Training Resources

Your Guide to What's Available

A successful security awareness program starts with targeted training that breaks down complicated topics into engaging content. This growing catalog of modules covers everything you need and more.

Awareness Training

Our comprehensive catalog covers core awareness topics in addition to dozens of supplemental modules addressing today's most pressing information security issues.

Click Thinking Express

Developed for today's attention spans, these modules distill key concepts into 60-second sessions for anywhere, anytime viewing.

Games

To add variety to your training plan, we offer a wide range of games that make learning fun and keep employees engaged.

Specialized Training

Training that's tailor-made for specific objectives, including a Cyber Security Awareness Month curriculum you can use any time.

Live Actor Videos

Highly engaging and fun videos provided by the NCSA addressing a wide range of topics.

Click Thinking Bundles

A catalog of awareness training materials including infographics, newsletters, spotlights and more that grows with each monthly Click Thinking bundle.

Topics Covered

- What is Phishing?
- Types of Phishing
- Understanding URLs
- Spotting Phishing Scams
- Cyberattacks
- Human Factor
- Passwords
- Social Engineering
- Mobile Device Security
- Incident Response
- Ransomware
- Social Media
- Spear Phishing
- Security and the Cloud
- Network Security
- Removable Media
- Personally Identifiable Information
- Business Email Compromise
- Travel and Out of Office
- Personal/Physical Security
- Vishing and Smishing
- Applications
- Professional Networking
- Bring Your Own Device
- Public Wifi
- Internet of Things
- Web Browsing and Work
- Working from Home
- Sensitive Data
- Clean Desk Policy
- Executive Targeting
- Catfishing
- Phishing Careers
- GDPR
- PCI-DSS
- Online Holiday Shopping
- Vocabulary of Info Security
- Data Classification
- Data Loss Prevention
- Data Breaches
- Insider Threats
- Access Control
- Staffing and Cybersecurity
- Account Takeover
- Spam

All modules are available with and without quizzes to assess engagement and learning.

Barracuda
Your journey, secured.

Baseline Training

P101A-1	What is Phishing?	**2:47**	A high-level introduction to the concept of phishing.
P101A-2	Types of Phishing	**2:58**	An overview of phishing, spear phishing, smishing and vishing.
P101A-3	Understanding URLs	**4:56**	Insights into web addresses that protect browsers from threats.
P101A-4	Spotting Phishing Scams	**3:46**	Many of the most popular phishing techniques revealed.
A101A-1	Cyberattacks	**2:32**	Tips on keeping company data secure and safe from hackers.
A101A-2	Human Factor	**2:21**	Policies designed to safeguard employees and company data.
A101A-3	Passwords	**2:56**	Tips for creating strong passwords that resist hacking.
A101A-4	Social Engineering	**2:53**	Ways to avoid being manipulated by scammers.
A101A-5	Mobile Device Security	**1:57**	How to protect devices from being accessed by cybercriminals.
A101A-6	Incident Response	**1:26**	Steps to take when faced with a phishing attempt.

Additional Training

A102A-1	Ransomware	**3:03**	How to protect your data from being held hostage.
A102A-2	Social Media	**3:05**	Popular social media scams and how to avoid them.
A102A-3	Spear Phishing	**3:23**	How to recognize spear phishing and react if targeted.
A102A-4	Security and the Cloud	**2:38**	Outlines risks when using the cloud and how to avoid them.
A102A-5	Network Security	**3:34**	Best practices designed to protect the company network.
A102A-6	Removable Media	**3:28**	A look at the risks of using removeable media.
A102A-7	Personally Identifiable Info	**3:15**	How to identify and protect Personally Identifiable Information (PII).
A102A-8	Business Email Compromise	**3:34**	Business Email Compromise (BEC) Scams and prevention tips.
A102A-9	Travel and Out of Office	**2:47**	Tips to secure company information during business travel.
A102A-10	Personal and Physical Security	**3:57**	Tactics cybercriminals use to gain access to secure areas.
A102A-11	Vishing and Smishing	**3:24**	Voice and text phishing explained, with tips for protecting business.
A102A-12	Applications	**3:12**	Explores dangers of download apps from the internet.
A103A-1	Professional Networking	**3:22**	Tips for protecting yourself and company when networking.
A103A-2	Bring Your Own Device	**2:45**	The risks of using one device for personal and business use.
A103A-3	Public Wifi	**3:37**	Explores dangers of using public wifi and how to avoid them.

Barracuda
Your journey, secured.

▶ Additional Training continued

A103A-4	Internet of Things	**3:07**	Examines the risks of using internet-connected devices.
A103A-5	Web Browsing and Work	**2:05**	Highlights ways to stay cyber-safe when web browsing at work.
A103A-6	Working From Home	**3:35**	Protecting your company from cyberthreats when working at home.
A103A-7	Sensitive Data	**3:51**	Properly handling, storing and disposing of sensitive data.
A103A-8	Clean Desk Policy	**4:04**	Outlines how a clean desk policy can deter cybercriminals.
A103A-9	Executive Targeting	**4:58**	Insights into the ways scammers phish top executives.
A103A-10	Catfishing	**4:43**	Explores the motives of catfishers and how to avoid targeting.
A103A-11	Phishing Careers	**3:38**	How cybercriminals target both sides of the hiring process.
A103A-12	GDPR	**4:57**	Insights into new GDPR guidelines.
A103A-13	PCI-DSS	**4:36**	An overview of payment card information data security standards.
A103A-14	Online Holiday Shopping	**4:57**	Shows how cybercriminals scam online holiday shoppers.
A103A-15	Vocabulary of Info Security	**4:14**	The basics of Information Security defined.
A103A-16	Data Classification	**5:32**	Outlines how to create a data classification policy.
A103A-17	Data Loss Prevention	**4:45**	Spells out how to develop a data loss prevention plan.
A103A-18	Data Breaches	**3:41**	A look at the causes of data breaches and how best to respond
A103A-19	Insider Threats	**4:46**	Reviews insider threat categories and how to identify them.
A103A-20	Access Control	**5:14**	Defines how access permissions impact information security.
A103A-21	Staffing and Cybersecurity	**5:05**	Staffing best practices that keep cybersecurity top of mind.
A103A-22	Account Takeover	**4:47**	Examines how account takeover and lateral phishing work.
A103A-23	Spam	**3:53**	An overview of spam and the problems it can create.

Click Thinking Express (each module runs less than a minute)

CTE-1	Phishing Signs	Tips for identifying phishing emails and how to protect yourself.
CTE-2	Phishing Types	Explores and explains different phishing methods scammers rely on.
CTE-3	Web Addresses	Identifies what to look for in a web address to ensure a safe browsing experience.
CTE-4	Hyperlinks	Reveals how hyperlinks can mask fraudulent websites.
CTE-5	Cyberattacks	A look at who's vulnerable and how to protect yourself.

▶ Click Thinking Express continued

CTE-6 Human Factor	Highlights the important role individuals play in cyber security.
CTE-7 Incident Response	Outlines how to respond if you click a malicious link or download.
CTE-8 Mobile Devices	Tips for securing your devices and the information on them.
CTE-9 Passwords	Identifies what makes a password strong and why it's important.
CTE-10 Social Engineering	Looks at the human side of cyberattacks and how scammers manipulate victims.
CTE-11 Spotting Phishing Scams	A list of things to look for to identify phishing emails.
CTE-12 Data Classification	Rationale and examples of how organizations classify data.
CTE-13 Data Breaches	Insights into how data breaches occur and how to prevent them
CTE-14 Data Loss Prevention	Examines how to prevent data losses in organizations.
CTE-15 PII	Outlines Personally Identifiable Information (PII) and how to protect it.
CTE-16 Web Browsing and Work	A look at best practices to safeguard the company when going online.
CTE-17 Public Wifi	Reveals tips for safer online web browsing when using public wifi.
CTE-18 Internet of Things	Tips for keeping your wifi-enabled devices from being hacked.
CTE-19 Ransomware	A high-level look at ransomware prevention tactics.
CTE -20 Sensitive Data	Helps users understand how to protect your organization's data.
CTE-21 Security and the Cloud	Reviews best practices when using the cloud to store data or access apps.
CTE-22 Removable Media	A look at best practices when using removable and portable storage devices.
CTE-23 Mobile Device Security	Outlines how to protect your mobile devices from cyberthreats.
CTE-24 Clean Desk Policy	Reveals how an uncluttered desk can be a cyber crime deterrent.
CTE-25 Business Email Compromise	Reviews tips to recognize if your email network has been compromised.
CTE-26 Network Security	A look at ways to protect your network from attackers who seek access.
CTE-27 Social Media	Examines how cybercriminals exploit users of social media platforms.
CTE-28 Catfishing	Spotlights romance scams and their impact on business and personal life.

Barracuda
Your journey, secured.

Live Actor Videos

Computer Theft	**2:11**	Best practices for keeping devices safe.
Data Handling	**2:13**	Best practices for handling data.
Internet Downoads	**1:42**	Best practices for downloading data and apps.
Passwords	**3:22**	Best practices for using passwords.
Ransomware	**2:33**	Best practices for avoiding ransomware attacks.
Removable Media	**1:35**	Best practices for handling removable media and devices.
Vishing	**2:39**	Best practices for avoiding vishing attacks.
Wifi	**2:18**	Best practices for using wifi at work.

Specialized Training

Cyber Security Awareness - Week 1 Training	Part of a comprehensive four-week cybersecurity awareness curriculum.
Cyber Security Awareness - Week 2 Training	Part of a comprehensive four-week cybersecurity awareness curriculum.
Cyber Security Awareness - Week 3 Training	Part of a comprehensive four-week cybersecurity awareness curriculum.
Cyber Security Awareness - Week 4 Training	Part of a comprehensive four-week cybersecurity awareness curriculum.
Texas Cybersecurity Training Certification	Comprehensive training certified by the Department of Information Resources.

Essential Eight Curriculum

E8-01	Introduction	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-02	Application Whitelisting	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-03	Patching Applications	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-04	Configuring Microsoft Office	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-05	Application Hardening	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-06	Restrict Admin Privileges	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-07	Patching Operating Systems	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-08	Multi-factor Authentication	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-09	Daily Backups	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.
E8-10	Social Engineering	Part of a curriculum covering Australia's Essential Eight cyberthreat mitigation program.

Barracuda
Your journey, secured.

Games

CT101A-1	Ransomware Game	Players learn about ransomware from a cybercriminal's perspective.
CT101A-2	Who's In? Game	Players attempt to steal sensitive data using tactics used by thieves.
CT101A-3	Fetch a Phish	Players learn about 13 email threat types by capturing sea creatures.
CT101A-4	Phishellaneous Level One	Jeopardy style game that covers P101 concepts.
CT101A-5	Phishellaneous Level Two	Jeopardy style game that covers A101 concepts.
CT101A-6	Phishellaneous Combined	Jeopardy style game that covers P101 and A101 concepts.
CT101A-7	Is This a Phish?	Players test their ability to spot phishing emails (10 emails).
CT101A-8	Looking Phishy	Comprehensive find-a-word phishing awareness puzzle (12 words).
CT101A-9	Attention Getters	Mini find-a-word phishing awareness puzzle (3 words).
CT101A-10	Often Overlooked	Mini find-a-word phishing awareness puzzle (3 words).
CT101A-11	Sure Signals	Mini find-a-word phishing awareness puzzle (3 words).
CT101A-12	Things to Watch For	Mini find-a-word phishing awareness puzzle (3 words).
CT101A-13	Reel Phishy	Interactive fishing game that teaches phishing awareness.
CT101A-14	13 Threats Puzzler	Interactive infographic puzzle that outlines top email phishing types.
CT101A-15	Is This A Phish? Mini 1	Players test their ability to spot phishing emails (3 emails).
CT101A-16	Is This A Phish? Mini 2	Players test their ability to spot phishing emails (3 emails).
CT101A-17	Is This A Phish? Mini 3	Players test their ability to spot phishing emails (3 emails).
CT101A-18	Is This A Phish? Mini 4	Players test their ability to spot phishing emails (3 emails).

Barracuda
Your journey, secured.

Click Thinking Bundles

- Ransomware
- Social Media
- Spear Phishing
- Security and the Cloud
- Network Security
- Removable Media
- Personally Identifiable Information
- Business Email Compromise
- Travel and Out of Office
- Personal/Physical Security
- Vishing and Smishing
- Applications
- Professional Networking
- Bring Your Own Device
- Public Wifi
- Internet of Things
- Web Browsing and Work
- Working from Home
- Sensitive Data
- Clean Desk Policy
- Executive Targeting
- Catfishing
- Phishing Careers
- GDPR
- PCI-DSS
- Online Holiday Shopping
- Vocabulary of Info Security
- Data Classification
- Data Loss Prevention
- Data Breaches
- Insider Threats
- Access Control
- Staffing and Cybersecurity
- Account Takeover
- Spam
- Data Privacy
- Safer Internet
- Data Backup
- Removable Media
- Passwords

Bundles contain a newsletter, infographic and, in some cases, additional training materials, such as topic spotlights. To download a bundle visit the Click Thinking section in the Content Center.

Barracuda
Your journey, secured.

All modules are available in ENGLISH with ENGLISH subtitles. In addition, Phishing 101 and Awareness 101 sets have been translated into the langauges listed below. Unless otherwise noted, translations are complete and include voiceover, subtitles and text that appears in video. Voiceovers are chosen for mainstream use. Some spoken dialects may vary.

PHISHING 101 IS ALSO AVAILABLE IN

ARABIC
CHINESE
- Traditional Chinese Subtitles w/Cantonese Voiceover
- Simplified Chinese Subtitles w/Mandarin Voiceover
- Traditional Chinese Subtitles w/Mandarin Voiceover

DUTCH
FRENCH (Canadian)
FRENCH (European)
GERMAN
ITALIAN
INDONESIAN
JAPANESE
KOREAN
MALAYSIAN
POLISH
PORTUGUESE (Brazilian)
PORTUGUESE (European)
SPANISH (European)
SPANISH (Neutral/Latin American/U.S.)
SWEDISH (Subtitles Only)
THAI
TURKISH
VIETNAMESE

AWARENESS 101 IS ALSO AVAILABLE IN

ARABIC
CHINESE
- Traditional Chinese Subtitles w/Cantonese Voiceover
- Simplified Chinese Subtitles w/Mandarin Voiceover

DUTCH
FRENCH (Canadian)
FRENCH (European)
GERMAN
ITALIAN
JAPANESE
POLISH
PORTUGUESE (European)
SPANISH (European)
SPANISH (Neutral/Latin American/U.S.)
TURKISH

NOTE
Based on demand and changing markets, more modules in additional languages may be available in the Content Center. Please check there for up-to-date listings.

CLICK THINKING EXPRESS

Click Thinking Express modules covering P101 and A101 topics are avaiable in English, in addition to a growing number of languages. These include but are not limited to French, Italian, German and Spanish. As additional languages are added they'll be included here.

Barracuda
Your journey, secured.

P101A—1 What is Phishing
Why is phishing so effective: It's becoming easier to detect phishing attacks • It's not really a threat • It exploits natural human trust • The annual financial impact is less than $1 million worldwide
Which statement applies to phishing attacks: Phishing requires human interaction • Phishers want you to divulge confidential info • They spread by various means, mainly email • All of these are correct
What are the consequences of phishing: Loss of financial information • Damage to personal or business reputation • Security breaches • All of these are correct
Why is social engineering so effective: It exploits natural human trust • It targets only the elderly • It's carried out on evenings and weekends • It's not heavily penalized by authorities
Where do phishers pretend to send emails from: Retailers • Social media sites • Friends and relatives • All of these are correct
What are phishers trying to get you to do: Click on suspicious emails • Download harmful malware • Open attachments • All of these are correct

P101A—2 Types of Phishing
What phishing techniques do phishers use to steal information: Phishing, Spear Phishing, Vishing and SMishing • Spear Phishing and Vishing • Vishing and SMishing • Spear Phishing and SMishing
Phishers target: Large groups of random people • Random individuals • Large groups of specific people • Specific individuals
Spear phishing refers to: A direct attack on a specific organization • A directed attack on a specific individual • A random attack on any organization • A random attack against any individuals
Legit organizations may request information through email: Often • Just in specific cases • Never • Once a year
Voice Phishing: Uses SMS instead of an email • Doesn't exist • Usually involves high-quality phone calls • Uses a phone call instead of an email
SMishing uses: Email • Social media • Short Message Services • Phone calls

P101A—3 Understanding URLs
The terms 'URL' and 'web address': Are often used interchangeably • Are not related • Mean different things • None of these is correct
Which protocol is encrypted to keep your information secure: HTTP • HTTPZ • HTTPS • HTTPOK
Incorrectly spelled domain names indicate: The destination may be fraudulent • The programmer goofed up • Your web browser needs service • All of these are correct
A hyperlink can be: A word or phrase • A URL • An image • All of these are correct
What should you do before clicking on a hyperlink: Check your pop-up blocker • Nothing, just click away • Mouse over it to reveal the URL • All of these are correct
How can you protect yourself from suspicious URLs: Type the correct address in your browser • Never click anything suspicious • Spot them in the first place • All of these are correct

P101A—4 Spotting Phishing Scams
Signs of phishing include: A sense of urgency • A generic greeting • Spelling and/or grammatical errors • All of these are correct
The bank deposit scam typically includes: A message from the bank president • A free checking offer • Good news about interest rates • A request to verify account information
The electronic fax scam can be identified by: No greeting • A generic greeting • Phony Links • All of these are correct
An email that simply says 'hello' is: A scammer's way to see if you'll respond • Probably from a friend • Should be replied to immediately • Cute, harmless fun
The unknown attachment scam email: May be addressed to undisclosed recipients • May include addressees you don't recognize • May have an urgent tone • All of these are correct
Hackers target employees primarily because: They have nothing better to do • Employees don't care • Tricking them is easier than hacking the system • None of these are correct

A101A—1 Cyberattacks
Cybercriminals: Have no geographical constraints • Have time and money • Are intelligent • All of these are correct
Cyberattacks erode the trust of: Customers • Shareholders • Public • All of these are correct
Malware: Is short for "malicious software" • Performs unwanted actions on your computer • Can't harm your computer • Two of these are correct
The following are types of malware: Viruses • Worms • Trojan Horses • All of these are correct
Malware is spread through: Email • Social networks and instant messaging • Infected websites • All of these are correct
A drive-by download: Targets cars with onboard computers • Can be performed while driving • Downloads malware to your computer without your knowledge • Is a hacker myth

A101A—2 Human Factor
As an employee: You must take your role in company security personally • You can have a direct effect on cyber security • You can be a weak or strong link • All of these are correct
Cybercriminals attack using: Social engineering and phishing attempts • Drive-by download attempts • Social media sites and email • All of these are correct
You can greatly reduce the chance of security breaches by: Thinking before you click • Using your work computer only for work • Using your work computer as little as possible • Two of these are correct
Failure to follow security protocols can result in: A security violation • Customer identity theft • Financial loss • All of these are correct
Acceptable use policies are rules dictating how employees can use: Networks • Websites • Systems and electronic devices • All of these are correct
Using your work computer for business and lawful purposes: Can prevent security breaches • Can protect company data • Can safeguard customer information • All of these are correct

A101A—3 Passwords
Passwords: Are strong, unless you make them weak • Keep systems locked from unauthorized users • Don't matter because you'll forget them • Two of these are correct
A strong password should: Contain upper- and lower-case letters • Use at least one special character • Include at least one numeric character • All of these are correct
Pass phrases are: Words strung together in a password • Terms you can use to enter elite clubs • Translated into several languages • Based on Morse Code
When creating multiple passwords: Create different ones for different websites • Keep banking and financial passwords separate • Write them down as is • Two of these are correct
The best way to remember passwords is to: Share them with others • Commit them to memory • Write them down • Share them with others

A101A—4 Social Engineering
Social engineering is defined as: Manipulating people into divulging confidential information • Unknowingly giving criminals access to your computer • Hacking the human mind • All of these are correct
Criminals use social media: To watch cat videos • For recipe trading • To scope out potential targets • None of these is correct
As a rule of thumb with social media, don't post: Unless you want the world to see it • Confidential data that criminals could use • When you'll be vacationing or out of town • All of these are correct
Victims of social engineering attacks: Can lose confidential data • Can trigger security breaches • Can lead to compromised systems • All of these are correct
The most prevalent type of social engineering: Is committed by computer-savvy teens • Is done by phone • Involves large crime syndicates • Is committed by relatives
What should you do if you think you're being targeted: Verify the caller's identity • Ask for a number where you can call them back • Remember that you're in control • All of these are correct

A101A—5 Mobile Devices
Mobile devices: Need protection like computers • Contain sensitive information • Are a target for thieves • All of these are correct
Loss or theft of your mobile device can: Expose you to risk • Expose your workplace to risk • Expose your workplace to security breaches • All of these are correct
The most effective mobile device protection is: A sturdy case • A code • A secret pocket • None of these is correct
Security experts recommend auto lock after: 30 seconds of nonuse • 2 minutes of nonuse • 5 minutes of nonuse • 10 minutes of nonuse
A data wipe: Can protect important information • Deletes important data after several failed logins • Makes backups important • All of these are correct
Shoulder surfers seek: ATM PINs • Passwords • Codes they can use to gain access • All of these are correct

A101A—6 Incident Response
Incident response is how you react to: Clicking a suspicious link • Opening a suspicious attachment • Getting a suspicious phone call • All of these are correct
Failure to react immediately may let a hacker: Gain unauthorized access • Steal someone's identity • Commit a crime • All of these are correct
If you're uncertain about a suspicious email: Delete it and go back to work • Forward it to friends who know computers • Click a link to confirm your suspicion • Inform your supervisor
Proper response to a suspicious email includes: Not responding • Verifying using the number you have on record • Notifying your manager if it can't be verified • All of these are correct

A102A—1 Ransomware
Ransomware attacks can victimize: Big companies • Small businesses • Individuals • All of these are correct
Older systems are a target of hackers because: The may contain valuable vintage games • They're easy to infect • Newer systems are more secure • Two of these are correct
If you're not sure if your operating system is up to date: Don't worry, it will update automatically • Get a completely new computer • Check with your technology support team • None of these are correct
Ransomware works because: Humans accidentally let it work • It employs a technique called phishing • It exploits natural human trust • All of these are correct
To avoid becoming a victim: Be wary of emails that don't seem right • Watch for emails with spelling/grammar errors • Be wary of emails promising something too good to be true • All of these are correct
You can avoid becoming a ransomware victim by: Not clicking malicious links • Keeping your system up to date • Staying vigilant • All of these are correct

Barracuda
Your journey, secured.

A102A—2 Social Media
Why do cybercriminals use social media: Because they're lazy • It makes it easy to friend other cybercriminals • They feel connected when they do • It's a perfect smokescreen for their scams
In which social media scam does a cybercriminal pretend to be a customer support helper: Phony Survey • Fake Contest • Teaser from Friend • Customer Service Intercept
Phony surveys: Are often inserted into legitimate social media feeds • Can be used to gather personal information • Are a favorite of cybercriminals • All of these are correct
The fake contest scam: Seems too good to be true • Tricks you into giving up personal information • Has been a favorite of cybercriminals for years • All of these are correct
"You should see these hilarious pictures of you" might be found in which social media scam: Live-Stream Scam • Fake Storefront • Teaser from Friend • Customer Service Intercept
If a post seems legitimate but you're not quite sure: Delete it immediately • Share it for others to weigh in • Contact the friend or business that supposedly sent it • Like it and see what happens

A102A—3 Spear Phishing
Spear phishing differs from phishing in that it: Targets companies that harm aquatic life • Only occurs in Fortune 500 companies • Targets a specific company for attack • Always nets cyberattackers millions
What percent of all cyberattacks begin with a spear phishing attempt: 65% • 95% • 85% • 55%
Negative effects of spear phishing include: Loss of credibility with stockholders • Loss of customer account data • Loss of customer credit card numbers • All of these are correct
The CEO email scam works because: It comes from a position of authority • CEOs are notorious pranksters • Recipients are wired to please those in authority • Two of these are correct
What should you do if you get an email from the CEO: Pat yourself on the back • Do what it says without question • If you don't normally get these be suspicious • Print it and show your colleagues
If you think an email from the CEO is suspicious: Do not click on anything in the email • Contact the sender using the number you have on file • Let information security know • All of these are correct

A102A—4 Security and the Cloud
Companies use the cloud to: Store data • Access software • Show how technically savvy they are • Two of these are correct
A data breach can compromise: Credit card numbers • Social Security Numbers • Account data • All of these are correct
Employees: Should never use the cloud • Should each have a cloud of their own • Play a key role in cloud security • Don't need to worry about cloud security
You can help keep the cloud secure by: Keeping passwords private • Committing passwords to memory • Writing passwords backwards if you must write them down • All of these are correct
Emails from social engineers: Can be an attempt at gaining cloud passwords • May appear to come from a trusted source • Should be verified using the number you have on file • All of these are correct
If you step away from your workspace: Power down your computer • Turn on Caps Lock so passwords won't work • Lock your screen • Do so only when no one is around

A102A—5 Network Security
The first layer of network security is: Pop-up blocker • Network firewall • Email Security • Data loss prevention
Additional layers of protection can include: Data loss prevention • Email security • Web protection • All of these are correct
Network security systems are most vulnerable to attack: On weekends and holidays • When employees let their guard down • During testing • None of these are correct
A favorite tactic for attacking networks is: Sending phishing emails • Hacking the system • Blackmailing/bribing network security • Off-hours break-ins
VPN stands for: Verifiable Private Network • Virtual Password Network • Veritable Passkey Network • Virtual Private Network
Network security is: Not your responsibility • An issue only IT should deal with • Pointless, everything is hackable • A joint effort between those who created the system and the employees using it

A102A—6 Removable Media
Removable media is: A type of news streaming service • A filter that blocks unwanted newscasts • A myth, no media can be removed • Any device used to store and transport data
Removable media can be: A USB drive • A disk • A smartphone • All of these are correct
Any time you use removable media: You could lose it • It could fail • It could contain malware • All of these are correct
Half of all USB drives found in company parking lots are: Thrown away • Inserted into devices by curious employees • Put there by guerrilla marketers • None of these are correct
Plugging unfamiliar removable media into your device can: Launch a cyberattack • Install malware • Infect the network • All of these are correct
If you find a piece of removable media: Destroy it to be safe • Plug it into your device to see if it's malicious • Turn it over to Information Security for analysis • Make copies and share it

A102A—7 Personally Identifiable Information (PII)
PII stands for: Potential Identity Information • Personally Identifiable Information • Preview Individual Identity • Personal Individual Intelligence
Cybercriminals can use PII to: File false tax returns • Open credit cards in others' names • Run for political office • Two of these are correct
An example of PII is: Birthdate • Passport Number • Work Phone Number • Race
What's not considered PII unless combined with PII: Postal Code • Driver's License Number • Personal Email Address • Bank Account Number
Birthdate is not considered PII because: It's not required on most applications • People are sensitive about their age • Different countries use different calendars • Many people share the same birth date
When working with PII: Keep it protected • Don't share it with any suspicious person or entity • Adhere to company guidelines for protecting it • All of these are correct

A102A—8 Business Email Compromise (BEC)
BEC stands for: Business Essentials Compromise • Business Email Compromise • Beat Email Cybercrime • Begin Email Cache
The first step a cybercriminal takes in a BEC scam is: Research • Grooming • Transfer • None of these are correct
A cybercriminal will typically request a wire transfer: The first of the month • Around the holidays • When the CEO is out of town • None of these are correct
Cybercriminals access the company network by: Sending phishing emails • Hacking the system • Sweet talking security • Bribing the CEO
If a BEC scam is considered successful the first time: You can assume the worst is over • Information Security can get the money back • It's usually repeated • Two of these are correct
You can help prevent BEC scams by: Verifying transfer requests by phone or in person • Never relying on email alone • Verifying suspicious requests with your finance team • All of these are correct

A102A—9 Travel and Out of Office
An out of office email message should be: Very detailed and descriptive • Vague so that cyberattackers can't gain insights they can use • Funny, because why not? • None of these are correct
So trusted colleagues can reach you: Provide a number where you can be reached • Don't tell them, it's too dangerous • If your system allows, leave a detailed OOO just for them • Two of these are correct
If a device prompts you to update your system while you're away: Check with your technology team first • It could be malware in disguise • Try updating before/after your travels • All of these are correct
If you must use public wifi while traveling: Only visit sites with the HTTPS protocol • Log out when finished • Never send sensitive information • All of these are correct
To protect yourself from shoulder surfers: Use chairs that spin around so you can spot them • Leave your laptops/devices at home • Change passwords when finished traveling • None of these are correct
Engage screen locks on mobile devices: After 10 minutes of inactivity or less • After 5 minutes of inactivity or less • Never • After 7 minutes of inactivity or less

A102A—10 Personal and Physical Security
Badging is the act of: Hijacking a company's wifi • Using a fake or stolen ID to gain access • Making threats on someone else's behalf • None of these are correct
Piggybacking is the act of: Impersonating someone else • Using a fake or stolen ID • Entering a secure area on someone else's card swipe • Jumping over surveillance devices
A rogue device can be a: USB stick • Laptop • Wifi access point • All of these are correct
If you suspect impersonation: Do nothing—you're likely being paranoid • Ask to see credentials • Notify security if credentials can't be shown • Two of these are correct
A shoulder surfer: Steals laptop carriers off people's shoulders • Opens secure doors with a shoulder bump • Hovers nearby to steal sensitive information • All of these are correct
One of the easiest ways to protect company data is to: Work at home • Get off the grid • Empty your cache • Lock your computer screen when not in use

A102A—11 Vishing and SMiShing
These departments are frequent vishing targets: Customer Service • Maintenance • IT Help Desks • Two of these are correct
Vishers research targets using: Company websites • Professional networking platforms, like LinkedIn • Social media accounts • All of these are correct
A technique vishers use when they don't know the answer is to: Hang up • Use profanity • Mumble • None of these are correct
SMiShing texts are designed to get you to: Visit a malicious website • Download malware on your phone • Send gift cards • Two of these are correct
Be wary of texts that: Demand you respond immediately • Threaten dire consequences if you don't act • Request password resets to business email accounts • All of these are correct
Vishing and SMiShing attacks can harm a company's: Reputation • Customers • Logo • Two of these are correct

Barracuda
Your journey, secured.

A102A—12 Applications
When downloading apps: Avoid apps from file sharing sites • Choose apps with numerous reviews and numerous downloads • Download from reputable app stores… • All of these are correct
While not all free apps are malicious: Be cautious when using them • They can include extras that take up valuable storage space • They all contain spyware • Two of these are correct
Bundled apps: Can include troublesome add-ons that are hard to detect/remove • Are great because they give you more • All contain spyware • None of these are correct
Before you download any app: Make sure it's fun • Understand the conditions so you know what you're agreeing to • Make sure you're downloading from a file sharing site • None of these are correct
New software updates for your device: Should not be ignored • Address known security threats • Can protect against malicious apps • All of these are correct
Before downloading any app on a work device: Make sure it's been downloaded numerous times • Make sure it gets good reviews • Check with management • Make sure it's from a reputable source

A103A—1 Professional Networking
In business, placing trust in the wrong hands can lead to: Phishing attacks • Theft • No harm whatsoever • Two of these are correct
When meeting someone new at a business mixer: Verify their credentials later • Just assume he or she is legitimate • Call security • None of these are correct
If someone you meet takes a special interest in you: Don't talk to him or her • Ask yourself why • Lie about who you are and what you do • Create a diversion and leave
Suspicious new contacts may be looking for: Trade secrets to give them a competitive advantage • Information to spear phish you • Information to phish your company • All of these are correct
One of the most expensive cybercrimes occurred when: A fake deliverer stole a corporate jet • An imposter stole an oil company's passwords • The Ocean's 11 cast robbed the casino • All of these are correct
When networking online: Verify • Ask yourself why • Don't assume • All of these are correct

A103A—2 Bring Your Own Device (BYOD)
'BYOD' stands for: Build Your Own Device • Bring Your Own Device • Be Your Own Developer • Nothing, it's just random letters
It's okay to leave your device unattended when working in public: If it's only for a few minutes • If you're in a familiar place • It's never okay to leave a device unattended in public • None of these are correct
A strong password includes: Letters • Numbers • Special characters • All of these are correct
When free downloads secretly install malware it's called: Sideloading • Freeloading • Scamloading • Darkloading
A site that installs malware without any action on your part: Is doing a drive-by download • *Doesn't exist* • *Only effects certain PCs* • *None of these are correct*
Visiting sites with the following protocol will keep your device safe: HTTPEZ • HTTPS • HTTPAOK • HTTPSAFE

A103A—3 Public Wifi
Cyber criminals use public wifi to: Exploit vulnerable systems • Steal passwords and log-in information • Collect info that can be used to launch ransomware attacks • All of these are correct
You can verify the legitimacy of the public wifi network by: Making an educated guess • Asking an employee of the establishment offering the wifi • Doing nothing, there's no need • All of these are correct
Cyber criminals often mimic public wifi networks by: Using a name that's similar • Spelling their fake network differently • Doing nothing • Two of these are correct
Using a VPN: Encrypts your message • Makes it nearly impossible for cyber thieves to decode • Makes you a hard target • All of these are correct
When using public wifi: Don't allow your wifi to auto connect to pubic networks • Stay away from networks that don't require a password • Log out of accounts when finished • All of these are correct
Shoulder surfers take advantage of public wifi users by: Looking over their shoulders to steal sensitive information • Reaching over their shoulders… • Bumping them with their shoulders… • None of these

A103A—4 Internet of Things
The internet of things can include devices such as: Gaming systems • Smart TVs • Baby Monitors • All of these are correct
Cybercriminals can use internet-enabled devices to: Access your network • Launch ransomware attacks • Coordinate large-scale cyberattacks • All of these are correct
Buying brand-name devices from reputable vendors: Has no impact on internet security • Can ensure your device security features are current • Is good for your image • None of these are correct
The default password for any internet-enabled device: Is completely secure • Should be changed as soon as possible • Usually includes the programmer's initials • Can never be changed
You can secure your home network by: Staying off it entirely • Using a VPN • Using frightening emojis • All of these are correct
Phishing emails designed to compromise your network usually: Want you to click on something • Have spelling and grammar errors • Use an urgent tone • All of these are correct

A103A—5 Web Browsing and Work
Visiting an infected website while web browsing can result in: Malware downloads • Ransomware attacks • Phishing attacks • All of these are correct
Most companies have one of these to outline proper browsing conduct: Mission statement • Acceptable Use Policy • Employee Handbook • All of these are correct
If you don't know your company's web browsing policies, consult: Your manager• Human Resources • Acceptable Use Policy • All of these are correct
As a rule of thumb…: You can browse anywhere as long as it's private • If you wouldn't want your manager to know about it, don't visit • Anything is acceptable around work hours • Two of these are correct
Even a quick visit to an off-limits site can lead to: Unintentional malware downloads • Disciplinary action • A variety of risks • All of these are correct

A103A—6 Working From Home
Designating a space at home specifically for work: Lessens the chance work devices will be lost or stolen • Lets others know to stay away • Isn't important • Two of these are correct
If you must write passwords down: Use invisible ink • Insert random characters you know to avoid • Have a friend do it • None of these are correct
If your company uses security tokens: Keep them with you • Store them if you can't keep them with you • Refuse to use them • Two of these are correct
When you step away from your device: Lock your screen • Store it if you'll be away for a long time • Log out of all work related apps and networks • All of these are correct
You can safeguard your own network: By using a VPN • By never piggybacking on a neighbor's wifi • By making sure it's secure • All of these are correct
Company online security policies may be outlined: In an employee handbook • In an Acceptable Use Policy • By your manager • All of these are correct

A103A—7 Sensitive Data
Which of the following is generally not considered sensitive data: Account numbers • Customer ID numbers • Passwords • Your company name
Sensitive data can be used to commit all but the following crimes: Ransomware attacks • Reckless driving • Identity theft • Spear phishing attempts
You should treat sensitive data: The same as any other data • Like you don't care • As if it were your own personal data • All of these are correct
Sensitive data that's no longer useful to you: Should be thrown away • Isn't useful to anyone else • Could be useful to thieves • Should be sold on the dark web
Papers should be shredded using a: Scissors • Strip-cut shredder • Saber • Cross-cut shredder
The only way to guarantee data can't be retrieved fro a device is to: Destroy it • Overwrite it • Reformat it • Erase it

A103A—8 Clean Desk Policy
A clean desk policy can: Prevent cybercrime • Help meet compliance guidelines • Help meet green standards • All of these are correct
Post-it notes: Are okay to leave out • Should be discarded once info on them is stored safely or memorized • Should never be used, ever • None of these are correct
Leaving printed emails on your desk: Is encouraged because it's helpful • Can provide scammers with useful info • Is okay, if it's temporary, and they're cleared at day's end • Two of these are correct
If you leave USB drives out on your desk: They could be stolen or infected with malware • It's more convenient for you • Nothing bad could possibly happen • None of these are correct
Personal items, like pictures or certificates: Are generally okay to keep out • Can be seen by everyone, even scammers • Could provide the basis for a phishing attack • All or these are correct
Leaving a cup from your favorite coffee shop on your desk: Couldn't possibly lead to a scam • Will keep scammers away • Lets scammers know where to shoulder surf you • All of these are correct

A103A—9 Executive Targeting
CEOs and high-level executives are: Too important to be phished • Not worth phishing • Susceptible to phishing • Immune to phishing attempts
Scammers typically research executive targets: Using information found online • With high-tech spy satellites • By kidnapping them • None of these are correct
The executive profile scam: Is hacker myth • Is an appeal to ego • Can't hurt the company • Never works
The remember we met scam: Only happens in older companies • Exploits extensive executive networking • Never works • Two of these are correct
The from the CEO scam: Leverages the CEO's authority • Usually happens when the CEO is away • Has a sense of urgency • All or these are correct
This scam may include a picture of a CEO's colleague: Executive profile scam • Remember we met scam • From the CEO scam • None of these are correct

A103A—10 Catfishing
Catfishers exploit: Only the elderly • Foreigners • The human need to connect • Emojis
Catfishers seek: Money • Power • Control • All of these are correct
Sextortion is: Not a thing • A harmless way to enhance an online relationship • The act of blackmailing through threat of exposing intimate photos • Acceptable online behavior
A yes answer to the following suggests catfishing: Is the person too good to be true? • Is the relationship moving too fast? • Has the person physically met with me? • Two of these are correct
You can verify a profile picture source by: Asking the person where it came from • Uploading it to Google image search • Staring at it until it comes to you • It can't be done
The best way to protect yourself is to: Alert the authorities once you've been scammed • Trap the catfisher • Avoid being scammed in the first place • Quit the internet

Barracuda
Your journey, secured.

A103A—11 Phishing Careers
An email about an exciting job opening: Should be acted on immediately • Should be regarded carefully • Poses no threats • All of these are correct
Scammers mimic which job-related platforms: Monster • Indeed • LinkedIn • All of these and more
To verify if a job opportunity email is legitimate: Search the job site directly • Click the link to find out • Respond to the email • None of these are correct
Scammers target hiring managers: Because they're jealous • To get access to PII • Because they rely on email a lot • Two of these are correct
An email with the subject line 'my resume': Is automatically legitimate • Should be deleted immediately • Could harbor malicious links • Should be ignored
If you're part of a large hiring group: Route incoming applications through one computer • Don't hire anyone • You can't be scammed • Consider downsizing

A103A—12 GDPR (General Data Protection Regulations)
The GDPR replaces: Some of the existing data protection rules in the EU • All of the existing data protection rules in the EU • No rules whatsoever • None of these are correct
Companies outside the EU are: Not impacted by GDPR • Have a six-month grace period • Subject to GDPR rules if they trade with, collect or process data with EU firms • Are immune to GDPR
Which is not a right under GDPR: The right to be clearly informed • The right to rectification • The right to be forgotten • The right to remain silent
In the event of a serious data breach, the national supervisory authority must be notified: Within 24 hours • Within 48 hours • Within 72 hours • Immediately
Companies that carry out regular and systematic monitoring: Are immune from GDPR • Must maintain on-site servers • Must employ a Data Protection Officer • Are only located in the EU
Failure to comply with GDPR guidelines can lead to: Warnings and reprimands • Bans on data processing • Fines up to 20 million euros or four percent of annual global turnover • All of these are correct

A103A—13 PCI-DSS (Payment Card Information-Data Security Standards)
PCI-DSS were developed to protect Cardholders • Merchants • Cardholders and merchants • All of these are correct
PCI-DSS apply to any business: That facilitates payment card transactions • That stores cardholder data • That transmits or processes cardholder data • All of these are correct
When creating a secure network: It's okay to use factory defaults for system settings • It's not okay to use factory defaults for system settings • There are not set rules • None of these are correct
Why is a security awareness program important: Most data breaches involve some social engineering • It's really not that important • Most companies don't believe in them • None of these are correct
Enacting strong access control entails: Restricting access to data on need-to-know basis • Assigning unique IDs to those with computer access • Restricting physical access to data • All of these are correct
PCI-DSS guidelines are updated: Every two years • Every year • Every five years • As needed

A103A—14 Online Holiday Shopping
Many cyber attacks begin with: A phishing email in your spam folder • An ad on social media • A satellite radio ad • Two of these are correct
Email offers that don't reflect the company name in the address are: Likely fake • Nothing to worry about • A secret way to promote a great offer • Competitor tests
The following denotes a secure website: A padlock icon in the title bar • The "https" prefix • Green text in the title bar • All of these are correct
Making purchases on public wifi can: Show others you're a smart shopper • Expose credit card information and account numbers to hackers • Increase your credit score • None of these are correct
If using a shared computer to shop online: Be careful about germs • Share your credit card information, too • Browse in private mode to keep others from accessing your information • You've got nothing to fear
Scammers play on your emotions with: Deals that are too good to be true • Offers that expire extremely quickly • Ads that mimic big-name retailers • All of these are correct

A103A—15 Vocabulary of Information Security
An asset can be: Intellectual property • Physical property • A company's employees • All of these are correct
A threat is: An event that could bring harm to an organization • Nothing to worry about • A positive article about your business • Something that only exists in movies
The following is not an example of a threat actor: Hacktivist • Cybercriminal • State-sponsored attacker • Blogger
An attack can be driven by: Greed • Vengeance • Ego • All of these are correct
Risk is a concept that acknowledges: Undesired events may compromise an organization • Preparation eliminates undesireable events • Employees play no role… • All threats are technical in nature
A vulnerability can be: Technical • Human • Physical • All of these are correct

A103A—16 Data Classification
A data classification policy: Eliminates ambiguity • Clarifies what goes where • Dictates how information should be treated and protected • All of these are correct
Businesses adopt data classification policies because: Having one is a good idea • They are required to • They love to create extra work • Two of these are correct
Data should be classified in a manner that: Keeps things alphabetical • Creates questions and ambiguity • Makes for as little as work possible • Protects the organization, employees and customers/clients
Private sector policies may include these categories: Public • Internal • Interesting • Two of these are correct
Public sector policies may include these categories: Unclassified • Top Secret • Sensitive • All of these are correct
Data can be reclassified: True • False • Whenever • None of these are correct

A103A—17 Data Loss Prevention (DLP)
The first step in preventing data loss is to: Classify your data • Alphabetize your files • Invest in padlocks • Eliminate excess files
Businesses data lives: In file cabinets and desk drawers • On devices used by remote and third-party workers • In the cloud • All of these are correct
Nearly half of all data breaches: Originate internally by unwitting or malicious employees • Are annoying but harmless • Are impossible to prevent • Occur at night
Data is most vulnerable: During peak hours • When you're away from your desk • None of these are correct • When in motion
Your company's threat landscape is: A measure of physical safety • All of these are correct • The extent to which your data is at risk • Senior management's concern
An effective DLP: Creates a culture that understands the importance of protecting data • Involves only senior managers • Makes data available on a need to know only basis • Should never be modified

A103A—18 Data Breaches
The following is not a data breach category: Cyberattack • Human Error • Lost or Stolen Device • Gossip
Cyberattacks: Are usually tied to phishing • Can't harm your company • Only happen in movies • Target tech companies only
A lost or stolen device: Is not a risk to your data • Could lead to a data breach • Can't be hacked • None of these are correct
An inside job data breach can be motivated by: Financial reasons • Nationalistic reasons • Vengeance • All of these are correct
Your data breach response team: Should be made up of tech-savvy interns • Isn't important • Should be experienced • All of these are correct
By approaching them properly, data breaches can be: Eliminated completely • Managed and mitigated effectively • Dealt with once and forgotten • None of these are correct

A103A—19 Insider Threats
Insider threats can harm your company's: Brand • Financial position • Customer and shareholder confidence • All of these are correct
Careless users: Don't lock their computers when not in use • Leave written passwords on their desks • Are vigilant • Two of these are correct
Compromised users: May be victims of phishing attacks • May not now they're compromised until after the fact • May be targets of social engineers • All of these are correct
Malicious users: Are highly motivated • Can cover their tracks • May be motivated by greed, vengeance, ideology or other reasons • All of these are correct
Careless and compromised users can benefit from: Training • Reprimands • Isolation • Two of these are correct
A sign of a malicious user could be: Unexplained weight gain • Unexplained financial gain • Unexplained absences • None of these are correct

A103A—20 Access Control
Access control revolves around these concepts: Assignment, Authentication, Authorization • Assignment, Permission, Activity • Clearance, Compliance, Cohesion • Authentication, Authorization, Assessment
Authentication is: The act of verifying an individual is who they say they are • Only required of senior level employees • A subjective process • None of these are correct
An individual can be authenticated but may not be authorized: True • False
The oldest access control model in use is: Discretionary Access Control • Mandatory Access Control • Role-Based Access Control • Attribute Based Access Control
An access control model often used by government is: Discretionary Access Control • Mandatory Access Control • Role-Based Access Control • Attribute Based Access Control
The model your company chooses will be influenced by: The type of business you run • The information you use in your everyday business • Regulations and compliance standards • All of these are correct

A103A—21 Staffing and Cybersecurity
A new hire's access should be clarified with security and IT: Never • Once the new employee has settled in • Prior to starting • None of these are correct
The point of hire is an excellent time to: Emphasize the importance of a security-minded culture • Kick back and let new people worry about security • Determine access privileges • None of these are correct
Access privileges should be adjusted when employees are promoted or transferred: True • False
The first thing to do when an employee terminates is to: Inform IT and Security • Plan a going-away party • Conduct an exit audit • Collect access assets
After an employee terminates: You have nothing to be concerned about • Periodically review his/her accounts for access attempts • They may never return • None of these are correct
Any former employee who still has access: Is a potential data breach • Isn't a problem • Is an ally in the fight against cybercrime • All of these are correct

A103A—22 Account Takeover
Account takeover gives cybercriminals the power to: Send phishing emails from legitimate accounts • Impersonate colleagues • Target accounts within the company • All of these are correct
The first step in account takeover is: Network hacking • Infiltration • Monetization • External recon
Pivoting is not a key step in account takeover: True • False
The last step in account takeover is: External recon • Pivoting • Infiltration • Monetization
Lateral phishing: Is an offshoot of account takeover • Targets company vendors and partners • Can ruin brand reputations and relationships • All of these are correct
Avoiding account takeover and lateral phishing requires: A robust security culture • Employee training to identify phishing • The help of an information security awareness firm • All of these are correct

A103A—23 Spam
Spam is also referred to as: Negative email • There is no other reference • Junk mail or junk email • None of these are correct
Spam is any email that arrives in your email that you didn't solicit: True • False
Spam accounts for what percentage of all email traffic: Just over 50% • 10% • 30% • 90%
Spammers send millions of emails because: The more they send the more likely someone will respond • They like hitting the send button • No one knows why • All of these are correct
Malicious spam may contain: Dangerous downloadable files • Links to malicious websites • Links that can cause ransomware attacks if clicked • All of these are correct
The sheer volume of spam: Is good for business • Can't cause problems • Can overwhelm email networks • All of these are correct