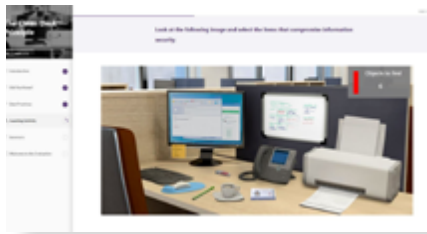




# Security Awareness Training Catalog

Enjoy the industry's highest-quality security awareness training experience with courses that distill everything your organizations needs to change end user behaviors and ensure your sensitive information is safeguarded from cyber criminals.



## Security Awareness Training

Enhance your training program with fun, engaging security awareness content that supports cyber security leaders and their behavior change initiatives. Enjoy multilingual, mobile responsive, and accessible content that makes security awareness training available to all users and promotes an inclusive atmosphere.

## Quizzes

Test end user knowledge retention from your security awareness courses with quizzes that utilize different question formats. Pull from a bank of pre-configured quiz questions or create your own to ensure your users are receiving the most pertinent testing material and response feedback possible.

# Security Awareness Library

## GENERAL KNOWLEDGE

### End User 6 to 10 min

- Access Control
- Bring Your Own Device (BYOD)
- Business Email Compromise
- Cloud Services
- Confidentiality on the Web
- Data Leakage
- Email
- Identity Theft
- Incident Reporting
- Information Classification
- Information Lifecycle
- Intellectual Property
- Introduction to Information Security
- Malware
- Mobile Devices
- Open Wi-Fi Risks
- Password
- Phishing
- Phishing Websites
- Physical Security
- Privacy
- Protecting Payment Card Data
- Protecting Your Home Computer
- Ransomware
- Responsible Use of the Internet
- Smartphones
- Social Engineering
- Social Networks
- The Clean Desk Principle
- Traveling Securely
- Unintentional Insider Threat
- Working Remotely

### 3D Cartoon Characters



### Real Action Characters



## CYBER GAME

### Serious Game 3 to 8 min

- BEC
- Cloud Based Services
- Data Transfer
- Ransomware
- Securing the Home Office
- Social Engineering
- Social Networks
- Strong Password
- ★ • Traveling Securely
- ★ • Working Remotely

### Cyber Challenge 3 min

- Cloud Services
- Email
- Incident Identification for Reporting
- Information Classification
- Information Lifecycle
- Malware
- Mobile Devices
- Phishing
- Privacy
- Protecting Your Home Office
- Ransomware
- Social Engineering
- Traveling Securely



### ★ RECENTLY ADDED

## RISK-BASED

### Microlearnings 3 to 4 min

- Access Control
- ★ • Application Account Compromise
- Applying the Clean Desk Principle
- Authentication Method
- ★ • Browser Compromise
- Business Email Compromised (BEC)
- C-Level Email Impersonation
- ★ • Computer Compromise
- Cyber Quiz
- ★ • Email Account Compromise
- Friend or Foe?
- Handling Unidentified Individuals
- ★ • Malicious Digital QR Codes
- ★ • Malicious Digital QR Codes
- Mass Market Phishing
- OAuth Consent Grant
- Phishing by Phone
- Policy Tips Around Sensitive Information
- Ransomware
- Report Message
- Risky USB
- Securing the Home Office Environment
- Sharing an Organization Computer
- Smishing
- Spear Phishing
- Teams Phishing
- Understanding App Consent Requests
- Unintentional Insider Threat
- Unsecured Sharing of Sensitive Documents
- Vishing
- Web Phishing
- Whaling

### Nanolearnings 2 to 3 min

- Anatomy of a Spear Phishing Attack
- Being Security Aware
- Cloud-Based Sharing
- Credential Theft
- Cyber Attack Detection
- Identity Theft - Example of an Attack
- Double Barrel Phishing Attack
- Insider Threat
- Phishing - Six Clues That Should Raise Your Suspicions
- Phishing Website
- Preventing Security Breaches
- Protecting Sensitive Information - Information Handling
- Ransomware
- Smishing
- Social Engineering
- Social Engineering via Email
- Social Networks
- Spear Phishing - The CEO Fraud
- Spoofing
- Stegosplit
- Vishing
- Web Conferences Risks
- Wi-Fi Security
- What is two-factor authentication

### Nanovideos 1 to 2 min

- ★ • Browser-in-the-browser Attack
- Credential Theft
- Cyber Fraud
- Employee Data Breach
- Financial Data Exposure
- ★ • Generative AI: What is it? Understanding the Risks
- Identity Theft
- Importance of Security Culture in the Organization
- Malicious Software
- Ransomware
- Website URL



### ★ RECENTLY ADDED

## ROLE-BASED

### Information Security Awareness for: 30 to 40 min

- **Executives**
  - Introduction to Information Security
  - Passwords
  - Phishing
  - Confidentiality on the Web
  - Mobile Devices
  - Data Leakage
  - Business Email Compromise
- **Finance**
  - Introduction to Information Security
  - Passwords
  - Phishing
  - Confidentiality on the Web
  - Protecting Payment Card Data
  - Data Leakage
- **Help Desk**
  - Introduction to Information Security
  - Passwords
  - Access Control
  - Social Engineering
  - Phishing
  - Incident Reporting
- **Human Resources**
  - Introduction to Information Security
  - Passwords
  - Phishing
  - Confidentiality on the Web
  - Privacy
  - Data Leakage
- **IT Administrators**
  - Network Security Overview
  - Common Network Attacks
  - Securing Networks
  - Securing Data Repositories
- **IT Developers**
  - Application Security Overview
  - Common Application Attacks
  - Secure Development
  - Cryptography Overview
  - Access Control
  - Information Lifecycle
- **IT Privileged Users**
  - Introduction to Information Security
  - Passwords
  - Access Control
  - Phishing
  - Malware
  - Ransomware
  - Unintentional Insider Threat
  - Incident Reporting
  - Working Remotely
- **Managers**
  - Security Challenges
  - Security Governance
  - Leading by Example

### OWASP 15 to 45 min

- **Open Web Application Security Project (OWASP)**

## COMPLIANCE & PRIVACY 15 to 45 min

- **CCPA Essentials**
- **GDPR Essentials**
- **HIPAA/HITECH**
- ★ - **Personal Information Protection and Electronic Documents Act**
- **Personal Information Protection in the Private Sector in Quebec**
  - Key aspects of the reform
  - Companies' obligations
  - Default protection of personal information
  - Individuals' rights, and how to protect their information
- **Personally Identifiable Information (PII)**
- **PCI DSS Awareness**
- **POPI Act**
- **Privacy Essentials**
  - The Protection of Personal Data
  - Collecting Personal Data
  - Privacy Principles
  - Privacy Breaches
- **Protected Health Information (PHI)**
- **Protected Health Information for Europe**
- **Security by Design (SBD)**

### ★ RECENTLY ADDED


# End User

Designed to strengthen the human element of your organization's information security, end user courses help participants understand best practices on a wide variety of cyber security topics. Each module includes interactive learning activities that reinforce those key messages.



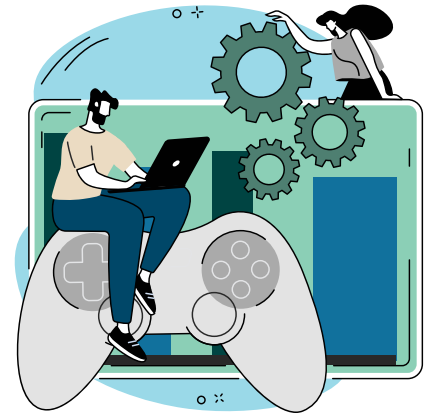
CODE	TOPIC	DESCRIPTION	DURATION
101	Introduction to Information Security	<ul style="list-style-type: none"> <li>Learn about information security and its overall importance</li> <li>Understand users' responsibilities in protecting the organization's information</li> </ul>	6 to 10 min
102	Information Classification	<ul style="list-style-type: none"> <li>Understand how and why organizations classify their information</li> <li>Practice classifying information according to levels of sensitivity</li> </ul>	
103	Information Lifecycle	<ul style="list-style-type: none"> <li>Understand the value of an organization's information</li> <li>Learn how to manage information correctly throughout its lifecycle</li> </ul>	
104	Intellectual Property	<ul style="list-style-type: none"> <li>Learn what is considered intellectual property</li> <li>Understand behaviors and situations that may violate intellectual property rights</li> </ul>	
105	Passwords	<ul style="list-style-type: none"> <li>Understand the importance of creating effective passwords</li> <li>Learn how to create a strong yet easy to remember password</li> </ul>	
106	Physical Security	<ul style="list-style-type: none"> <li>Understand why organizations must secure all their facilities and equipment</li> <li>Learn how common work areas can be protected from threats</li> </ul>	
108	Access Control	<ul style="list-style-type: none"> <li>Learn why organizations must control access to their networks and systems</li> <li>Understand the processes involved in granting and monitoring access</li> </ul>	
201	Email	<ul style="list-style-type: none"> <li>Recognize common email threats and email misuse</li> <li>Learn what precautions to take with incoming and outgoing emails</li> </ul>	
203	Confidentiality on the Web	<ul style="list-style-type: none"> <li>Understand the risks of inadvertently disclosing sensitive information on the web</li> <li>Understand and recognize potential online threats</li> </ul>	
205	Social Engineering	<ul style="list-style-type: none"> <li>Learn about social engineering and how it can fuel a variety of cyber threats</li> <li>Recognize common social engineering tactics used by cyber criminals</li> </ul>	
206	The Clean Desk Principle	<ul style="list-style-type: none"> <li>Recognize the importance of keeping unattended work areas clear of sensitive information</li> <li>Discover how to ensure the security of various documents and portable devices</li> </ul>	
207	Privacy	<ul style="list-style-type: none"> <li>Learn about privacy and related rights and obligations</li> <li>Identify what is considered personal information</li> </ul>	
208	Protecting Payment Card Data	<ul style="list-style-type: none"> <li>Understand an organization's obligation to protect payment card data</li> <li>Learn about the threats to payment card data</li> </ul>	


CODE	TOPIC	DESCRIPTION	DURATION
			 6 to 10 min
210	Phishing	<ul style="list-style-type: none"> <li>Learn about common phishing tactics and how they threaten information security</li> <li>Recognize and identify the features of a phishing message and website</li> </ul>	
211	The Bring Your Own Device (BYOD) Trend	<ul style="list-style-type: none"> <li>Understand the security issues related to the use of personal devices for business purposes</li> <li>Learn the strategies adopted by organizations to reduce BYOD-related risks</li> </ul>	
301	Malware	<ul style="list-style-type: none"> <li>Learn about the different types of malware</li> <li>Understand the human behaviors and technical factors involved in preventing malware infection</li> </ul>	
304	Responsible Use of the Internet at Work	<ul style="list-style-type: none"> <li>Learn how organizations can be impacted by inappropriate internet usage</li> <li>Understand what constitutes potentially harmful internet practices on corporate devices or accounts</li> </ul>	
306	Identity Theft	<ul style="list-style-type: none"> <li>Understand how identity theft affects victims and organizations</li> <li>Learn about common methods used to carry out identity theft</li> </ul>	
307	Social Networks	<ul style="list-style-type: none"> <li>Understand information confidentiality and information ownership issues related to social network usage</li> <li>Learn about the potential threats posed by fraudsters and cybercriminals</li> </ul>	
308	Working Remotely (Mobile Users)	<ul style="list-style-type: none"> <li>Learn about mobile users and working remotely</li> <li>Understand the risks related to user mobility</li> </ul>	
321	Mobile Devices	<ul style="list-style-type: none"> <li>Understand the vulnerabilities related to mobile devices</li> <li>Learn about preserving the security and integrity of mobile devices</li> </ul>	
322	Traveling Securely	<ul style="list-style-type: none"> <li>Preserve the security of information while traveling and working remotely</li> <li>Learn about the potential threats to information and technology used by traveling employees</li> </ul>	
323	Protecting Your Home Computer	<ul style="list-style-type: none"> <li>Learn the common methods used by cyber criminals to gain access to your information</li> <li>Recognize home environment vulnerabilities and risky internet activities</li> </ul>	
324	Ransomware	<ul style="list-style-type: none"> <li>Learn about ransomware and how it can negatively impact an organization</li> <li>Recognize how ransomware attacks are launched</li> </ul>	
325	Data Leakage	<ul style="list-style-type: none"> <li>Understand what constitutes a data leak and how it affects an organization</li> <li>Learn common internal and external data leaks causes</li> </ul>	
326	Business Email Compromise	<ul style="list-style-type: none"> <li>Understand what constitutes a business email compromise attack and how it is mounted</li> <li>Learn the common phishing-based scams used in such attacks</li> </ul>	
327	Unintentional Insider Threat	<ul style="list-style-type: none"> <li>Understand how users can unintentionally put the information security at risk</li> <li>Learn common user actions and behaviors that can lead to a security incident</li> </ul>	
328	Incident Reporting	<ul style="list-style-type: none"> <li>Understand the importance of detecting and handling security incidents promptly</li> <li>Learn how to identify and detect various types of security incidents</li> </ul>	
329	Phishing Websites	<ul style="list-style-type: none"> <li>Understand common tactics used by hackers to construct phishing websites</li> <li>Learn how to effectively safeguard your data from malicious sites</li> </ul>	

CODE	TOPIC	DESCRIPTION	DURATION
			 6 to 10 min
330	Open Wi-Fi Risks	<ul style="list-style-type: none"><li>• Understand the potential risks of connecting to an unsecured Wi-Fi network</li><li>• Learn best practices when it comes to sharing information of a network outside your home or office</li></ul>	
331	Cloud Services	<ul style="list-style-type: none"><li>• Recognize the potential vulnerabilities related to storing, sharing, and accessing cloud-based documents or systems</li><li>• Learn how to use cloud services securely with cyber-safe collaboration techniques</li></ul>	
506	Smartphones	<ul style="list-style-type: none"><li>• Learn about the information security risks related to smartphone usage</li><li>• Discover best practices for protecting information stored on smartphones</li></ul>	

# Serious Game

Serious Game modules put end users in the middle of immersive, exciting scenarios that test their cyber security knowledge in a gaming-style environment. Each module focuses on a specific topic as players collect points and race against the clock to complete interactive learning activities.




CODE	TOPIC	DESCRIPTION	DURATION  5 to 10 min
1	Strong Password	<ul style="list-style-type: none"> <li>Play as a special agent and race against the clock to secure sensitive information by relying on strong password expertise</li> </ul>	
2	Securing the Home Office	<ul style="list-style-type: none"> <li>Play as a special agent and race against the clock to secure a home office and keep confidential data out of the hands of hackers</li> </ul>	
3	Ransomware	<ul style="list-style-type: none"> <li>Play as a cybersecurity investigator trainee and race against the clock to identify the source of a ransomware attack before an organization's entire system is compromised</li> </ul>	
4	BEC	<ul style="list-style-type: none"> <li>Play as a cybersecurity investigator and examine different emails to identify all valid vendor payments and stop any potentially fraudulent payments due to Business Email Compromise</li> </ul>	
5	Cloud Based Services	<ul style="list-style-type: none"> <li>Play as a legendary cybersecurity analyst with the responsibility of identifying the source of the data leaks and putting a stop to it, before any more damage can be done</li> </ul>	
6	Data Transfer	<ul style="list-style-type: none"> <li>Play as an employee in the Business Operations department and finish your weekly to-do list by carefully managing your files and emails for a stress-free weekend, without risking being interrupted due to a major data breach</li> </ul>	
7	Social Engineering	<ul style="list-style-type: none"> <li>Take on two different roles, as you join the Red Team to design a mock cyberattack scenario and switch over to the Blue Team to select the appropriate defenses against cyber threats</li> </ul>	
8	Social Networks	<ul style="list-style-type: none"> <li>Play as a new junior Social Media Associate and complete your training by staying abreast of current affairs in your field and meeting with key managers</li> </ul>	
9	Traveling Securely	<ul style="list-style-type: none"> <li>Play as a world-renowned academic and apply best information security practices as you travel to attend a top-secret conference at the Secret Service's campus</li> </ul>	
10	Working Remotely	<ul style="list-style-type: none"> <li>Play as a student research assistant who needs to keep their data safe while commuting and working from the coffee shop to meet a tight deadline</li> </ul>	



# Cyber Challenge

Cyber challenges are engaging, gamified learning activities that test and reinforce fundamental security awareness knowledge on topics like phishing, email security, and more.



CODE	TOPIC	DESCRIPTION	DURATION  3 min
102	Information Classification	<ul style="list-style-type: none"> <li>Classify information based on its sensitivity levels so as to apply appropriate security measures</li> </ul>	
103	Information Lifecycle	<ul style="list-style-type: none"> <li>Plan for proper information disposal based on format and level of sensitivity</li> </ul>	
201	Email	<ul style="list-style-type: none"> <li>Describe and differentiate the email-based strategies fraudsters use to infiltrate organizational networks or access confidential information</li> </ul>	
205	Social Engineering	<ul style="list-style-type: none"> <li>Understand and protect yourself against cyberattacks that originate from deceptive social interactions</li> </ul>	
207	Privacy	<ul style="list-style-type: none"> <li>Identify personal information managed by your organization and handle it in compliance with security and privacy requirements</li> </ul>	
210	Phishing	<ul style="list-style-type: none"> <li>Recognize and identify the features of a phishing message and website</li> </ul>	
301	Malware	<ul style="list-style-type: none"> <li>Examine and identify ways in which malicious programs can infiltrate your electronic devices</li> </ul>	
321	Mobile Devices	<ul style="list-style-type: none"> <li>Adopt best practices when using mobile devices in order to protect your company and personal information</li> </ul>	
322	Traveling Securely	<ul style="list-style-type: none"> <li>Recognize and evaluate information security risks when traveling</li> </ul>	
323	Protecting Your Home Office	<ul style="list-style-type: none"> <li>Identify and eliminate information security vulnerabilities in your home office for safer remote work</li> </ul>	
324	Ransomware	<ul style="list-style-type: none"> <li>Understand the risks associated with ransomware attacks, and apply best practices to keep your organization's information safe</li> </ul>	
328	Incident Identification for Reporting	<ul style="list-style-type: none"> <li>Identify security incidents and report them to the appropriate instances in a timely manner to help protect your organization</li> </ul>	
331	Cloud Services	<ul style="list-style-type: none"> <li>Assess the risk level associated with various cloud computing practices to keep your and your organization's information safe</li> </ul>	

## RISK-BASED


# Microlearning

Built to increase employee knowledge retention and promote lasting behavioral change, microlearning modules feature concise training content. Each module targets specific risks and helps organizations meet productivity objectives.



CODE	TOPIC	DESCRIPTION	DURATION
3001	Vishing	<ul style="list-style-type: none"><li>Learn how to identify a voice message-based phishing attack and protect your confidential information</li></ul>	3 to 4 min
3002	Web Phishing	<ul style="list-style-type: none"><li>Understand how to verify a person's credentials before giving out personal information, as well as what constitutes a web phishing attack</li></ul>	
3003	Mass Market Phishing	<ul style="list-style-type: none"><li>Understand how to identify a real scam and protect their personal information, such as with a mass-market gift card scam</li></ul>	
3004	Spear Phishing	<ul style="list-style-type: none"><li>Learn how cybercriminals can operate and the motives behind potential attacks by taking on the pretend role of a hacker</li></ul>	
3005	Smishing	<ul style="list-style-type: none"><li>Recognize the common elements of a phishing attack received via text message and how to keep information safe</li></ul>	
3006	Whaling	<ul style="list-style-type: none"><li>Understand how senior executives can be easily compromised through targeted phishing scams called whaling</li></ul>	
3007	C-Level Email Impersonation	<ul style="list-style-type: none"><li>Discover how to identify a C-level email impersonation, a targeted attack that plays on the authority of the sender</li></ul>	
3008	Business Email Compromise (BEC)	<ul style="list-style-type: none"><li>Learn how to identify tricks cybercriminals use to extort money, as well as identify a compromised business email account</li></ul>	
3009	Handling Unidentified Individuals	<ul style="list-style-type: none"><li>Reinforce the best practices described in the Incident Reporting module by asking learners to make the correct decisions when faced with an unidentified person walking around the office</li></ul>	
3010	Ransomware	<ul style="list-style-type: none"><li>Learn how to react correctly to an unexpected email attachment and a computer infected with malware</li></ul>	
3011	Unintentional Insider Threat	<ul style="list-style-type: none"><li>Recognize how to act correctly when disposing of confidential documents by applying information security best practices</li></ul>	
3012	Friend or Foe?	<ul style="list-style-type: none"><li>Understand when and how to apply information security best practices when faced with an individual trying to access a restricted area</li></ul>	
3013	Access Control	<ul style="list-style-type: none"><li>Discover the consequences of lending computers to colleagues, as well as best practices related to this scenario</li></ul>	
3014	Applying the Clean Desk Principle	<ul style="list-style-type: none"><li>Understand what actions to take to reduce the risk of leaking sensitive information about a confidential project by combining best practices from different cyber security topics</li></ul>	

CODE	TOPIC	DESCRIPTION	DURATION
			 3 to 4 min
3015	Risky USB	<ul style="list-style-type: none"><li>Learn the dangers of plugging unknown USB devices on computers, which could lead to a malware infection or the installation of a dangerous program</li></ul>	
3016	Phishing by Phone	<ul style="list-style-type: none"><li>Learn how to keep sensitive information safe from cyber criminals who deploy phishing attempts via phone</li></ul>	
3017	Cyber Quiz	<ul style="list-style-type: none"><li>Compete against Isa from Terranova Security in a gameshow that tests fundamental cyber security knowledge</li></ul>	
3021	Report Message	<ul style="list-style-type: none"><li>Understand the importance of reporting a suspicious message and the appropriate steps to take in such a scenario</li></ul>	
3022	Understanding App Consent Requests	<ul style="list-style-type: none"><li>Learn the fundamentals of app consent grants and the best practices you should follow to ensure information is share securely and only with relevant individuals</li></ul>	
3023	Unsecured Sharing of Sensitive Documents	<ul style="list-style-type: none"><li>Discover the inherent vulnerabilities related to sharing sensitive documents and how to edit, store, access, and share confidential information securely</li></ul>	
3024	Sharing an Organization Computer	<ul style="list-style-type: none"><li>Discover the issues related to sharing a company computer with an unauthorized individual and how you can ensure usage policies are upheld at all times</li></ul>	
3025	Securing the Home Office Environment	<ul style="list-style-type: none"><li>Find out how to properly secure a home office environment by learning about precautions related to your computer and other devices, Wi-Fi network, and more</li></ul>	
3026	Policy Tips Around Sensitive Information	<ul style="list-style-type: none"><li>Learn how an organization can use policy tips to set boundaries for sensitive information, as well as steps you can take when you're confronted with a message that restricts information sharing</li></ul>	
3027	Teams Phishing	<ul style="list-style-type: none"><li>Learn how phishing attacks may be delivered via Microsoft Teams, as well as steps you can take to identify suspicious chat messages</li></ul>	
3028	OAuth Consent Grant	<ul style="list-style-type: none"><li>Find out how to protect yourself and your organization from OAuth, or third-party permission phishing attempts by installing applications from reputable sources and creating a unique username and password for each service</li></ul>	
3029	Authentication Method	<ul style="list-style-type: none"><li>Learn about the risks that come with relying on a third party to sign in to an online service, and identify the safest authentication method in a given context</li></ul>	
3030	Email Account Compromise	<ul style="list-style-type: none"><li>Find out how to detect signs of email account compromise, and leverage best practices to help prevent intrusions, such as enabling two-factor authentication</li></ul>	
3031	Application Account Compromise	<ul style="list-style-type: none"><li>Identify the signs that one of your application accounts has been compromised, including notifications of failed login attempts and changes made to your personal information without your knowledge</li></ul>	
3032	Browser Compromise	<ul style="list-style-type: none"><li>Learn to detect the signs that your browser has been compromised and is being used for malicious purposes, such as noticing toolbars or browser extensions that you did not install</li></ul>	
3033	Computer Compromise	<ul style="list-style-type: none"><li>Discover common signs that your computer has been infected by a virus, such as encountering unexpected pop-up advertisements and your device operating at a slower pace than usual</li></ul>	

CODE	TOPIC	DESCRIPTION	DURATION
3034	Malicious Digital QR Codes	<ul style="list-style-type: none"><li>Identify the signs that a digital QR code is unsafe to scan and apply best practices to mitigate risks associated with scanning a malicious QR code online</li></ul>	 3 to 4 min
3035	Malicious Printed QR Codes	<ul style="list-style-type: none"><li>Identify the signs that a printed QR code is unsafe to scan and apply best practices to mitigate risks associated with scanning a malicious QR code displayed in public spaces</li></ul>	


## RISK-BASED

# Nanolearning

Ideally suited for just-in-time training for phishing simulation clickers or as short standalone eLearning opportunities, nanolearning modules ensure end users understand specific cyber security fundamentals. Each module walks users through risks, consequences, and best practices related to a given topic.



CODE	TOPIC	DESCRIPTION	DURATION
2001	Ransomware	<ul style="list-style-type: none"><li>Learn how to identify malicious programs and what you should do if you think you received a ransomware email</li></ul>	2 to 3 min
2002	Vishing	<ul style="list-style-type: none"><li>Recognize the best practices related to detecting and safeguarding against phone scam tactics</li></ul>	
2003	Phishing – Six Clues	<ul style="list-style-type: none"><li>Ensure a strong understanding of the six core clues that you need to be aware of to identify a phishing threat</li></ul>	
2006	Protecting Sensitive Information	<ul style="list-style-type: none"><li>Learn how to identify, handle, and protect sensitive information securely</li></ul>	
2007	Cyber Attack Detection	<ul style="list-style-type: none"><li>Compete against Isa from Terranova Security in a gameshow that tests fundamental cyber security knowledge</li></ul>	
2008	Preventing Security Breaches	<ul style="list-style-type: none"><li>Understand how to reduce the risk of information security breaches</li></ul>	
2010	Wi-Fi Security	<ul style="list-style-type: none"><li>Learn about the risks of Wi-Fi security and about the precautions you can take</li></ul>	
2011	Identity Theft	<ul style="list-style-type: none"><li>Recognize the signs of common identity theft scams and how to avoid them</li></ul>	
2013	Social Engineering	<ul style="list-style-type: none"><li>Learn how to defend yourself against social engineering attacks</li></ul>	
2015	Being Security Aware	<ul style="list-style-type: none"><li>Understand what you can do every day to secure your home, belongings, computers, and other sensitive information</li></ul>	
2016	Spear Phishing CEO Fraud	<ul style="list-style-type: none"><li>Learn how CEO fraud works, and how to detect and avoid these types of threats</li></ul>	
2025	Phishing Website	<ul style="list-style-type: none"><li>Learn about how to identify a phishing website and its key features</li></ul>	
2026	Social Networks	<ul style="list-style-type: none"><li>Learn about the risks posed by criminals on social networks and how to protect personal information</li></ul>	
2035	Smishing	<ul style="list-style-type: none"><li>Understand how to identify and protect yourself against text-based threats</li></ul>	

CODE	TOPIC	DESCRIPTION	DURATION
			 2 to 3 min
2050	Anatomy of a Spear Phishing Attack	<ul style="list-style-type: none"><li>• Learn the steps and mechanisms used to create personalized or targeted phishing attacks</li></ul>	
2051	Insider Threats	<ul style="list-style-type: none"><li>• Discover the different types of insider threats and the precautions you can take</li></ul>	
2052	Social Engineering via Email	<ul style="list-style-type: none"><li>• Learn the steps and mechanisms used to leverage social engineering schemes via email</li></ul>	
2053	Spoofing	<ul style="list-style-type: none"><li>• Understand how hackers can spoof popular websites and common warning signs to watch for</li></ul>	
2054	Double Barrel Phishing Attack	<ul style="list-style-type: none"><li>• Learn the common tactics and red flags related to double barrel phishing attacks</li></ul>	
2055	Stegosplit	<ul style="list-style-type: none"><li>• Learn how digital images can be leveraged as key components of stegosplit attacks</li></ul>	
2056	Web Conferences Risks	<ul style="list-style-type: none"><li>• Understand the risks and common hacker tactics associated with web conferences</li></ul>	
2057	Cloud-Based Sharing	<ul style="list-style-type: none"><li>• Recognize the vulnerabilities related to cloud-based document and information sharing</li></ul>	
2058	What is two-factor authentication	<ul style="list-style-type: none"><li>• Learn about usage, format and reporting and the best practice associated with 2FA</li></ul>	

## RISK-BASED

# Nanovideo

Ideally suited for just-in-time training for phishing simulation clickers or as short standalone video-based eLearning, nanovideo modules showcases the risks, consequences, and best practices related to a given topic.



CODE	TOPIC	DESCRIPTION	DURATION
4	Ransomware	<ul style="list-style-type: none"><li>Learn the key warning signs of a ransomware threat, the consequences of downloading a ransomware file, and best practices to secure data against these attacks</li></ul>	1 to 2 min
5	Website URL	<ul style="list-style-type: none"><li>Understand how to safely view and identify malicious website URLs, and techniques cyber criminals can use to trick users into clicking</li></ul>	
6	Credential Theft	<ul style="list-style-type: none"><li>Understand the key warning signs and how to spot a credential theft threat, as well as how to safeguard sensitive data from credential theft attacks</li></ul>	
7	Identity Theft	<ul style="list-style-type: none"><li>Learn what types of data are targeted during identity theft attacks, how successful identity theft affects victims, and best practices that help users keep data safe</li></ul>	
8	Financial Data Exposure	<ul style="list-style-type: none"><li>Learn how financial data can be exposed in cyber attacks and how to avoid potential data leakage by sharing, storing, and accessing related information using cyber security best practices</li></ul>	
9	Cyber Fraud	<ul style="list-style-type: none"><li>Learn about the common tactics used by cyber criminals to commit cyber fraud, warning signs recipients should be aware of, and best practices to be aware of</li></ul>	
10	Employee Data Breach	<ul style="list-style-type: none"><li>Learn how employees can be targeted in data breaches, the hallmarks of messages hackers may deploy to trick recipients into divulging information, and best practices that help keep data safe</li></ul>	
11	Malicious Software	<ul style="list-style-type: none"><li>Understand how malicious software can compromise a computer or mobile device, the consequences of a resulting infection, and how to safeguard data from malware</li></ul>	
12	Importance of Security Culture in the Organization	<ul style="list-style-type: none"><li>Understand how having a strong security culture benefits an organization, and how one can help foster their organization's security culture</li></ul>	
13	Browser-in-the-browser Attack	<ul style="list-style-type: none"><li>Recognize common signs of browser-in-the-browser attack and learn about five ways to protect yourself and your organization</li></ul>	
14	Generative AI: What is it? Understanding the Risks	<ul style="list-style-type: none"><li>Understand what generative AI is, know the risks associated with its use, and follow best practices to keep yourself and your organization safe</li></ul>	

## ROLE-BASED

# Information Security Awareness for:

Constructed to appeal to various context-specific security awareness best practices, each role-based explores the cyber security roles and responsibilities related to different functions with an organization. Terranova Security offers role-based courses for professionals in finance, human resources, executives, and much more.



CODE	TOPIC	DESCRIPTION	DURATION
FIN	Finance	<ul style="list-style-type: none"><li>Learn what types of attacks frequently target professionals in the finance sector, how successful attacks can impact the organization, and how to safeguard against cyber criminals</li></ul>	30 to 40 min
GEST	Managers	<ul style="list-style-type: none"><li>Learn how managers can be targets of complex, multifaceted cyber threats, best practices for keeping data secure, and the role they play in fostering a cyber-aware culture</li></ul>	
HR	Human Resources	<ul style="list-style-type: none"><li>Understand the rules and regulations behind processing user data for HR purposes, what kinds of tactics hackers can use to try and steal data, and how to keep information safe</li></ul>	
TIA	IT Administrators	<ul style="list-style-type: none"><li>Learn the cyber threats commonly associated with IT administrators, and best practices related to keeping sensitive information, networks, and systems safe</li></ul>	
TID	IT Developers	<ul style="list-style-type: none"><li>Understand the building blocks behind secure IT development, how cyber criminals can exploit different vulnerabilities, and how developers can detect and avoid attacks</li></ul>	
EXEC	Executives	<ul style="list-style-type: none"><li>Provide senior executives and managers the information required to understand, assess, and defend against the most common cyber threats targeting them</li></ul>	
PRIT	IT Privileged Users	<ul style="list-style-type: none"><li>Provide IT privileged users with best practices and tools to identify, evaluate and protect themselves against cyber threats</li></ul>	
HD	Help Desk	<ul style="list-style-type: none"><li>Provide IT Help Desk employees with best practices and tools to identify, evaluate and protect themselves against cyber threats</li></ul>	

## ROLE-BASED

# OWASP

CODE	TOPIC	DESCRIPTION	DURATION
OWASP	Open Web Application Security Project (OWASP)	<ul style="list-style-type: none"><li>Learn about security threats and best practices related to OWASP and its processes</li></ul>	15 to 45 min



# Compliance & Privacy

Ensuring that all organizations can easily understand and comply with various data privacy regulations, this course provides high-quality training content and activities exploring key data protection trends.



CODE	TOPIC	DESCRIPTION	DURATION
801	Personally Identifiable Information (PII)	<ul style="list-style-type: none"><li>Learn everything you need to know about PII</li></ul>	15 to 45 min
803	Protected Health Information (PHI)	<ul style="list-style-type: none"><li>Learn everything you need to know about PHI and how organizations can ensure compliance</li></ul>	
818	GDPR Essentials	<ul style="list-style-type: none"><li>Learn GDPR essentials and how organizations can ensure compliance</li></ul>	
819	CCPA Essentials	<ul style="list-style-type: none"><li>Learn CCPA essentials and steps organizations must take to ensure compliance</li></ul>	
820 to 823	Privacy Essentials	<ul style="list-style-type: none"><li>Learn about general privacy issues and the positive impacts of enhanced awareness</li></ul>	
830 to 833	Personal information protection in the private sector in Quebec	<ul style="list-style-type: none"><li>Cover the legislative requirements for processing personal data in the private sector, within Quebec, following the recent adoption of Law 25</li></ul>	
840	Protected Health Information for Europe	<ul style="list-style-type: none"><li>Know the essential principles of the application of GDPR to health data, as well as related best practices for health professionals</li></ul>	
846 to 848	Personal Information Protection and Electronic Documents Act	<ul style="list-style-type: none"><li>Understand the key principles of Canada's Personal Information Protection and Electronic Documents Act, and learn how you can contribute to ensuring your organization's compliance</li></ul>	
HIPAA/HITECH	HIPAA/HITECH	<ul style="list-style-type: none"><li>Learn HIPAA/HITECH essentials and how to ensure compliance</li></ul>	
PCI	PCI DSS Awareness	<ul style="list-style-type: none"><li>Learn about PCI DSS and the positive impacts of enhanced awareness</li></ul>	
POPIA	POPI Act	<ul style="list-style-type: none"><li>Learn about the POPI Act to comply with its eight conditions and protect your South African clients' privacy</li></ul>	
SBD	Security by Design (SBD)	<ul style="list-style-type: none"><li>This course aims to familiarize users with best security practices at each stage of the development cycle of a project or IT service</li></ul>	

# Communication & Reinforcement Tools

**Increase employee engagement with a diverse suite of communication tools, with new assets added regularly**

## Newsletters

Send training updates and security best practice highlights directly to your users.

## Posters

Promote your training program with visuals you can tailor to match your brand.

## Wallpapers and Web Banners

Increase program engagement with vivid, thought-provoking digital messaging.

## Comics

Add a fun visual aspect to your training program with short comics depicting characters in relatable scenarios.

## Infographics

Share cyber security tips and best practices in a compact, engaging format that's perfect for social or intranets.

## Cyberpedia

Get everything you need to know about key cyber security topics in exhaustive, informative webpages.

## What is Videos

Send cyber security tips and best practices to users in bite-sized streaming video format.

***All communication tools are currently available in EN, FR-CA, FR-FR, and ES LATAM. For additional language support, please contact the Terranova Security Customer Success team.***

**GLOBAL PARTNER OF CHOICE IN SECURITY AWARENESS TRAINING**

**REQUEST A QUOTE**