



IronOak IT's

Security Awareness Training Catalog

Browse the Categories and Courses listed below. Each one is a self contained online training session that encourages you and your staff to be aware of and on the lookout for Scams and other risks in your workplace.

Categories Available (click to go to section)

1	Security Awareness	6	Web Security
2	Authentication	7	Malware
3	Email Phishing	8	Working Remotely
4	Data Protection	9	Mobile/Removable Devices
5	Social Engineering	10	Physical Security

Sequence

IronOak IT's recommended topics to start with

1	1	How to Protect Yourself Online	The guidance and techniques you need to stay safe in the modern digital landscape.
2	1	How to be a Human Firewall	Explains what a human firewall is and how they are essential to maintaining an organization's cybersecurity. Provides guidance and tips on how individuals can secure their personal devices.
3	1	Cyber Security 101	Explains what cyber security is and the importance of security human firewalls in keeping your company data safe.
4	1	Spoofing Attacks	Explains what spoofing is and the techniques used by criminals. It also includes how to help prevent becoming a victim of spoofing.
4	3	Email Security Explored	Explores the tactics cybercriminals use to exploit email communication and the dangers of sending emails to unintended recipients.
4	3	Social Media Phishing	Explains the tactics of phishing targets through the use of fake social media profiles and posts. Covers what steps you can take to stay safe from this form of cyber attack.
5	1	ChatGPT and AI Security	Short video on the topic of ChatGPT and AI security.
5	3	What Happens When You Click	Explores the potential consequences of clicking on a malicious link in a phishing mail, text or social media message.
5	3	Email Communication Standards	Covers the workplace standards which all employees should apply when using company email.
5	3	Malicious Attachments Standards	Explains how malicious attachments are delivered through email.
6	3	Phishing 101	Explains what phishing is, how to spot its red flags and how to protect yourself from phishing attacks.
7	2	Authentication Explored	Explores the history of user authentication and password hacking. Provides guidance on how to create a strong password and illustrates the benefits of password managers and multi-factor authentication.
8	2	Brute Force Attacks	Explains how hackers use brute force to crack passwords, and how to ensure your password is strong enough to defeat brute force.
9	2	Password Security Training	Explains the importance of having strong passwords. Categories: Passwords; Authentication; Multi-factor
10	2	Staying Safe with a Strong Password	Explains how to stay safe by using strong passwords.
11	2	Multi-factor Authentication 101	Explains what multi factor authentication is and the benefits of using it to secure your devices and online accounts. Categories: Authentication; Multi-factor Authentication.
12	2	Credential Stuffing	Hackers will try stolen login credentials on every account and platform they can in order to maximize the effectiveness of their attacks. Learn how to stay safe from credential stuffing attacks.
13	1	Selfie Spoofing	Explains how scammers can use our online photos to trick facial recognition technology and commit identity theft.
14	1	Incident Response 101	Explains the importance of responding quickly and effectively to security incidents.

Difficulty	Category	Name	Duration	Categories	Description
	1	Security Awareness			
		Security Awareness Explored	10:33	All Categories	Explores the cybersecurity landscape, explaining the tactics used by cybercriminals and how to protect yourself from cyber attacks.
Basic					
Basic		ChatGPT and AI Security	2:55	Web Security; Data Protection; Coding; Data	Short video on the topic of ChatGPT and AI security.
		QR Code Phishing	2:59	Phishing; Human Firewall; Malware Awareness; Spoofing.	Explains what QR code phishing is and why it's becoming a popular tool for cybercriminals. Provides guidance on how to protect yourself from QR code phishing.
Moderate					
		How to be a Human Firewall	6:32	Human Firewall; Social Engineering.	
Basic					Explains what a human firewall is and how they are essential to maintaining a secure environment. Provides guidance and tips on how individuals can secure their personal and corporate data.
		How to Protect Yourself Online	7:04	Human Firewall; Data Breaches; Incident Response; Social Media, Web Security; Wi-Fi Security.	
Basic					The guidance and techniques you need to stay safe in the modern digital world.
Basic		Incident Response 101	3:06	Incident Response.	Explains the importance of responding quickly and effectively to security incidents.
		Internet of Things (IoT) Security	4:13	Human Firewall; Malware Awareness; Ransomware; Spyware.	Explains why Internet of Things (IoT) security is so important, the challenges involved, and how to stay safe.
Moderate					
		Cyber Security 101	3:05	Human Firewall.	
Basic					Explains what cyber security is and the importance of security human factors.
		Shadow IT Threats	4:52	Access Control; Data Protection; Human Firewall; Web Security; WIFI Security.	
Moderate					Explains what Shadow IT is, typical examples, why it's used (benefits), and the risks it poses.
		Selfie Spoofing	3:01	Multi-factor Authentication; Social Engineering; Social Media; Spoofing.	
Basic					Explains how scammers can use our online photos to trick facial recognition systems.
		Spoofing Attacks	2:26	Spoofing; Social Engineering.	Explains what spoofing is and the techniques used by criminals. It also provides tips on how to avoid spoofing.
Basic					
		Zero Trust New!	3:12	Authentication, Data Protection, Privilege Access, Secure System Configuration.	
Moderate					Explores the main principles of Zero Trust security including the benefits and challenges.
		Regulatory Compliance vs AI Cybersecurity	3:37	Data Protection, GDPR, Vulnerability Assessments.	Global regulations are evolving to deal with the risks of AI driven cyber threats. Ensuring compliance and secure.
Moderate					
	2	Authentication			
		Authentication Explored	8:40	Data Protection; Passwords; Social Engineering; Authentication; Human Firewall;	
					Explores the history of user authentication and password hacking. Provides a deep dive into password security and illustrates the benefits of password managers and multi-factor authentication.
Basic		Brute Force Attacks	2:43	Authentication; Passwords.	Explains how hackers use brute force to crack passwords, and how to protect against brute force.
Basic					
		Password Security Training	1:13	Authentication; Human Firewall.	
Basic					Explains the importance of having strong passwords. Categories: Passwords, Authentication.
Basic		Staying Safe with a Strong Password	1:17	Passwords; Authentication; Multi-factor	Explains how to stay safe by using strong passwords.

Basic	Multi-factor Authentication 101		3:41	Passwords; Authentication; Multi-factor	Explains what multi factor authentication is and the benefits of using it. Categories: Authentication; Multi-factor Authentication.
Moderate		Secure Passwords	1:29	Access Control; Authentication.	Explains the importance of strong passwords and provides an easy method to create a strong password.
		Credential Stuffing	1:40	Authentication.	Hackers will try stolen login credentials on every account and platform to see if they work. Learn how to stay safe from credential stuffing with unique passwords.
Basic		Dictionary Attacks	1:15	Authentication; Passwords.	Explains the dictionary method of brute force password hacking, and how to stay safe from a dictionary attack.
	3	Email Phishing			
Basic		Email Security Explored	7:10	Email Security; Phishing; Spear Phishing; Whaling; CEO Fraud; Business Email Compromise; Spoofing.	Explores the tactics cybercriminals use to exploit email communications and how to protect against unintended recipients.
Moderate		Anatomy of a Whaling Attack	5:30	Email Security; CEO Fraud, Ransomware; Business Email Compromise; Spoofing.	Video telling the true story of a real world whaling cyber attack.
Moderate		CEO Fraud - Business Email Compromise	1:34	Business Email Compromise; Email Security; Spoofing.	Explains what CEO Fraud/BEC is and how to identify such scams.
Moderate		How to Protect Against Phishing	12:00	Phishing; Business Email Compromise; Vishing; Smishing.	Covers the tactics and techniques hackers use in phishing attacks, how to protect against them, and how to prevent future attacks.
Moderate		Identify Business Email Compromise	1:34	Business Email Compromise; CEO Fraud, Email Security; Phishing; Spear Phishing; Whaling.	Clues for Spotting Business Email Compromise Attacks Explains how to identify Business Email Compromise attacks.
Basic		Social Media Phishing	2:40	Phishing; Social Media; Social Engineering; Web Security.	Explains the tactics of phishing targets through the use of fake social media profiles and how you can take to stay safe from this form of cyber attack.
Moderate		Spear Phishing Standards	1:18	Phishing; Spear Phishing; Email Security; Social Engineering.	Explains how hackers use your habits and hobbies to carry out phishing attacks.
Basic		What Happens When You Click	3:05	Email Security; Phishing; Incident Response.	Explores the potential consequences of clicking on a malicious link in an email.
Moderate		Staying Safe From Qishing	1:30	Phishing; Mobile Device Security.	Explains what QR code phishing is and provides practical guidance on how to stay safe from QR code.
Moderate		Staying Safe From Vishing	1:30	Human Firewall; Mobile Device Security; Vishing.	Explains vishing with the use of an example and provides tips on how to stay safe from vishing.
Basic		Email Communication Standards	1:09	Email Security.	Covers the workplace standards which all employees should apply when communicating via email.
Basic		Malicious Attachments Standards	0:51	Malware Awareness; Email Security; Phishing; Spyware.	Explains how malicious attachments are delivered through email.
Basic		Phishing 101	0:03	Email Security; Phishing.	Explains what phishing is, how to spot its red flags and how to protect against it.
	4	Data Protection			
Basic		Data Protection Explored	7:47	Data Protection; Social Media; Web Security; Third Party Cookies; Access Control.	Explores the concept of data protection and why it's necessary. Covers various regulations which can help you protect your data.

Basic	5	Handling Confidential Data Standards	1:27	Data Protection; Human Firewall; Working Remotely; Email Security.	Explains how to handle confidential data from work.
Moderate		How to Protect Confidential Data	13:27	Data Protection; Access Control.	Illustrates the different types of confidential data and the secure practices to keep confidential data secure.
Basic		Staying Safe from Identity Theft	1:46	Data Protection; Social Engineering.	Explains how to stay safe from identity theft.
Basic		Workplace Confidentiality 101	3:44	Data Protection; Access Control.	Explains how to differentiate between confidential and public information and how to protect confidential information from loss or theft.
Moderate		Insider Threats		Authentication; Data Protection; Human Firewall; Physical Security; Social Engineering.	Explains what insider threats are including the different types of insider threats and how to report them anonymously.
Moderate		Personally Identifiable Information (PII)	4:19	Data Breaches; Data Protection; Social Engineering; Social Media; Web Security.	Explains what Personally Identifiable Information (PII) is and the measures to protect PII.
Advanced		SOC 2 Overview New!	1:58	Data Protection; Third Party Vendors.	Explains how the SOC 2 compliance framework is used to help ensure data is protected and handled in a secure manner.
Basic	5	Social Engineering			
Basic		Social Engineering Explored	8:04	Social Engineering; Passwords; Phishing; Clean Desk.	Explores the types of social engineering attacks cybercriminals use to gain unauthorized access.
Basic		Social Engineering 101	5:50	Social Engineering; Passwords	Explains how cybercriminals use social engineering to steal credentials and how to protect against social engineering attacks.
Moderate		Staying Safe from Smishing		Mobile Device Security; Phishing; Malware Awareness; Social Engineering; Smishing.	Explains how to stay safe from SMS phishing attacks.
Advanced		Advanced Persistent Threat (APT)	5:23	Phishing.	Explains what Advanced Persistent Threats are and the 3 stages of an APT attack.
Basic		Gift Card Scams	2:25	Authentication; Phishing; Physical Security; Social Engineering.	Explores some common scams associated with gift cards.
Moderate		AI Imposter Scams		Authentication; Phishing; Smishing; Spoofing; Social Engineering; Vishing. 3:50	Explains how Artificial Intelligence (AI) has made imposter scams more sophisticated and specifically examines phishing, voice cloning and deepfake scams and how to avoid being scammed.
Moderate		Deepfakes	2:02	Authentication; Phishing; Social Engineering.	Explains how images, videos or audio can be manipulated to exploit human emotions and perpetrate crime.
	6	Web Security	9:06	Web Security; Malware Awareness; HTTPS.	Covers the origins of the web, the current cyber threats users face, and how to protect yourself.
Basic		Staying Safe when Using Social Media	1:33	Social Media; Web Security; Social Engineering; Human Firewall.	Explains how to stay safe when using social media.
Basic		How to Browse the Web Securely	14:45	Web Security; Wi-Fi Security.	Explains the techniques and practices that can keep you safe while browsing the web.
Basic		Staying Safe when Banking Online	1:19	Web Security; Mobile Device Security; HTTPS; Human Firewall.	Explains how to stay safe when banking online.
Moderate		HTTP Standards	1:18	HTTPS; Web Security.	Explains the importance of using HTTPS protocol while browsing the web.
		Staying Safe from Pop-ups	1:47	HTTPS; Human Firewall; Malware Awareness; Web Security.	Explains the dangers associated with pop-ups.
Basic					

Moderate	6	Staying Safe from Man in the Middle Attacks	1:23	HTTPS; Human Firewall; Web Security.	Explains how to stay safe from man in the middle attacks.
		Cloud Security	4:11	Malware Awareness; Web Security.	Explains what cloud computing is, risks involved, responsibilities and how to stay safe in the cloud.
Moderate		Public WiFi 101	5:16	Web Security; Wi-Fi Security.	Covers the risks involved with using un-secure public WiFi and how to stay safe.
Basic					
	7	Malware Explored	9:15	Spyware; Malware Awareness; Email Security; Web Security; Security Updates; Ransomware.	Explores the different types of malware, how they are distributed and how to protect against them.
Basic		Keyloggers	2:00	Physical Security; Spyware; Removeable Media Security; Malware Awareness; Wi-Fi Security.	Keyloggers can track every keystroke entered into your computer or mobile device. This video provides an overview of the types of keyloggers being used by cybercriminals and how to protect your devices safe.
Moderate		Malware 101	4:02	Malware Awareness.	Explains the danger that malicious software poses to your personal devices and provides guidance on how to protect against malware attacks.
Basic					
		Ransomware	1:54	Email Security; Malware Awareness; Ransomware; Web Security.	Explains how to stay safe from ransomware.
Moderate		Mobile Banking Trojans New!	2:10	Malware Awareness; Spyware.	Explains how mobile banking trojans target sensitive data and compromise your financial information.
	8	Working Remotely Explored	7:05	Social Media; Wi-Fi Security; Web Security;	Explores the potential cybersecurity risks of remote working and provides best practices on the move.
Basic		Staying Safe working from Home or Mobile	1:21	Working Remotely; Wi-Fi Security; Mobile Device Security; Human Firewall.	Explains how to stay safe when working from home or on the move.
Basic		Staying Safe when Using Public Wi-Fi	1:39	Wi-Fi Security; Working Remotely; Human Firewall; Spoofing.	Explains how to stay safe when using public Wi-Fi.
Moderate		Home Wi-Fi Standards	1 :1 1	Authentication; Passwords; Physical Security; Web Security; Wi-Fi Security; Working Remotely.	Explains the importance of keeping Home Wi-Fi secure.
Basic					
	9	Mobile/Removable Devices Explored	6:15	Mobile Device Security; Working Remotely; Wi-Fi Security; Web Security; Physical Security; Social Engineering;	Explores the benefits and risks of using mobile devices and provides best practices for security.
Basic		Removable Media	1:38	Removeable Media Security; Pretexting; Social Engineering; Mobile Device Security.	Explains the importance of treating all external data storage devices as if they are untrusted.
Basic		Malicious USB	2:11	Malware Awareness; Mobile Device Security.	Explores the cyber crime tactic of juice jacking: infecting USB charging stations to hijack a targets device.
Moderate		Bluetooth Hijacking	2:35	Access Control; Mobile Device Security; Removable Media Security.	Covers the range of cyber attacks hackers commit on bluetooth devices and how to protect against them.
Moderate					

	10	Physical Security			
		Clean Desk	1:15	Clean Desk; Physical Security; Social Engineering.	Explains the importance of keeping confidential documents safe and
Basic					
Basic		Physical Security 101	3:58	Physical Security.	Explains how to secure physical files, devices and locations against c
Basic		Shoulder Surfing	1:21	Physical Security; Social Engineering.	Explains why not to share confidential information with people who ar
		USB Baiting		Access Control; Malware Awareness; Physical Security.	Explains how USB dropping or baiting can give a cybercriminal access
Moderate					indicate a drop attack and the security precautions you can take to pr