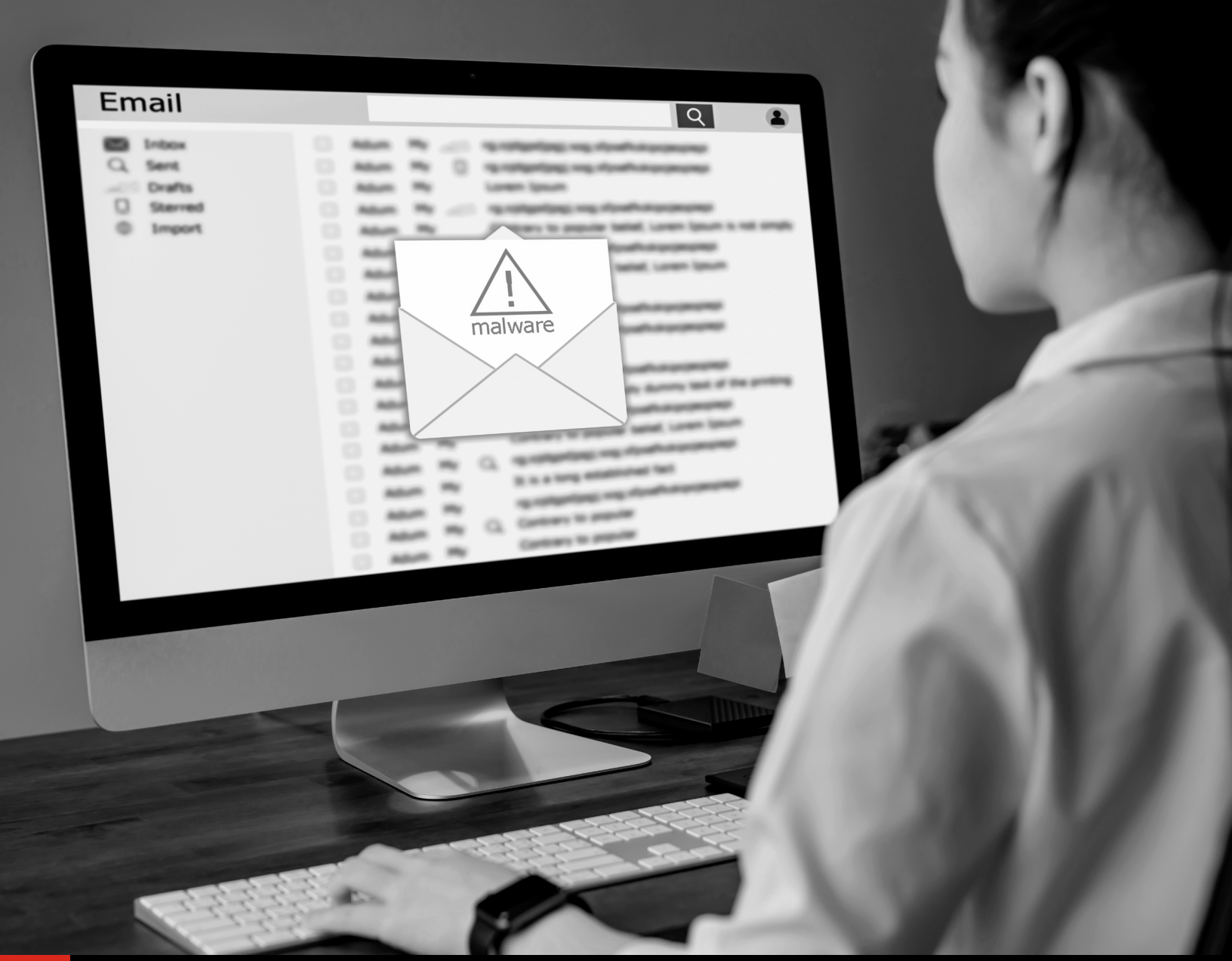


Security Awareness Training

CES' Security Awareness Training uses the world's largest security awareness training platform with simulated phishing attacks to teach employees to make smarter security decisions by understanding the mechanisms of spam, phishing, spear phishing, malware, ransom-ware, and social engineering threats.

Challenge

Regardless of how many employees you have, just ONE click from a single untrained team member can jeopardize your entire company. Every day staff at all levels are constantly exposed to sophisticated attacks that can ruin your company's bottom line—not to mention its reputation; Threats include...

- Malware (spyware, viruses, worms)
- Phishing (spear phishing, whaling, pharming, CEO phishing)
- Man-in-the-Middle (MitM)
- Denial-of-Service (DOS) or (TCP SYN flood attacks, teardrop attacks, smurf attacks, ping-of-death attacks, botnets)
- SQL Injections
- Zero-day exploit
- Password attacks
- Cross-site scripting
- Rootkits
- Internet of Things (IoT) attacks

Between the rise of hybrid work models and considering the current global climate, fortifying your business' security posture has become the dire first step to help reduce attacks and protect sensitive data. The real challenge? Ensuring every employee on your first front line of defense is equipped and trained with all the knowledge to identify/prevent breaches before they occur.

34%
Of businesses hit with malware take a week or more to recover their data

91%
Of successful data breaches start with a spear-phishing attack

$133,000
Average cost of the ransom-ware attack on businesses

$4.2 billion
Estimated 2020 losses due to 791,790 reported cybercrimes

$26 billion
Annual estimated losses due to Email scams

17%
2021 data breaches increaased compared with 2020

The Solution

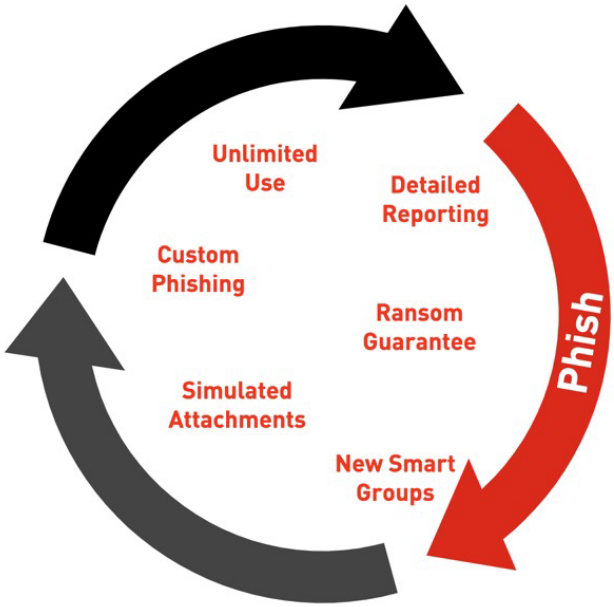
Staff can be the weakest and strongest link in an organization's security strategy. Precisely why CES' Security Awareness Training provides the detailed training to help build a highly functioning human firewall. Our scalable platform trains teams at all levels through:

- Baseline testing to assess the phish-prone percentage of users
- One of the largest libraries of security awareness training content
- Fully automated simulated phishing attack
- Thousands of customizable templates with unlimited usage
- Enterprise-strength reporting
- And more...

1 Train your users

2 Phish your users

3 See results



"Access the world's largest integrated platform for security awareness training with simulated phishing attacks with CES and KnowB4."

Through unlimited testing, detailed reporting, simulated attachments, and more teams help...

- Increase awareness of the many types of cyberattacks and how to recognize and report them
- Lower the number of phishing attempts by quickly identifying unauthorized access
- Analyze enterprise-strength reporting for further training and insight

Market Growth

$99.6B by 2027

12.2% CAGR 2021-2027

With 91% of successful data breaches starting with a single spear-phishing attack, train employees using intuitive programs that show them how to make smarter security decisions with simulated engineering attacks, insights into security gaps, and plans to strengthen your security posture.

Phish Alert Button
Do your users know what to do when they receive a suspicious email or attachment?

Domain Spoof Test
One of the first things hackers try is to see if they can spoof the email address of your CEO.

Email Exposure Check Pro
Have your users made you an easy target for spear phishing? Find out now!

Domain Doppelgänger
Find out if your domain has an evil twin with the Domain Doppelgänger tool.

Phishing Security Test
Did you know that 91% of successful data breaches started with a spear phishing attack?

Awareness Program Builder
Get your free customized Automated Security Awareness Program with calendar and PDF.

Ransomware Simulator Tool
Is your network effective in blocking ransomware and social engineering attacks?

Weak Password Test
Did you know 81% of hacking-related breaches used either stolen and/or weak passwords?

Benefits

CES' custom-built Security Awareness Training platforms are designed specifically for businesses' unique needs. Created "by admins for admins," we've constructed an easy-to-use solution to manage and avoid rising social engineering problems. Meanwhile, our Security Operations Center (SOC) combines a highly specialized cyder-security team with CES connectivity offerings to offer a proactive 24x7 managed service.

Benefits include...

- World-class customer assurance experience
- Advanced reporting and performance metrics
- Training specialized in all industry segments
- Single point of contact (SPOC) for service orders, installation, billing, management, etc.
- Implementation and project management using PMI, ITI, Agile, methodologies, and best practices
- Incident management and troubleshooting
- Proactive monitoring and support
- Access to engineers with certifications insecurity (CISA, CISM, CISSP, GCIH, CHFI, GCFA, Network (Cisco CCENT & CCNA), Microsoft MCSA, CompTIA A+, Network+, Server+.
- Additional layer of security: human awareness and vigilance
- Increased number of reported incidents
- Decreased number of cybersecurity incidents caused by human error and data misuse
- Identification of security risks and risk levels in the context of likelihood and impact
- Recommendations for mitigating risks and risk remediation plans
- Management, logging, and reporting systems that meet the reporting and compliance requirements
- 24x7 SOC support

Security Awarness Training
info@usclaro.com
833-992-5276

Claro
Enterprise Solutions