livingsecurity

Content Catalog

Last Update: September 2022

Living Security is dedicated to diversity.

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

50% of actors in Living Security content are **WOMEN.**

85% of Living Security content includes **BIPOC** actors.

Ways to view our content

By Type

- CyberEscape Online
- Series
- Modules
- Assessments
- Puzzles
- Campaign in a Box

By Category

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

By Audience

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

Table of Contents

See also: ***different ways to view content.***

CYBERESCAPE ONLINE

Storylines designed to play as a team, with up to 10 users at once. Includes videos, puzzles, and quiz questions.

CyberEscape Online

- Born Secure: Entrance Exam
- Born Secure: Entrance Exam (Retail)
- Critical Mass

Teams Training

- Cybersecurity Tonight
- Healthcare Cyber Checkup
- Secure My Life Now!
- The Cyber Race

Virtual Tabletop Experience (VTX)

- War Room

SERIES

Storylines that play out over multiple episodes. May include puzzles and assessments.

- T.G.I.S.
- True Eye
- Phishing IRL
- The Squad
- Born Secure: Training Grounds
- Secure My Life
- Cybersecurity Tonight

MODULES

Independent video modules. May include short assessments.

Day in the Life (2 min)

- HR
- Finance
- General
- Priv. User
- Support

Big Ideas (3-5 min)

- Data Classification
- General Cybersecurity
- Password Management
- Phishing
- PII
- Privacy
- Privilege User/Permissions
- Vishing

Security Basics (1-2 min)

- Data Classification
- Device Security
- Encryption
- Insider Threat

Security Basics (cont'd)

- Internet of Things (IoT)
- Malware
- MFA
- Mobile Security
- Password Managers
- Phishing
- Physical Security
- Policy Violations
- Remote Work
- Reusing Passwords
- Secure Your Apps
- Shadow IT
- Sharing Passwords
- Smishing
- Spear-Phishing
- Tailgating
- Vishing
- Whaling

Compliance Basics (1-2 min)

- CCPA
- Data Privacy
- GDPR
- HIPAA
- PCI
- PHI
- PII
- PIPEDA

Role-Based 'Why' (1-2 min)

- Customer Support 'Why'
- Exec. Assistant 'Why'
- Finance 'Why'
- Help Desk 'Why'
- HR 'Why'
- Marketing 'Why'
- Sales 'Why'
- Vendor/Supply Chain 'Why'
- Service Desk 'Why'

Case in Point (2-3 min)

- Advanced Financial Social Engineering
- Cloud Security Threats
- Internet of Things (IoT)
- Mobile Security
- Password Reuse
- Physical Security
- Point of Sale (PoS) Security
- Ransomware
- Reporting Suspicious Activity
- Safety Online
- Synthetic Identity Theft
- Themed Phishing

Table of Contents

See also: ***different ways to view content.***

As Living Security is always adding new content, this space is intentionally left blank for new Modules. Additional Types are continued on the following page.

Table of Contents

See also: ***different ways to view content.***

ASSESSMENT MODULES

Independent assessments and surveys to test user knowledge on a subject.

PUZZLE MODULES

Independent puzzles. May include short assessments.

CAMPAIGN IN A BOX

A blog, emails, and chat messages. May include infographics and/or a phishing simulation email.

Main Boxes

Mini Boxes

Teams / CyberEscape Online

livingsecurity

Critical Mass

General End Users | 45-60 min

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: 30 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

livingsecurity

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*

Healthcare Cyber Checkup

General Healthcare End User | 15 or 30 min

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. Healthcare CyberEscape Online focuses on cybersecurity as it relates to those who deal with patient health information. Challenges focus on key security concepts, such as phishing, passwords, and the expectations surrounding them as laid out by HIPAA.

LEARNING OBJECTIVES

- Physical security in a hospital or private clinic environment
- Phishing, specifically for PHI
- Strong passwords/passphrases (30 min version only)
- HIPAA and protected vs unprotected information (30 min version only)

INTEGRATED PUZZLES

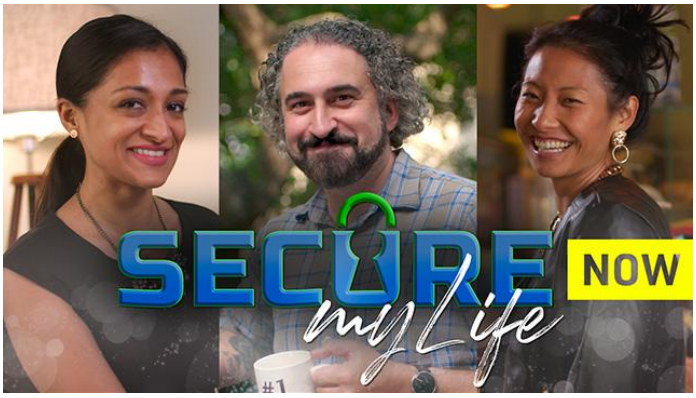
- *Physical Security in the Hospital or Physical Security in the Clinic*
- *Phishing for PHI**
- *Password Protecting PHI** (30 min version only)
- *What's Protected by HIPAA** (30 min version only)

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

Teams / CyberEscape Online

livingsecurity

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*

Cybersecurity Tonight

General End User | 60-85 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
*Available to Cybersecurity Awareness Month Clients Only
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)

livingsecurity

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

livingsecurity

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
- Hotspot - Identify the security vulnerabilities
- Classify - Determine the security level of assets
- Vishing - Follow a vishing attack scenario
- Unscramble - Create the sentences that describe cybersecurity best practices

Training Series

livingsecurity

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 (4)

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 (4)

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

livingsecurity

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
- Craft-a-Phish - Experience designing phishing emails
- HotSpot - Identify physical security vulnerabilities
- Corkboard - Understand high level attack strategies

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

Cybersecurity Tonight

General End User | 22:09
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.

Training Modules

livingsecurity

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'* | 21:00 | 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:

- HR Staff
- Finance
- General End User
- Privileged User
- Support Staff

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

livingsecurity

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 | 9:00 | 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 | 8:45 | 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 | 9:00 | 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 | 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 | 9:00 | 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 | 9:15 | 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 | 9:00 | 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 | 8:30 | 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

livingsecurity

Security Basics (1-2 min)

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 | 2:30 | 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 | 2:30 | 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 | 2:45 | 3 questions

DESCRIPTION

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

Insider Threat

End Users | 2:30 | 3 questions

DESCRIPTION

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

Internet of Things (IoT)

End Users | 2:30 | 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 | 2:30 | 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 | 2:45 | 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 | 2:30 | 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 | 2:30 | 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 | 2:45 | 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

livingsecurity

Physical Security
End Users | 2:45 | 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 | 2:30 | 3 questions

DESCRIPTION

Users will come to understand the importance of policy, how policies protect data, and how they protect individuals.

Remote Work
End Users | 2:45 | 3 questions

DESCRIPTION

Users will learn about the risks of remote work and how they can minimize those risks.

Reusing Passwords
End Users | 2:30 | 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.

Secure Your Apps
End Users | 2:30 | 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 | 3:00 | 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 | 2:30 | 3 questions

DESCRIPTION

Users will learn why sharing passwords is a security concern.

Smishing
End Users | 2:30 | 3 questions

DESCRIPTION

Users will learn about smishing, including why it's a threat and how an attack can be spotted.

Spear-Phishing
End Users | 2:30 | 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 | 2:30 | 3 questions

DESCRIPTION

Users will learn what tailgating is, what it's used for, and how to prevent it.

Vishing
End Users | 3:00 | 3 questions

DESCRIPTION

Users will learn what vishing is, what it's used for, and how to foil a vishing attack.

Whaling
End Users | 2:30 | 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.

Training Modules

livingsecurity

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 | 2:45 | 3 questions

DESCRIPTION

Users will learn the basics of the California Consumer Privacy Act.

Data Privacy

End Users | 3:00 | 3 questions

DESCRIPTION

Users will learn how to identify suspicious applications and agreements and how to properly adjust their privacy settings.

GDPR

End Users | 3:15 | 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 | 2:45 | 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 | 3:00 | 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 | 3:15 | 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 | 3:15 | 3 questions

DESCRIPTION

Users will learn about personally identifiable information and how they can safely share and collect it.

PIPEDA

End Users | 2:45 | 3 questions

DESCRIPTION

Users will learn the basics of the Personal Information Protection and Electronic Documents Act.

Training Modules

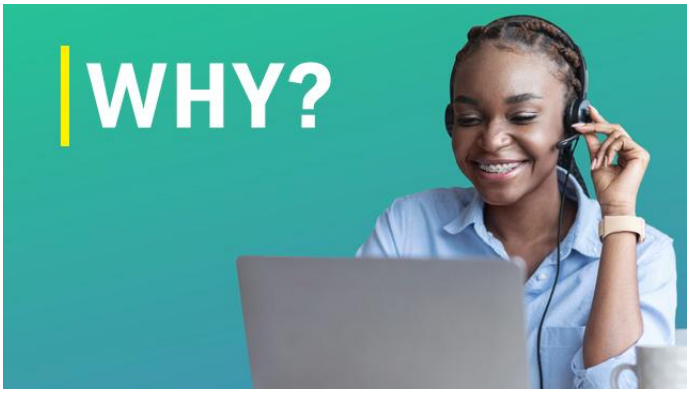
livingsecurity

Role-based ‘Whys’

(1-2 min)

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.



Customer Support ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for customer support personnel at all levels of the department.

Exec. Assistant ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for executive assistant personnel at all levels of the department.

Finance ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for finance personnel at all levels of the department.

Help Desk ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for service help personnel at all levels of the department.

HR ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for HR personnel at all levels of the department.

Marketing ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for marketing personnel at all levels of the department.

Sales ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for sales personnel at all levels of the department.

Vendor/Supply Chain ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for vendor and supply chain personnel at all levels of the department.

Service Desk ‘Why’

End Users | 2:30 | 3 questions

DESCRIPTION

Users will discover why security matters for service desk personnel at all levels of the department.

Training Modules

livingsecurity

Case in Point (2-3 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 | 6:00 | 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 Threats

General End Users | 4:00 | 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 | 5:15 | 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 | 4:15 | 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 Reuse

General End Users | 4:00 | 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 | 4:00 | 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 (PoS) Security

General End Users | 6:30 | 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 | 5:00 | 5 questions

DESCRIPTION

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

Training Modules

livingsecurity

Reporting Suspicious Activity
General End Users | 5:15 | 5 questions

DESCRIPTION

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

Safety Online
General End Users | 1:34 | 5 questions

DESCRIPTION

In this module, users will be exposed to basic domain awareness (HTTP/s and top-level domains), tips for using social media securely, and risks of the sharing economy.

Synthetic Identity Theft
General End Users | 2:37 | 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 | 5:00 | 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 | 4:15 | 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 | 5:00 | 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 | 5 questions

DESCRIPTION

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

Training Modules

livingsecurity

Secure Coding (1-2 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 | 2:30 | 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 | 3:00 | 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 | 3:15 | 3 questions

DESCRIPTION

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

Least Privilege

Developers | 2:45 | 3 questions

DESCRIPTION

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

OWASP Introduction

Developers | 2:45 | 3 questions

DESCRIPTION

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

Patching

Developers | 3:15 | 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 | 3:15 | 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 | 2:30 | 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 | 2:45 | 3 questions

LEARNING OBJECTIVES

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

Vulnerable Dependencies

Developers | 2:45 | 3 questions

LEARNING OBJECTIVES

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

Training Modules

livingsecurity

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 | 2:45 | 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 | 3:00 | 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 | 2:45 | 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

livingsecurity

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 | 10:00 | 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 | 9:00 | 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 | 10:15 | 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 | 9:45 | 5 questions

DESCRIPTION

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

Phishing

General End Users | 10:15 | 5 questions

DESCRIPTION

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

Ransomware

General End Users | 8:15 | 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 | 9:45 | 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 | 8:00 | 5 questions

DESCRIPTION

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

Training Modules

livingsecurity

Brick Wall (3-7 min)

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 | 7:30 | 5 questions

DESCRIPTION

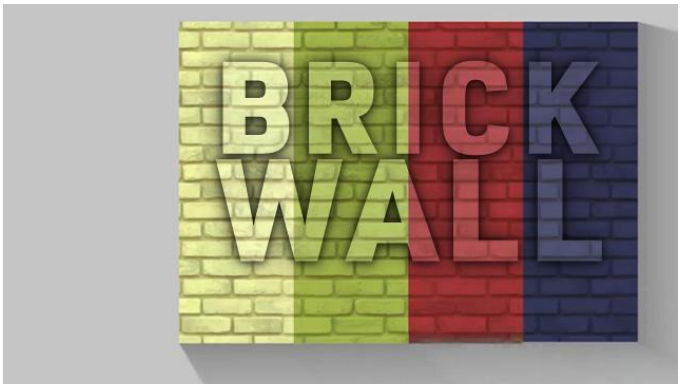
Users will learn about the rights afforded to Californian consumers under the California Consumer Privacy act (CCPA) and the responsibilities they have in upholding these rights.

Data Privacy

General End Users | 6:00 | 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.



GDPR Compliance

General End Users | 9:30 | 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

livingsecurity

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 | 2:45 | 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 | 3:00 | 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 | 2:45 | 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 | 3:00 | 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 | 3:45 | 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 | 3:00 | 3 questions
DESCRIPTION
In this module, users will learn about popular BEC scams involving gift cards.

Lock Your Computer
General End Users | 2:45 | 3 questions
DESCRIPTION
In this module, users will learn the importance of locking unattended devices.

Pretexting
General End Users | 2:45 | 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

livingsecurity

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 | 5:15 | 5 questions

DESCRIPTION

In this module, users will learn why cybersecurity is important to their job.

Passwords & Authentication

General End Users | 5:45 | 5 questions

DESCRIPTION

In this module, users will learn about passphrases, password managers, good password hygiene, and multifactor authentication

Malware & Ransomware

General End Users | 5:45 | 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 | 6:15 | 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 | 6:37 | 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 | 6:00 | 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 | 4:15 | 5 questions

DESCRIPTION

In this module, users will learn what social engineering is and how they can recognize when they're being manipulated.

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 | 4:00 | 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 | 3:30 | 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 | 3:45 | 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 | 3:45 | 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 | 3:45 | 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 | 3:30 | 3 questions

DESCRIPTION

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

Training Modules

livingsecurity

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 | 6:45 | 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 | 6:30 | 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 | 6:45 | 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 | 8:15 | 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 | 6:45 | 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 | 7:15 | 5 questions
DESCRIPTION
Executives will learn the unique risks of working remotely, whether at home or while traveling.

Training Modules

livingsecurity

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.
*Available to Cybersecurity Awareness Month Clients Only

This content is also available on the CyberEscape Online Platform.

Protecting Your Digital Identity
General End Users | 5:45 | 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 | 7:30 | 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 | 6:15 | 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 | 8:30 | 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 | 8:15 | 5 questions
DESCRIPTION
In this module, users will about the different types of crypto wallets and how to secure their digital assets.

Surveys & Assessments

livingsecurity

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.

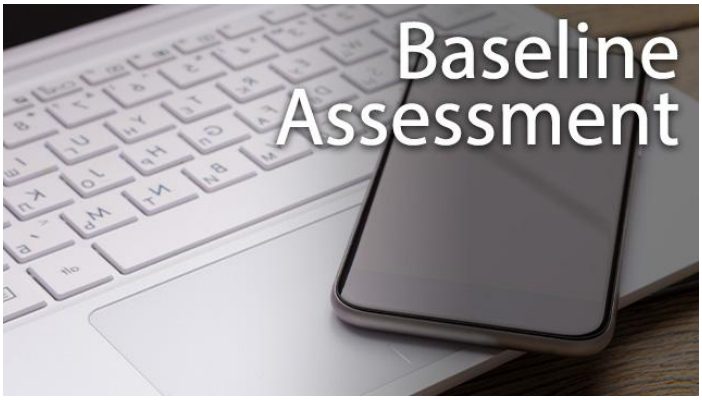
Culture Assessment

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.

Baseline Assessment



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.

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!

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.

Puzzle Modules

livingsecurity

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

General End Users | ~2 min

DESCRIPTION

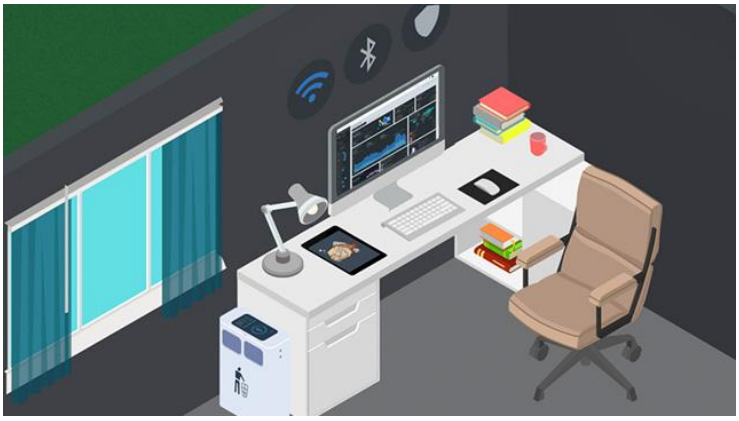
Users will identify the individual who is most likely to be targeted with a phishing attack by a criminal nation or state. Users will better understand what makes someone a high-value target for phishing attacks—power, access, influence, and poor security hygiene.

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 Security

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!

Craft-a-Phish

General End Users | ~2 min

DESCRIPTION

Users will place themselves inside the mind of a cybercriminal and learn to craft an enticing phishing email. By crafting a phishing email from the perspective of an attacker, users will learn ways in which people are exploited by trickery and persuasion via email.

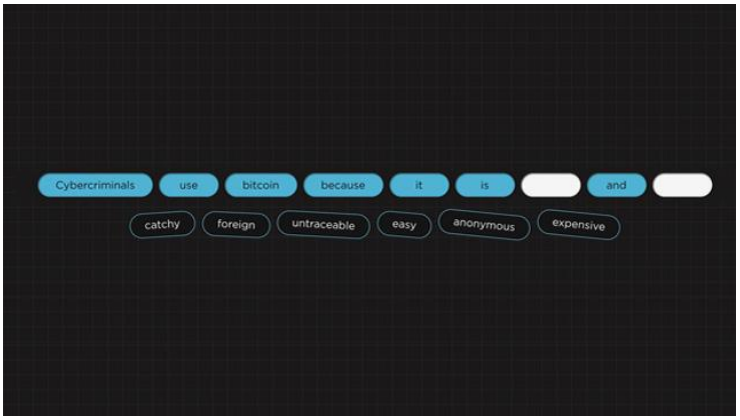
Flag Phishery

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.

Puzzle Modules



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.

Spot the Phish - Social Media

General End Users | ~2 min

*Available to Cybersecurity Awareness Month Clients Only

DESCRIPTION

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

Spot the Phish - Phishing Email

General End Users | ~2 min

*Available to Cybersecurity Awareness Month Clients Only

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

*Available to Cybersecurity Awareness Month Clients Only

DESCRIPTION

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

Preventing Digital Identity Theft

General End Users | ~5 min

*Available to Cybersecurity Awareness Month Clients Only

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

*Available to Cybersecurity Awareness Month Clients Only

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

*Available to Cybersecurity Awareness Month Clients Only

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.

Stop the Vish

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.

Puzzle Modules

livingsecurity

Be the Vish - Social Engineering Financial Information

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.

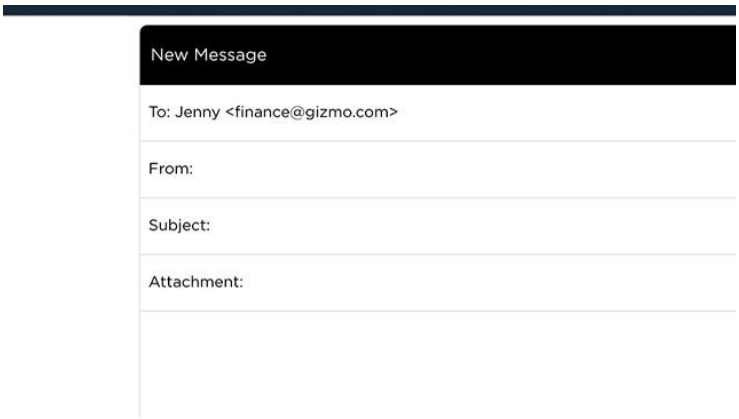
Privacy & PII - What to Protect

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.

Healthcare - Sorting PHI & Non-PHI Information

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.

Healthcare Workers Phishing

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.

Your Password Health Puzzle

General End Users | ~4 min

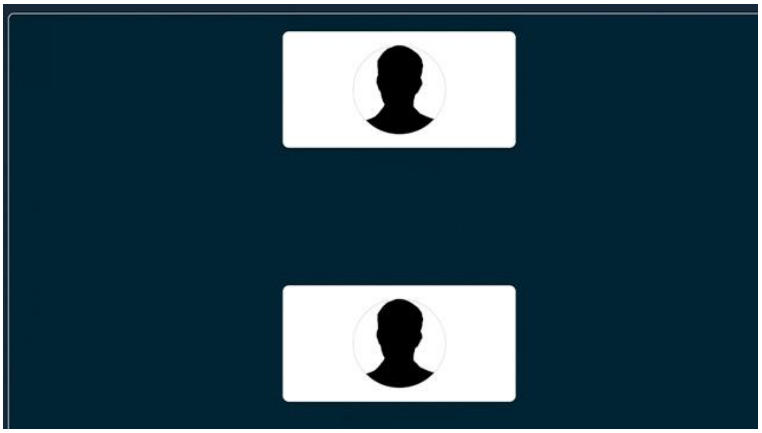
DESCRIPTION

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.

Puzzle Modules

livingsecurity



Emoji Passphrase Decoder

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.

Dealing with Ransomware: Your Options

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 - A Multi-Step Scheme Puzzle

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.

Physical Security in the Workplace

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 & Protecting PII Puzzle

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 Born Secure: Entrance Exam series.

Cyber Hygiene - Level Up Your Online Safety

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.

BEC Scam Builder

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.

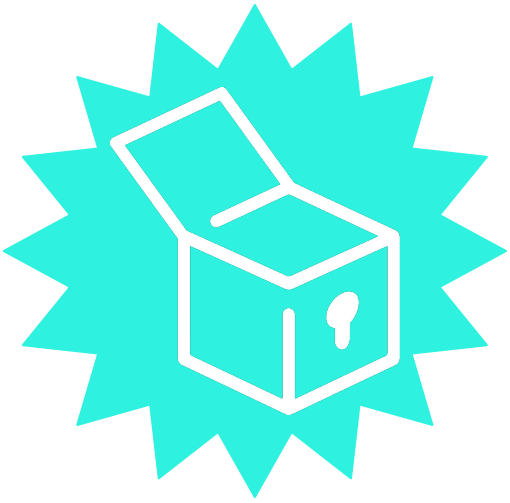
This content is also available in Born Secure: Entrance Exam series.

livingsecurity

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

2022 Year in Review
Coming December 2022

Browsing & Incident Reporting
Released September 2021

Digital Identity
Coming October 2022

Family First
Released February 2022

Governance & Compliance
Released September 2022

Holiday Scams
Released November 2021

Internet of Things & Online Shopping
Released December 2021

Malware
Released April 2021

Mobile Security
Released June 2021

Passwords
Released May 2021

Phishing
Updated May 2022

Privacy
Coming October 2022

Ransomware
Released March 2022

Secure Coding
Released November 2021

Social Engineering
Updated June 2022

Social Media Security
Released July 2021

State of the Scam
Released April 2022

Travel Safety
Updated August 2022

Updates
Released July 2022

Work Play Live
Released October 2021

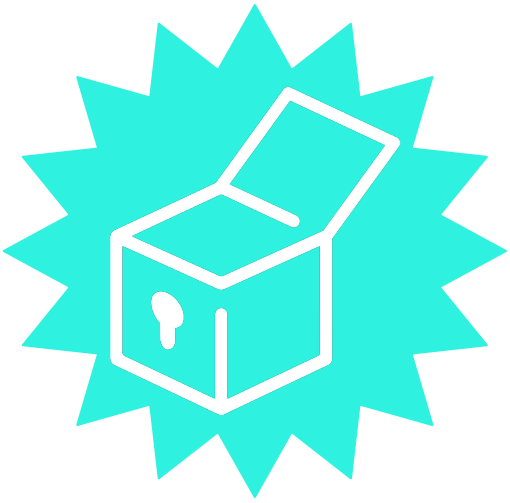
Campaign in a Box

livingsecurity

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



Back to School
Released July 2021

Cookies & Data Collection
Released September 2022

COVID-19 Travel Scams
Released June 2021

Cybersecurity for Executives
Released May 2022

Encryption
Released March 2022

Family First
Released February 2022

International Fraud Awareness Week
Released November 2021

Internet Safety Month
Released June 2021

IRS Scams
Updated March 2022

IRS Scams & Identity Management Day
Released March 2021

Location Sharing
Released August 2022

Passwordless Sign-On
Released June 2022

Patching
Released July 2022

Physical Security
Released June 2022

Putting the 'U' in Cybersecurity
Released April 2022

Romance Scams
Released February 2022

Sharing Security with Family
Coming November 2022

Web 3
Coming October 2022

Content by Category

See also: ***different ways to view content.***

AUTHENTICATION & ACCESS

- T.G.I.S.
- True Eye
- Born Secure: Training Grounds
- Secure My Life
- Cybersecurity Tonight
- Big Ideas: Password Management
- 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 Security *(Puzzle Module)*
- Password Safety & Account Security *(Puzzle Module)*
- Critical Mass *(CyberEscape Online)*
- Born Secure: Entrance Exam *(CyberEscape Online)*
- Healthcare Cyber Checkup *(CyberEscape Online)*

DATA SECURITY & PRIVACY

- True Eye
- The Squad
- Secure My Life
- Day in the Life
- Big Ideas: Data Classification
- Big Ideas: General Cybersecurity
- Big Ideas: PII
- Big Ideas: Privacy
- 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

Data Security & Privacy (cont'd)

- 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 Security *(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)*

DEVICE SECURITY

- True Eye
- Born Secure: Training GroundsSecure My Life
- Cybersecurity Tonight
- Day in the Life
- Big Ideas: General Cybersecurity
- 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

Content by Category

See also: ***different ways to view content.***

Device Security (cont'd)

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

PHISHING & SOCIAL ENGINEERING

- T.G.I.S.
- Phishing IRL
- The Squad
- Born Secure: Training Grounds
- Secure My Life
- Cybersecurity Tonight
- Day in the Life
- Big Ideas: Phishing
- Big Ideas: Vishing
- 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
- 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)*

Phishing & Social Engineering (cont'd)

- Craft-a-Phish *(Puzzle Module)*
- Flag Phishery *(Puzzle Module)*
- Spot the Phish - Social Media *(Puzzle Module)*
- Spot the Phish - Phishing Email *(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)*

PHYSICAL SECURITY

- True Eye
- Born Secure: Training Grounds
- 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)
- Healthcare Cyber Checkup (CyberEscape Online)

POLICY & 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

Content by Category

See also: ***different ways to view content.***

Policy & Compliance (cont'd)

- 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

- T.G.I.S.
- The Squad
- Secure My Life
- Cybersecurity Tonight
- Day in the Life
- Big Ideas: General Cybersecurity
- Role-Based 'Whys': Customer Support 'Why'
- Role-Based 'Whys': Exec. Assistant 'Why'
- Role-Based 'Whys': Finance 'Why'
- Role-Based 'Whys': Help Desk 'Why'
- Role-Based 'Whys': HR 'Why'
- Role-Based 'Whys': Marketing 'Why'
- Role-Based 'Whys': Sales 'Why'
- Role-Based 'Whys': Vendor/Supply Chain 'Why'
- Role-Based 'Whys': Service Desk 'Why'
- 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
- 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

- T.G.I.S.
- True Eye
- The Squad
- Secure My Life
- 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)*
- Spot the Phish - Social Media *(Puzzle Module)*
- Secure My Life Now! *(CyberEscape Online)*
- 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)*
- Spot the Phish - Social Media *(Puzzle Module)*
- Secure My Life Now! *(CyberEscape Online)*

Content by Audience

See also: ***different ways to view content.***

VERTICAL-BASED

Retail

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

Healthcare

- Compliance Basics: HIPAA
- Compliance Basics: PHI
- Healthcare Cyber Checkup *(CyberEscape Online)*

DEPARTMENT-BASED

Customer Support

- Day in the Life: Customer Support
- Role-based 'Whys': Customer Support 'Why'

Finance

- Day in the Life: Finance
- Role-based 'Whys': Finance 'Why'

Human Resources (HR)

- Day in the Life: HR
- Role-based 'Whys': HR 'Why'

Marketing

- Role-based 'Whys': Marketing 'Why'

Sales

- Role-based 'Whys': Sales 'Why'

Service Desk

- Role-based 'Whys': Service Desk 'Why'

Information Technology (IT)

- Secure Coding: Introduction
- Secure Coding: Authentication and Authorization
- Secure Coding: Injection
- Secure Coding: Least Privilege
- Secure Coding: OWASP Introduction
- Secure Coding: Patching
- Secure Coding: Source Code Secrets
- Secure Coding: Static Analysis
- Secure Coding: Threat Modeling
- Secure Coding: Vulnerable Dependencies

Vendor Management / Purchasing

- Case in Point: Vendor Email Compromise (VEC)
- Role-based 'Whys': Vendor/Supply Chain 'Why'

EMPLOYEE CLASS-BASED

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
- War Room *(Virtual Tabletop Experience)*

Highly Visible Roles

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

Privileged Users

- Big Ideas: Privileged Permissions
- Day in the Life: Privileged User
- 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
- High-Value Phishing *(Puzzle Module)*
- Secure Coding Basics *(Puzzle Module)*
- War Room *(Virtual Tabletop Experience)*

ROLE-BASED

Social Media Managers

- Vantage Point: Cyber Harassment for Social Media Managers

Executive Assistants

- Role-based Whys: Exec. Assistant 'Why'
- LS Talk: Executive Assistants