

## EMPLOYEE TRAINING IS CRITICAL TO SECURITY

Any organization with sensitive data is a target of opportunity for cybercriminals. Companies can address cyber security risks through technology, but did you know that employees can be your weakest link? As many as **86% of organizations have reported at least one person has clicked on a phishing link**, exposing their business to massive risk. ([Cisco's 2021 cybersecurity report](#))

Cybercriminals use social engineering tactics like "phishing" emails, telephone calls (vishing) from someone posing as a trustworthy source, or text messages (smishing) requesting quick action. These threat actors want sensitive information such as usernames, passwords, and financial information. Once obtained, the cybercriminals attempt to access or infect an employees computer with malicious software (malware), including viruses, ransomware, and spyware.

## PREPARE YOUR EMPLOYEES

Security Awareness Training administered by Systems Engineering can prepare your employees to recognize the latest cybercriminal techniques. With consistent training, your employees can help reduce the risk of a data breach or malware infection caused by social engineering. Enlisting a trusted partner to administer the program provides the resources and support for implementation and follow-up, including tracking and monitoring the program's effectiveness. To avoid compromising your cybersecurity posture, a trusted partner like Systems Engineering can provide a comprehensive and effective security awareness training program that helps ensure the security and privacy of your assets and information.



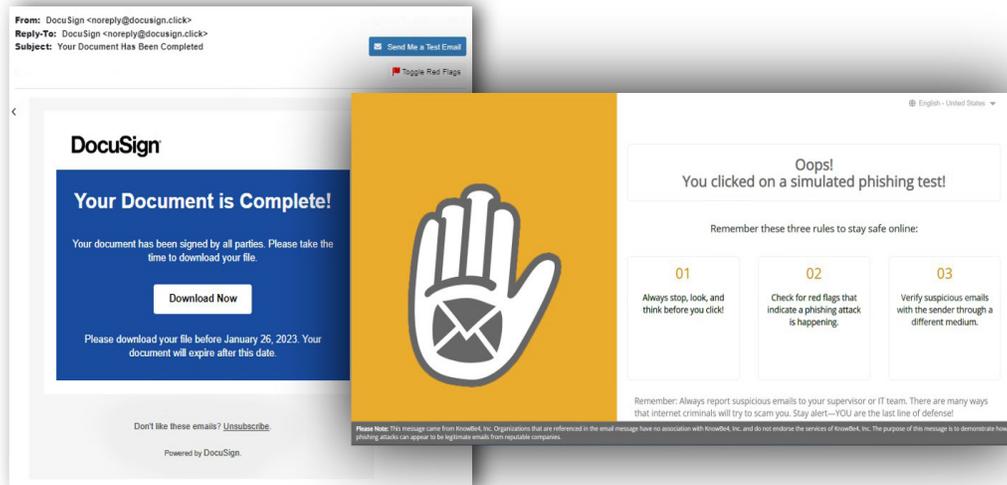
## MONTHLY TESTING & REPORTING

At various intervals, employees are sent simulated phishing emails. Those that engage with the fake email will be assigned a brief, mandatory training to refresh their skills on spotting and avoiding phishing attempts. Each month, we send progress reports to the main point-of-contact to monitor testing results and identify any potential issues. Then quarterly, we aim to have a discussion to review any trends, necessary updates, and answer any potential questions or concerns.

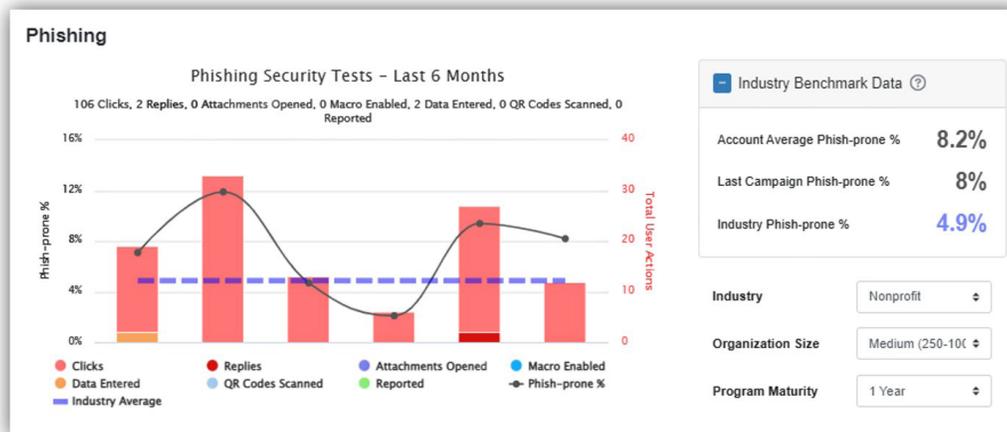
## FEATURES INCLUDED IN SECURITY AWARENESS TRAINING ADMINISTRATION

- **New Hire Compliance training.**
- **Annual Security Awareness compliance training.**
- **Streamlined user management for reporting accuracy.**
- **Monthly report of phishing test trends & user training status directly in your inbox.**
- **Quarterly review of historical trends in phishing compliance & industry averages.**

## EXAMPLE: SIMULATED PHISHING EMAIL



## EXAMPLE: PROGRESS AND TREND REPORTS



## EXAMPLE: MONTHLY TRAINING REPORT

Completed	In Progress	Not Started			
User	Groups	Location	Time Spent	Total Completed	Completed Past Due
user@company.com			00:26:01	1	0
user@company.com	Annual Compliance 2020, 2021 Compliance Training		00:56:24	1	0
user@company.com	Annual Compliance 2020, 2021 Compliance Training		00:51:50	1	0
user@company.com	Annual Compliance 2020, 2021 Compliance Training		01:34:10	3	0
user@company.com	2021 New Hires		01:03:01	1	0