

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

CYBER GAME

Serious Game 3 to 8 min

- BEC
- ★ • Cloud Based Services
- Ransomware
- Securing the Home Office
- Strong Passwordh

Cyber Challenge 3 min

- ★ • Email
- Phishing



★ RECENTLY ADDED

RISK-BASED

Microlearnings 3 to 4 min

- Access Control
- Applying the Clean Desk Principle
- Business Email Compromised (BEC)
- C-Level Email Impersonation
- Cyber Quiz
- Friend or Foe?
- Handling Unidentified Individuals
- Mass Market Phishing
- 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
- 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

- Cyber Fraud
- Employee Data Breach
- Financial Data Exposure
- Identity Theft
- Malicious Software
- Ransomware
- Website URL

ROLE-BASED

Information Security Awareness for: 30 to 40 min

- Executives
- Finance
- Human Resources
- IT Administrators
- IT Developers
- ★ • IT Privileged Users
- Managers

OWASP 15 to 45 min

- Open Web Application Security Project (OWASP)

COMPLIANCE & PRIVACY 15 to 45 min

- CCPA Essentials
- GDPR Essentials
- GDPR for Procurement Employees
- HIPAA/HITECH
- Personally Identifiable Information (PII)
- PCI DSS Awareness
- Privacy Essentials
- ★ • Personal information protection in the private sector in Quebec
- Protected Health Information (PHI)

GENERAL KNOWLEDGE


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

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

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


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

CODE	TOPIC	DESCRIPTION	DURATION  3 to 4 min
3015	Risky USB	<ul style="list-style-type: none">Learn the dangers of plugging unknown USB devices on computers, which could lead to a malware infection or the installation of a dangerous program	
3016	Phishing by Phone	<ul style="list-style-type: none">Learn how to keep sensitive information safe from cyber criminals who deploy phishing attempts via phone	
3017	Cyber Quiz	<ul style="list-style-type: none">Compete against Isa from Terranova Security in a gameshow that tests fundamental cyber security knowledge	
3021	Report Message	<ul style="list-style-type: none">Understand the importance of reporting a suspicious message and the appropriate steps to take in such a scenario	
3022	Understanding App Consent Requests	<ul style="list-style-type: none">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	
3023	Unsecured Sharing of Sensitive Documents	<ul style="list-style-type: none">Discover the inherent vulnerabilities related to sharing sensitive documents and how to edit, store, access, and share confidential information securely	
3024	Sharing an Organization Computer	<ul style="list-style-type: none">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	
3025	Securing the Home Office Environment	<ul style="list-style-type: none">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	
3026	Policy Tips Around Sensitive Information	<ul style="list-style-type: none">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	


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

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

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">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	1 to 2 min
5	Website URL	<ul style="list-style-type: none">Understand how to safely view and identify malicious website URLs, and techniques cyber criminals can use to trick users into clicking	
6	Credential Theft	<ul style="list-style-type: none">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	
7	Identity Theft	<ul style="list-style-type: none">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	
8	Financial Data Exposure	<ul style="list-style-type: none">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	
9	Cyber Fraud	<ul style="list-style-type: none">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	
10	Employee Data Breach	<ul style="list-style-type: none">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	
11	Malicious Software	<ul style="list-style-type: none">Understand how malicious software can compromise a computer or mobile device, the consequences of a resulting infection, and how to safeguard data from malware	

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">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	30 to 40 min
GEST	Managers	<ul style="list-style-type: none">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	
HR	Human Resources	<ul style="list-style-type: none">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	
TIA	IT Administrators	<ul style="list-style-type: none">Learn the cyber threats commonly associated with IT administrators, and best practices related to keeping sensitive information, networks, and systems safe	
TID	IT Developers	<ul style="list-style-type: none">Understand the building blocks behind secure IT development, how cyber criminals can exploit different vulnerabilities, and how developers can detect and avoid attacks	
EXEC	Executives	<ul style="list-style-type: none">Provide senior executives and managers the information required to understand, assess, and defend against the most common cyber threats targeting them	
PRIT	IT Privileged Users		

ROLE-BASED

OWASP

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

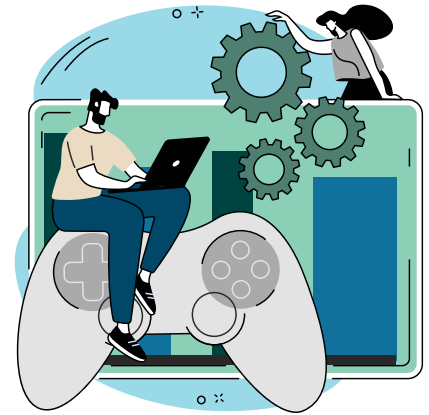


CODE	TOPIC	DESCRIPTION	DURATION
801	Personally Identifiable Information (PII)	<ul style="list-style-type: none"> Learn everything you need to know about PII 	15 to 45 min
803	Protected Health Information (PHI)	<ul style="list-style-type: none"> Learn everything you need to know about PHI and how organizations can ensure compliance 	
814	GDPR for Procurement Employees	<ul style="list-style-type: none"> Learn GDPR rules and regulations specific to procurement employees and their overall role in compliance 	
819	CCPA Essentials	<ul style="list-style-type: none"> Learn CCPA essentials and steps organizations must take to ensure compliance 	
820	Privacy Awareness	<ul style="list-style-type: none"> Learn about general privacy issues and the positive impacts of enhanced awareness 	
821	GDPR Essentials	<ul style="list-style-type: none"> Learn GDPR essentials and how organizations can ensure compliance 	
HIPAA/HITECH	HIPAA/HITECH	<ul style="list-style-type: none"> Learn HIPAA/HITECH essentials and how to ensure compliance 	
PCI	PCI DSS Awareness	<ul style="list-style-type: none"> Learn about PCI DSS and the positive impacts of enhanced awareness 	
820 to 823	Privacy Essentials	<ul style="list-style-type: none"> Learn about general privacy issues and the positive impacts of enhanced awareness 	
830 to 833	Personal information protection in the private sector in Quebec	<ul style="list-style-type: none"> Cover the legislative requirements for processing personal data in the private sector, within Quebec, following the recent adoption of Law 25 	

CYBER GAME

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
1	Strong Password	<ul style="list-style-type: none">Play as a special agent and race against the clock to secure sensitive information by relying on strong password expertise	5 to 10 min
2	Securing the Home Office	<ul style="list-style-type: none">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	
3	Ransomware	<ul style="list-style-type: none">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	
4	BEC	<ul style="list-style-type: none">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	
5	Cloud Based Services	<ul style="list-style-type: none">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	

CYBER GAME

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
210	Phishing	<ul style="list-style-type: none">Recognize and identify the features of a phishing message and website	 3 min
201	Email	<ul style="list-style-type: none">Recognize and identify all the ways fraudsters can infiltrate your network and keep your data safe	

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