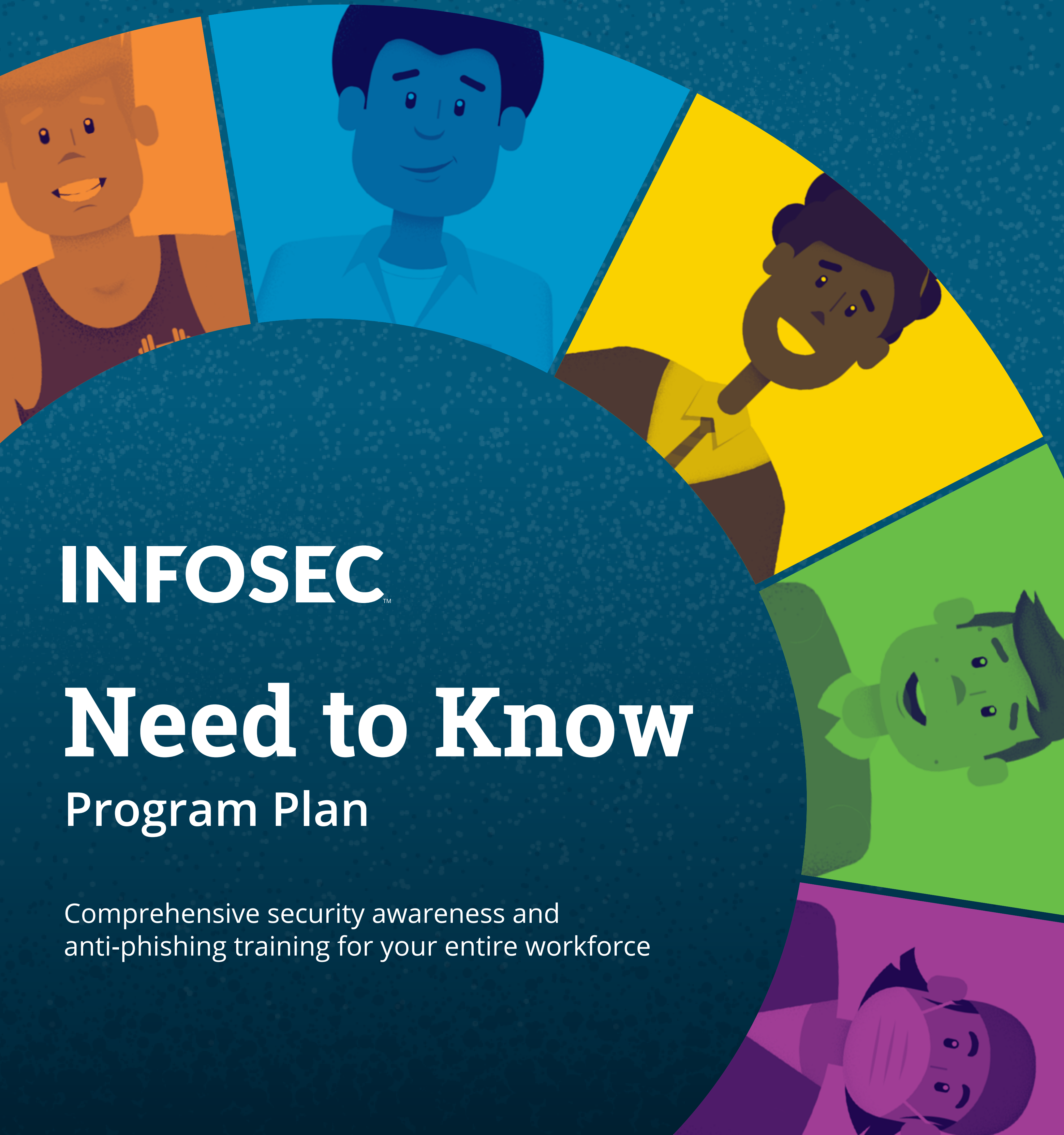


INFOSEC™

Need to Know

Program Plan

Comprehensive security awareness and anti-phishing training for your entire workforce

Security awareness program plan

The Need to Know Program Plan is your complete training curriculum and step-by-step guide to assembling a layered training program that will inspire your workforce to adopt effective cybersecurity habits.

Running a layered program works

Annual security awareness training might address compliance requirements, but it doesn't build cybersecurity into the culture of your organization. To motivate lasting cybersecurity behavior change, you need a security awareness program that covers every major cybersecurity topic and also keeps employees engaged all year.

Use this program plan to assemble a layered security awareness program that will inspire the behavior change your organization needs to stay cyber secure.

Step 1: Measure

To prove your training program is driving cybersecurity awareness and behavior change, first measure your organization's current risk level.

Security awareness training	Phishing simulations
Collect your existing risk data and any awareness or training metrics you already have before launching your program.	Record your organization's current phish rate and email reporting percentage or run a baseline phishing simulation to assess phishing risk.

Step 2: Introduce

Before diving into training, introduce your program and help employees understand what to expect in the coming months.

Deliver the Need to Know: Introduction module to preview upcoming training topics and introduce your employees to the series.	Announce your simulated phishing program and provide instructions for reporting suspicious emails using PhishNotify™.

Step 3: Prepare

Gather and review all training materials and decide how to display and deliver the supplemental resources.

Print posters and select infographics, digital banners and creative assets to reinforce your messaging.	Explore our pre-built phishing templates or create your own to simulate your organization's greatest threats.

Step 4: Launch

Select your training session, schedule your campaigns and launch the training session.

Deliver the session's training module and assessment. Hang the corresponding posters and publish digital assets on your intranet or security portal.	Send the session's simulated phishing campaign with the corresponding phishing education page.

Step 5: Analyze

How are your employees responding to training and phishing simulations and how does your data compare to your baseline metrics? Check your data and make changes if necessary.

Review your training completion rate and assessment scores and make adjustments as needed.	Review your phish rate and email report percentage and make adjustments as needed

Select your next training session and repeat

Demo Infosec IQ to see how it works!

What's included

Training campaign

11 Need to Know training modules
Assign themed training modules covering the cybersecurity topics recommended by NIST.

9 Assessments
Test employee knowledge and lesson retention with assessments for each core cybersecurity topic.

24 Campaign notification emails
Notify employees of new training exercises using the same imagery, tone and style as the Need to Know training modules.

(Optional) Additional training modules
Supplement Need to Know training with modules that cover specific industries, regulations or cybersecurity topics relevant to your organization.

Phishing simulations

27 Phishing templates
Test employee behavior change with phishing templates simulating the topics and attacks covered in the training materials.

9 Phishing education pages
Tie anti-phishing training to your awareness campaign with phishing education pages themed to the Need to Know modules.

Reinforcement tools

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

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

Digital banners
Keep cybersecurity top of mind by adding themed digital banners to your intranet homepage or company newsletter.

Character image files
Add the Need to Know characters and series imagery to new or existing training materials to reinforce messaging.

Stakeholder presentation
Notify employees of new training exercises using the same imagery, tone and style as the Need to Know training modules.

Download free resources

Download the free Need to Know training resources for a closer look at the training content included in this program plan.

Download

Access every training asset

Create a free Infosec IQ account for instant access to the entire Infosec IQ content library and preview all Need to Know training content.

Sign Up

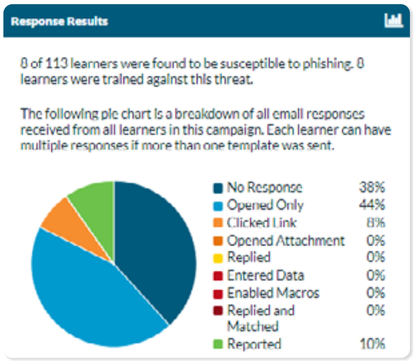
Before you get started

Measure your baseline metrics

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



Response Results

8 of 113 learners were found to be susceptible to phishing. 8 learners were trained against this threat.

The following pie chart is a breakdown of all email responses received from all learners in this campaign. Each learner can have multiple responses if more than one template was sent.

No Response	38%
Opened Only	44%
Clicked Link	8%
Opened Attachment	0%
Replied	0%
Entered Data	0%
Enabled Macros	0%
Replied and Matched	0%
Reported	10%

Don't know your organization's phish rate? Run a baseline phishing campaign!

Build a PhishSim™ campaign using the Baseline - Blind template battery to measure your organization's phishing susceptibility before launching your program.

(Optional) Present your plan to stakeholders

Get buy-in from your organization's leadership with our pre-built Need to Know stakeholder presentation and slide-by-slide talking points.

Put it all together

The following session structure includes our recommended training content and cadence. Although we recommend running the Need to Know 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.

MONTH 1	
Ready	Establish baseline metrics
Set	Prepare training resources and program cadence Posters Infographics Digital banners Program calendar
Go!	Launch training course and phishing campaign Training module Assessment Campaign notifications Phishing templates

QUARTER 1			QUARTER 2		
Month 2		Month 3	Month 4	Month 5	Month 6
Phishing simulations (ongoing)					
Phishing		Password security	Safe web browsing	Mobile security	Social engineering
QUARTER 3			QUARTER 4		
Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
Phishing simulations (ongoing)					
Malware	Physical security	Custom session	Working remotely	Removable media	Conclusion

Demo Infosec IQ to see how it works!

Session content

Introduction

Start at the beginning as Anthony introduces you to our plan for what's to come. Let's talk about hackers, cybersecurity and why it pays to keep a good head on your shoulders.

Need to Know: Introduction resources

AwareEd™

Training course
- Need to Know training module
- (Optional) Reporting Phishing Emails training module
- Campaign notifications

Downloadable resources
- Stakeholder presentation
- Email - PhishNotify Launch
- Character image files

Phishing

Learn how to spot the bait as Anthony guides his friend Cecil through the dangers of phishing. Is this actually a very exciting email from the boss, or is it just another hacker's trap?

Need to Know: Phishing resources

AwareEd

Training course
- Need to Know training module
- Assessment
- Campaign notifications

PhishSim

Phishing battery
- 3 phishing templates
- 1 phishing education page

Downloadable resources
- Poster
- Infographic
- Digital banners

Quick tip
Want to run your phishing simulation quarterly or annually rather than setting up a new campaign for each training topic? Add every Need to Know template battery to one PhishSim campaign and select the number of templates to send each learner over the course of the campaign.

Password security

A system is only as secure as its password. Join Anthony and Daryl as they face the challenges of creating a strong password...because security is not as easy as 1-2-3.

Need to Know: Password Security resources

AwareEd

Training course
- Need to Know training module
- Assessment
- Campaign notifications

PhishSim

Phishing battery
- 3 phishing templates
- 1 phishing education page

Downloadable resources
- Poster
- Infographic
- Digital banners

Demo Infosec IQ to see how it works!

Safe web browsing

It's a jungle in there. Explore the winding paths of the internet with Anthony and Cecil as they venture into thorny areas like fake browser warnings, HTTPS and dangerous URLs.

Need to Know: Safe Web Browsing resources

AwareEd	PhishSim	Downloadable resources
Training course » Need to Know training module » Assessment » Campaign notifications	**Phishing battery** » 3 phishing templates » 1 phishing education page	» Poster » Infographic » Digital banners

Mobile security

Join Anthony and Ivana as they explore the ups and downs of phone security. What is encryption? What kind of damage could a stolen phone do? Learn how to take security with you wherever you go.

Need to Know: Mobile Security resources

AwareEd	PhishSim	Downloadable resources
Training course » Need to Know training module » Assessment » Campaign notifications	**Phishing battery** » 3 phishing templates » 1 phishing education page	» Poster » Infographic » Digital banners

Social engineering

Some hackers don't need computers at all. Join Anthony and Erica in exploring the dirty business of social engineering — when all it takes is a lie to crack open a company.

Need to Know: Social Engineering resources

AwareEd	PhishSim	Downloadable resources
Training course » Need to Know training module » Assessment » Campaign notifications	**Phishing battery** » 3 phishing templates » 1 phishing education page	» Poster » Infographic » Digital banners

Demo Infosec IQ to see how it works!

Malware

Trojan horses, worms, RATs — There's a whole animal kingdom of malware out there. Join Anthony and Fiona as they explore the best ways to keep malware from migrating into your system.

Need to Know: Malware resources

AwareEd	PhishSim	Downloadable resources
Training course » Need to Know training module » Assessment » Campaign notifications	**Phishing battery** » 3 phishing templates » 1 phishing education page	» Poster » Infographic » Digital banners

Physical security

Anthony and his pal Harold talk physical security. Why do you secure everything (even the printer), and what could someone get by sneaking in? Here's how not to leave security out in the cold.

Need to Know: Physical Security resources

AwareEd	PhishSim	Downloadable resources
Training course » Need to Know training module » Assessment » Campaign notifications	**Phishing battery** » 3 phishing templates » 1 phishing education page	» Poster » Infographic » Digital banners

(Optional) Custom session

Do you have additional industry or compliance requirements, custom training or topics you'd like to cover in greater depth? Maybe you'd like to run a seasonal training session to boost awareness or address a common attack your organization faces. Customize this training session to fit the unique training requirements at your organization.

Search for training content by:

- Industry
- Regulation
- Role
- Training topic

Search Content Library

Demo Infosec IQ to see how it works!

Working remotely

Sometimes, trouble follows you home. Join in as Anthony and Ben explore the dangers of working remotely — from password cracks to malware attacks.

Need to Know: Working Remotely resources

AwareEd

Training course
- Need to Know training module
- Assessment
- Campaign notifications

PhishSim

Phishing battery
- 3 phishing templates
- 1 phishing education page

Downloadable resources

- Poster
- Infographic
- Digital banners

Removable media

Can a thumb drive topple a company? It's more likely than you think. Join Anthony and Harold as they check out the dangers of removable media — the good, the bait and the ugly.

Need to Know: Removable Media resources

AwareEd

Training course
- Need to Know training module
- Assessment
- Campaign notifications

PhishSim

Phishing battery
- 3 phishing templates
- 1 phishing education page

Downloadable resources

- Poster
- Infographic
- Digital banners

Conclusion

Take a moment to relax and review what you've learned as Anthony takes you through a few simple cybersecurity principles. Congratulations on completing your training!

Need to Know: Conclusion resources

AwareEd

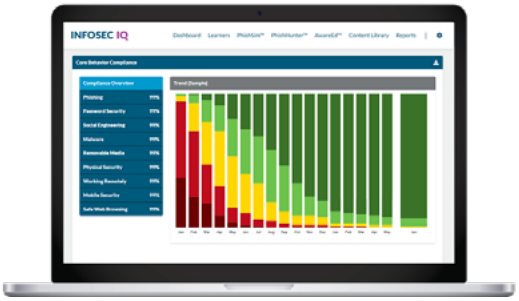
Training course
- Need to Know training module
- Campaign notifications

Demo Infosec IQ to see how it works!

Measuring campaign success

Measure early and often

After launching your program, pay close attention to employee engagement, training completion and phish rates and make training adjustments if necessary. 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 amongst employees? Remember to record these observations. Qualitative data, along with 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, but 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.

Download

WORKed Campaign Kit

Security is no laughing matter.
Wait...

Download

Marine Lowlifes Campaign Kit

Help your employees spot the most
dangerous phish lurking in their inbox

Download

Outsmart Them All

We made simulated phishing &
training easy

About Infosec

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We provide the best certification and skills development training for IT and security professionals, as well as employee security awareness training and phishing simulations. Learn more at infosecinstitute.com.

INFOSEC