer Support
- Why? Executive Assistant
- Why? Finance
- Why? Help Desk
- Why? HR
- Why? Marketing
- Why? Sales
- Why? Vendor/Supply Chain
- Why? Service Desk
- Case in Point: Reporting Suspicious Activity
- Secure Coding: Introduction
- Cyber Kitchen: Take Ownership: Cybersecurity is Everyone's Responsibility
- Cybersecurity Tonight: Cybersecurity is Part of Your Job
- Investigate: Insider Threat
- LS Talk: Executive Assistants
- LS Talk: Executives, the Ultimate Target
- LS Talk: Incidents & Preparing for Breach for Executives
- Hotspot: WFH *(Puzzle Module)*
- Born Secure: Entrance Exam *(CyberEscape Online)*
- Secure My Life Now! *(CyberEscape Online)*
- War Room *(Virtual Tabletop Experience)*

WEB SECURITY

- Campaign in a Box: Internet of Things
- Campaign in a Box: Mobile Security
- Campaign in a Box: Social Media Security
- Mini Box: Internet Safety
- Mini Box: Location Sharing
- Mini Box: Safe Surfing for the Family
- Mini Box: Web 3.0
- T.G.I.S.
- True Eye
- The Squad
- Secure My Life
- Born Secure: Webb of Lies
- Born Secure Quick Tips: AI Privacy
- Born Secure Quick Tips: AI Chatbots
- Born Secure Quick Tips: Saving Passwords to Your Browser

WEB SECURITY (cont'd)

- Born Secure Quick Tips: Staying Safe Online
- Born Secure Quick Tips: URL Shorteners
- Case in Point: Safety Online
- Case in Point: Work From Home (WFH)
- Secure My Life Quick Tips: Social Media
- Cyber Kitchen: Cybersecurity at Home
- Cyber Kitchen: Phishing
- Vantage Point: Cyber Harassment for Public Figures
- Vantage Point: Cyber Harassment for Social Media Managers
- Vantage Point: Cyberbullying for Parents and Teens
- Cybersecurity Tonight Quick Tips: HTTPS & Web Access
- Cybersecurity Tonight Quick Tips: Social Media Phishing
- Cybersecurity Tonight Quick Tips: Spear-Phishing and Whaling
- Cybersecurity Tonight Quick Tips: Themed Phishing
- LS Talk: Privacy for Executives
- The Cyber Race: Protecting Your Digital Identity
- The Cyber Race: Cryptocurrency & NFTs
- The Cyber Race: Deep Fakes
- The Cyber Race: Security in the Metaverse
- The Cyber Race: Protecting Your Crypto Wallet
- Hotspot: WFH *(Puzzle Module)*
- Staying Safe Online *(Puzzle Module)*
- Social Media Flags (Puzzle Module)
- Secure My Life Now! *(CyberEscape Online)*

See also: *different ways to view content.*

Content by Audience

VERTICAL-BASED

EDUCATION
- Brick Wall: FERPA

RETAIL
- Born Secure: Entrance Exam (Retail) *(CyberEscape Online)*
- Case in Point: Point of Sale (PoS) Security

HEALTHCARE
- Compliance Basics: HIPPA
- Compliance Basics: PHI
- Healthcare Cyber Checkup *(CyberEscape Online)*
- Healthcare Cyber Checkup (Series)

DEPARTMENT-BASED

CUSTOMER SUPPORT
- Cybersecurity for Customer Support Professionals
- Day in the Life: Support Professionals
- Why? Customer Support

DEVELOPERS
- Cybersecurity for Developers

FINANCE
- Cybersecurity for Finance Professionals
- Day in the Life: Finance
- Why? Finance

HUMAN RESOURCES (HR)
- Cybersecurity for HR Professionals
- Day in the Life: HR
- Why? HR

INFORMATION TECHNOLOGY (IT)
- Campaign in a Box: Secure Coding
- Cybersecurity for IT Professionals
- Why? IT
- Secure Coding: Introduction
- Secure Coding: Authentication and Authorization
- Secure Coding: Injection
- Secure Coding: Least Privilege
- Secure Coding: OWASP Introduction
- Secure Coding: OWASP Update
- Secure Coding: Patching
- Secure Coding: Source Code Secrets
- Secure Coding: Static Analysis
- Secure Coding: Threat Modeling
- Secure Coding: Vulnerable Dependencies

MARKETING
- Cybersecurity for Marketing Professionals
- Why? Marketing

SALES
- Cybersecurity for Sales Professionals
- Mini Box: Cybersecurity for Your Sales Team
- Why? Sales

SERVICE DESK
- Why? Service Desk

VENDOR MANAGEMENT / PURCHASING
- Case in Point: Vendor Email Compromise (VEC)
- Cybersecurity for Vendor Management & Purchasing Professionals
- Why? Vendor/Supply Chain

EMPLOYEE CLASS-BASED

EXECUTIVES
- Cybersecurity for Executives
- LS Talk: Executives, the Ultimate Target
- LS Talk: Incidents & Preparing for Breach
- LS Talk: Privacy for Executives
- LS Talk: Threat Landscape & Common Attacks for Executives
- LS Talk: Working Outside of the Office for Executives
- Mini Box: Cybersecurity for Executives
- War Room *(Virtual Tabletop Experience)*

HIGHLY VISIBLE ROLES
- LS Talk: Privacy for Executives
- Vantage Point: Cyber Harrassment for Public Figures

PEOPLE MANAGERS
- Cybersecurity for People Managers
- Investigate: Insider Threat
- LS Talk: Executives, the Ultimate Target
- LS Talk: Incidents & Preparing for Breach
- LS Talk: Privacy for Executives
- LS Talk: Threat Landscape & Common Attacks for Executives
- LS Talk: Working Outside the Office for Executives
- Why? People Managers

See also: *different ways to view content.*

Content by Audience

EMPLOYEE-CLASS BASED (cont'd)

PRIVILEGED USERS

- Cybersecurity for Privileged Users
- Big Ideas: Privileged Permissions
- Day in the Life: Privileged Users
- High-Value Phishing (Puzzle Module)
- Mini Box: Privileged Users
- Secure Coding Basics (Puzzle Module)
- War Room (Virtual Tabletop Experience)
- Why? Privileged Users

ROLE-BASED

SOCIAL MEDIA MANAGERS

- Campaign in a Box: Social Media Security
- Vantage Point: Cyber Harassment for Social Media Managers

EXECUTIVE ASSISTANTS

- Cybersecurity for Executive Assistants
- Why? Executive Assistant
- LS Talk: Executive Assistants

See also: *different ways to view content.*