INFOSEC IQ

Security Awareness Training Program Plan

MANUFACTURING

Program overview

Infosec is proud to introduce our security awareness training program built specifically for manufacturing companies. This twelve-month program will guide you to keep your organization safe from cybercriminals.

The program is centered around common cybersecurity issues and challenges specific to the manufacturing industry, covering essential cybersecurity topics recommended by the National Institute of Standards and Technology (NIST). Each training module is short (five to ten minutes long), straightforward and concise — giving your team the most efficient and effective training possible.

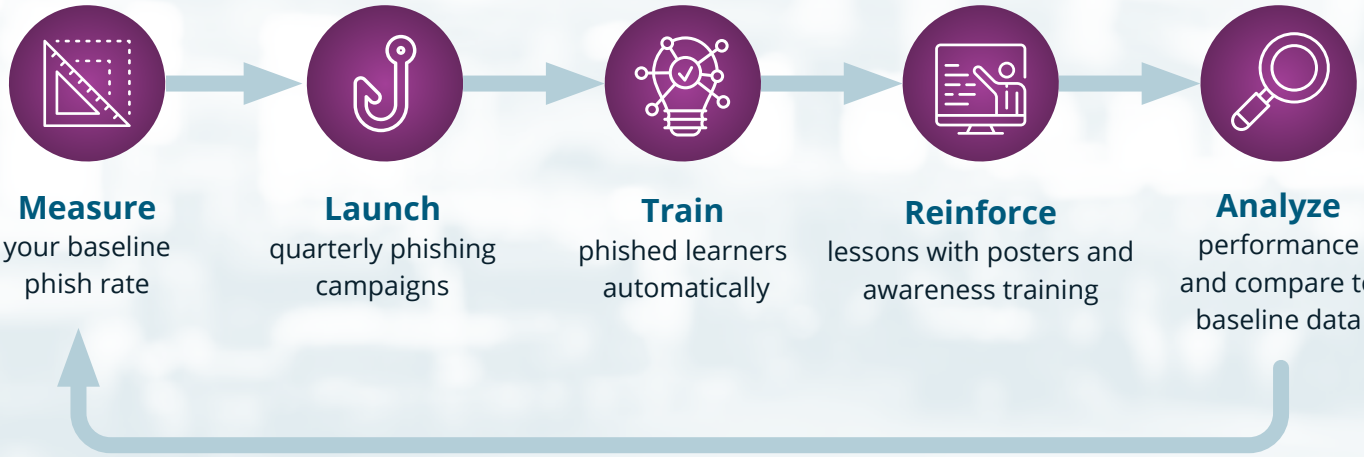
Translations

A global workforce requires a global training solution. That's why our core training series are available in 11 additional languages, including German, Portuguese (Brazilian), Dutch, Spanish (Latin America), Chinese Traditional, Chinese Simplified, French Canadian, French (EU), Italian, Japanese and Korean. 19 additional languages are available in the caption-only format: Russian, Polish, Vietnamese, Turkish, Romanian, Norwegian, Swedish, Hungarian, Hebrew, Finnish, Czech, Arabic, Indonesian, Thai, Spanish (EU), Hindi, Bengali, Danish and Malay.

Accessibility

Ensuring all your employees can enjoy the same high-quality training is important. That's why our training modules are built with accessibility in mind. Each module has Closed Captions (CC), an Audio Descriptive Track (ADT) and a downloadable PDF, allowing all employees to enjoy our awareness content in the format that fits them best.

How it works



What's included

Training topics

- CMMC 2.0
- Phishing
- Malware
- Physical Security
- IoT
- Social Engineering
- Multi-factor Authentication
- Ransomware
- Removable Media
- Insider Threats
- Intellectual Property
- Password Security
- Business Email Compromise (optional)

Phishing simulations

Watch employee behavior change with simulated phishing templates covering today's most common cybersecurity attacks. Each template provides the learner with immediate, in-the-moment training to help reinforce cybersecurity best practices.

Reinforcement tools

12 assessments

Test employee knowledge and lesson retention with assessment for each training topic.

12 posters

Hang posters in common areas and high traffic locations to extend your campaign communication offline.

12 infographics

Take a closer look at each cybersecurity topic with topical data and visual examples.

12 newsletters

Reinforce each cybersecurity topic with brief, conversational articles with real-life examples. Add the articles to your organization's newsletter, security portal or intranet.

Before you get started

Collect your existing employee-related risk data or measure your baseline metrics before launching your program. This data will serve as your quantitative starting point, allowing you to re-measure the same metrics throughout the course of your training program to quantify success and behavior change.

Baseline metrics may include:

- Phish rate
- Email report rate
- Training completion rates
- Security incidents
- Infected devices
- Lost/stolen devices & security badges
- Requests blocked via proxy server
- Security portal traffic
- Password strength data

To assess your organization's vulnerability to phishing attacks, we suggest initiating a baseline phishing campaign using our PhishSim template: Baseline Blind. This campaign will randomly send your employees simulated phishing tests, without the follow-up training, over a two-week period.

(Optional) Present your plan to stakeholders

Get buy-in from your organization's leadership with one of our pre-built stakeholder presentations and slide-by-slide talking points available now in our content library.

Put it all together

The following session structure includes our recommended training content and cadence. Although we recommend running the training program over the course of 12 months, you can adjust the frequency of training, session order and even the contents of the program to meet your organization's needs.

Series overview

Core Concepts (CC)

Breaks down complex cybersecurity issues into relatable and easy to understand concepts

Animated, straight-forward

Just the Facts (JTF)

Instructor-led training that takes security awareness head on

Live-action, instructor-led & straightforward

Need to Know (N2K)

Animated security awareness training that educates and entertains

Animated, fun & upbeat

Work Bytes (WB)

Security awareness training with a touch of magic

Live-action, humorous

Session calendar

QUARTER	MONTH	SESSION	TRAINING SERIES
QUARTER 1	MONTH 1	CMMC 2.0	CC
	MONTH 2	Phishing	CC JTF N2K WB
	MONTH 3	Malware	CC JTF N2K
QUARTER 2	MONTH 4	Physical Security	CC JTF N2K WB
	MONTH 5	IoT	CC JTF N2K WB
	MONTH 6	Social Engineering	CC JTF N2K WB
QUARTER 3	MONTH 7	Multi-factor Authentication	CC JTF N2K
	MONTH 8	Ransomware	CC JTF N2K
	MONTH 9	Removable Media	CC JTF N2K
QUARTER 4	MONTH 10	Insider Threats	CC JTF N2K
	MONTH 11	Intellectual Property	CC
	MONTH 12	Password Security	CC JTF N2K WB
	OPTIONAL	Business Email Compromise	CC JTF N2K WB

CC = Core Concepts JTF = Just the Facts N2K = Need to Know WB = Work Bytes

Session content

The outlined training sessions use content from our Core Concepts series. Each section will include the name of the course and the supplemental program resources. It's important to note that each course listed below includes one training module and its matching assessment.

Most of the below session topics are covered in our other series, which can be easily substituted to meet learner and organizational training preferences.

Month 1: CMMC 2.0

Explore the challenges of defense spending and government contracting with this look at the Cybersecurity Maturity Model Certification, or CMMC.

Course information

Core Concepts: CMMC 2.0

- Training module (7:13 min)
- Assessment (5 questions)

Program resources

N/A

Month 2: Phishing

Phishing catches people every day. Learn about phishing, how it works and how to avoid the phisher's net!

Course information

Core Concepts: Phishing

- Training module (7:20 min)
- Assessment (5 questions)

Program resources

Infographic: Just the Facts: Phishing
Poster: Just the Facts: Phishing
Newsletter: It's phishing season!

Month 3: Malware

Explore the ins and outs of malware with this module covering malware types, targets and delivery methods. Learn to detect and avoid dangerous malware attacks.

Course information

Core Concepts: Malware

- Training module (9:26 min)
- Assessment (6 questions)

Program resources

Infographic: Just the Facts: Malware
Poster: Just the Facts: Malware
Newsletter: The psychology of malware

Month 4: Physical Security

Close the door on hackers with this module on physical security in the workplace! Explore common physical security threats, tactics that intruders use and ways you can protect yourself and others.

Course information

Core Concepts: Physical Security

- Training module (4:18 min)
- Assessment (5 questions)

Program resources

Infographic: Ten tips for physical security
Poster: Just the Facts: Physical Security

Month 5: Internet of Things (IoT)

Could your toaster be dangerous? Explore the importance and the challenges of smart devices with this introduction to the Internet of Things.

Course information

Core Concepts: Internet of Things

- Training module (4:09 min)
- Assessment (5 questions)

Program resources

Infographic: Just the Facts: Internet of Things
Poster: Just the Facts: Internet of Things

Month 6: Social Engineering

Sometimes, all a hacker needs is the right word in the right place … and now they have your data! Explore the topic of social engineering and learn about the techniques and tricks that social engineers use to hack human behavior.

Course information

Core Concepts: Social Engineering

- Training module (6:43 min)
- Assessment (5 questions)

Program resources

Infographic: 10 ways to recognize and combat social engineering
Poster: Just the Facts: Social Engineering

Month 7: Multi-Factor Authentication

It takes more than passwords to keep your data safe. Dive into the world of multi-factor authentication and explore text tokens, biometrics and more.

Course information

Core Concepts: Multi-factor Authentication Assessment

- Training module (3:53 min)
- Assessment (5 questions)

Program resources

Infographic: Just the Facts: Multi-factor Authentication (MFA)
Poster: Just the Facts: Multi-factor Authentication (MFA)

Month 8: Ransomware

Don't let them lock up your data! Explore the growing threat of ransomware: what it is, how it works and how to protect yourself and your systems from it.

Course information

Core Concepts: Ransomware

- Training module (5:13 min)
- Assessment (5 questions)

Program resources

Infographic: Just the Facts: Phishing
Poster: Just the Facts: Phishing
Newsletter: It's phishing season!

Month 9: Removable Media

You can store a library's worth of data in a drive the size of a finger. But how do you protect that data? Could that drive possibly be a threat? Take a moment to learn about removable media.

Course information

Core Concepts: Removable Media

- Training module (4:50 min)
- Assessment (5 questions)

Program resources

Infographic: Just the Facts: Removable Media
Poster: Just the Facts: Removable Media

Month 10: Insider Threats

Sometimes the threat is coming from inside the building! Learn about insider threats: what they are, how they start and what you can do to stop them.

Course information

Core Concepts: Insider Threats

- Training module (7:26 min)
- Assessment (5 questions)

Program resources

Infographic: 10 tips to recognize and prevent insider threats
Poster: Just the Facts: Insider Threats

Month 11: Intellectual Property

What is intellectual property, and how does it affect you? Learn about IP: what it is, the different types, and why it should be protected.

Course information

Core Concepts: Intellectual Property

- Training module (3:44 min)
- Assessment (5 questions)

Program resources

N/A

Month 12: Password Security or

Your password protects you from hackers and scammers, but how strong is it? Learn how to create long, strong passwords that stop hackers in their tracks.

Course information

Core Concepts: Password Security

- Training module (4:25 min)
- Assessment (5 questions)

Program resources

Infographic: Just the Facts: Password Security
Poster: Just the Facts: Password Security
Newsletter: Creating the best password

(Optional) Business Email Compromise or BEC

What is Business Email Compromise, and what does it mean for you? Take a look at BEC and learn what you need to know about protecting yourself from this common cyberattack.

Course information

Core Concepts: Business Email Compromise

- Training module (5:15 min)
- Assessment (5 questions)

Program resources

Infographic: 9 BEC attack red flags
Poster: Just the Facts: Business Email Compromise

Phishing simulations

To enhance the security of your organization, we suggest conducting simulated phishing tests alongside your training courses. This will help you identify any gaps in employee awareness and evaluate the effectiveness of your current training programs.

To save you time, Infosec IQ provides pre-built automations that allow you to run recurring monthly or quarterly phishing campaigns using a selected template category. One of the commonly used categories is the Catch of the Week, which includes simulated phishing templates that reflect the current season or replicate a phishing attack that has been in the news recently.

If you're interested in launching a similar simulated phishing program, it can be done with just a few clicks! On the Infosec IQ PhishSim campaign page, we have campaign templates that are pre-configured with client-proven settings and relevant content that contributes to the overall success of a security awareness training program.

Our Catch of the Week template will randomly send each learner two templates at random each month. To launch this, simply select that template, review the settings and schedule your campaign. If needed, your Client Success Manager can also help configure this at any point during your program.

Employees who don't have a corporate email address

It is essential for all employees to be aware of cyber-threats, even if they do not have access to a corporate email address. These employees still have access to tools, machines and work environments where cyber-incidents are possible. By educating this group of employees on cybersecurity best practices, you'll help your organization:

- Safeguard valuable data
- Mitigate financial loss
- Maintain operational continuity
- Meet compliance regulations

How do you train them?

Since you won't be able to individually assign them the same training course and simulated phishing tests, we offer tools and resources that emphasize the same cybersecurity best practices covered in those trainings.

- **Display program resources.** Our infographics, posters and newsletters can be displayed in breakrooms, common meeting areas and on televisions.
- **Host a group training.** Trainers can invite employees to a group training session to watch videos and discuss cybersecurity. Each employee can sign in, and you can track who has completed the training for compliance purposes.
- **Looped training content.** Our modules' closed captions are available and can be transformed into a presentation. This presentation can be looped in breakrooms or common meeting spaces. We also have sample presentations available for download in our Infosec IQ content library.

Measuring campaign success

Measure early and often

After launching your program, pay close attention to employee engagement, training completion and phish rates and make necessary training adjustments. View campaign run reports or reference auto-reports to compare results to your baseline measurements and report progress to stakeholders. Use the Infosec IQ dashboard to easily view your training completion rates, compliance score for each cybersecurity topic and phishing performance over time.

Qualitative observations

What feedback did you receive from employees during the campaign? Did you see an increase in cybersecurity discussions with your team or among employees? Remember to record these observations. Qualitative data and quantitative metrics can help you be more effective when reporting results to your leadership. Culture change is a reflection of people's attitudes and behaviors, so be sure you're capturing the whole picture to report out and up.

Keep the momentum

This plan was designed to help you run a comprehensive, layered security awareness and anti-phishing program from start to finish. Still, the job of security awareness and training is never truly complete. Once your program is finished, keep your security awareness momentum going with new security awareness campaigns and training materials

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC