FORTINET

GUIDE

Planning Your Security Awareness and Training Calendar

Since the threat landscape is changing quickly and becoming more malicious, security awareness programs need to evolve and ensure they are keeping pace with today's threats. Building a continuous learning cycle helps embed a culture of cyber awareness within an organization and ensures everyone is playing a role in protecting against threats.

Why Continuous Learning Is Important

It's important that training is continual and timely. German psychologist Hermann Ebbinghaus pioneered experimental studies of memory in the late 19th century, culminating with his discovery of "The Forgetting Curve." He found that if new information isn't applied, we'll forget about 75% of it after just six days.[1]

Although creating a large training module that checks the boxes for training compliance mandates and delivering it to employees once a year may be appealing, the resulting challenge is that security awareness will not be at the forefront of day-to-day operations.

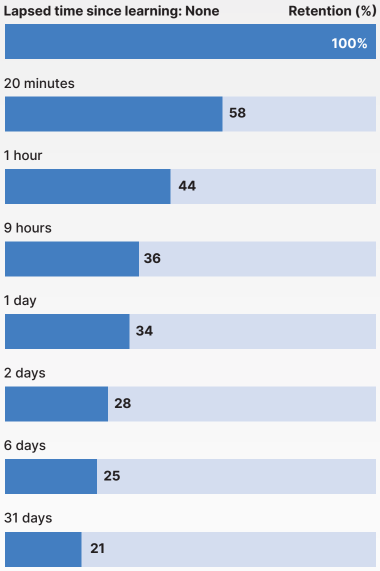
Building a culture that rewards the positive behaviors that an organization wants to see doesn't have to be complex and difficult to roll out. A little planning and creativity up front, with some check-ins during the year, can help ensure that you achieve organizational cybersecurity awareness throughout the year.

This document is meant as an idea generator, to help you build out your security awareness and training program calendar.

This step, building your calendar, comes after you have defined your program goals and strategy. For help with the first step, see the Defining Goals and Planning Your Security Awareness and Training Program Guide.

The Forgetting Curve

If new information isn't applied, we'll forget about 75% of it after just six days.



Source: Hermann Ebbinghaus

Security Awareness and Training Aligned to Employee Onboarding

When a new hire is onboarded into your organization, it's important that security awareness training is included in that onboarding process.

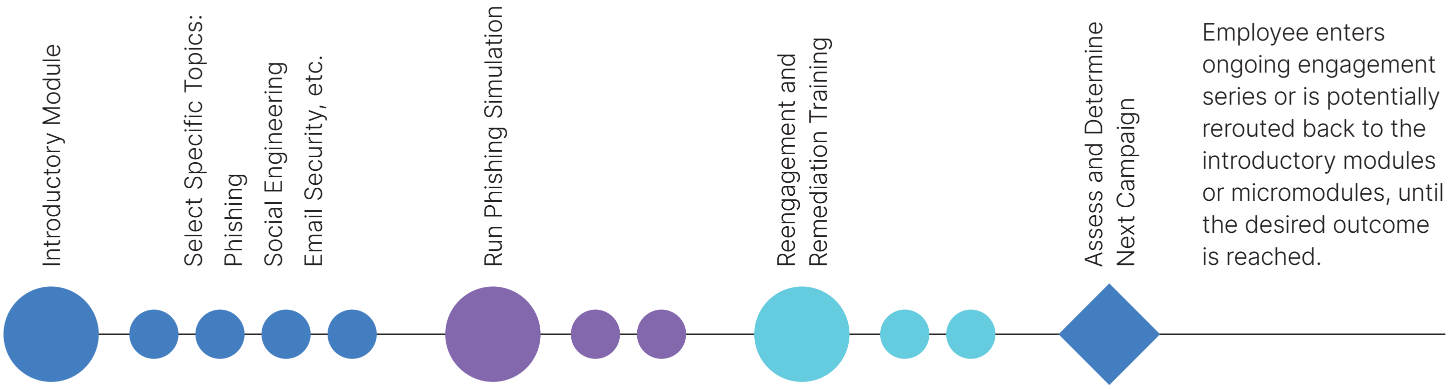
Presenting the essentials of good security behavior to new employees from day one helps to communicate to new hires that the organization values the security and protection of its data, networks, and users.

Start with an introductory training module that will teach learners how to describe the concept of information security awareness and training, and list actions that they can take to protect personal and company information.

From there, choose specific add-on modules that address the key areas that are important for your organization. For example, if you know that phishing is a particular concern for your organization, then you will want to select the phishing, social engineering, and email security modules as well. These can be bundled with the introductory module, or offered over a defined onboarding period.

You may then want to test your users by running phishing simulation exercises. From there, users who fall victim to the simulated phish can be redirected to additional micromodules to be reminded of key teachings.

Sample Onboarding



Employee enters ongoing engagement series or is potentially rerouted back to the introductory modules or micromodules, until the desired outcome is reached.

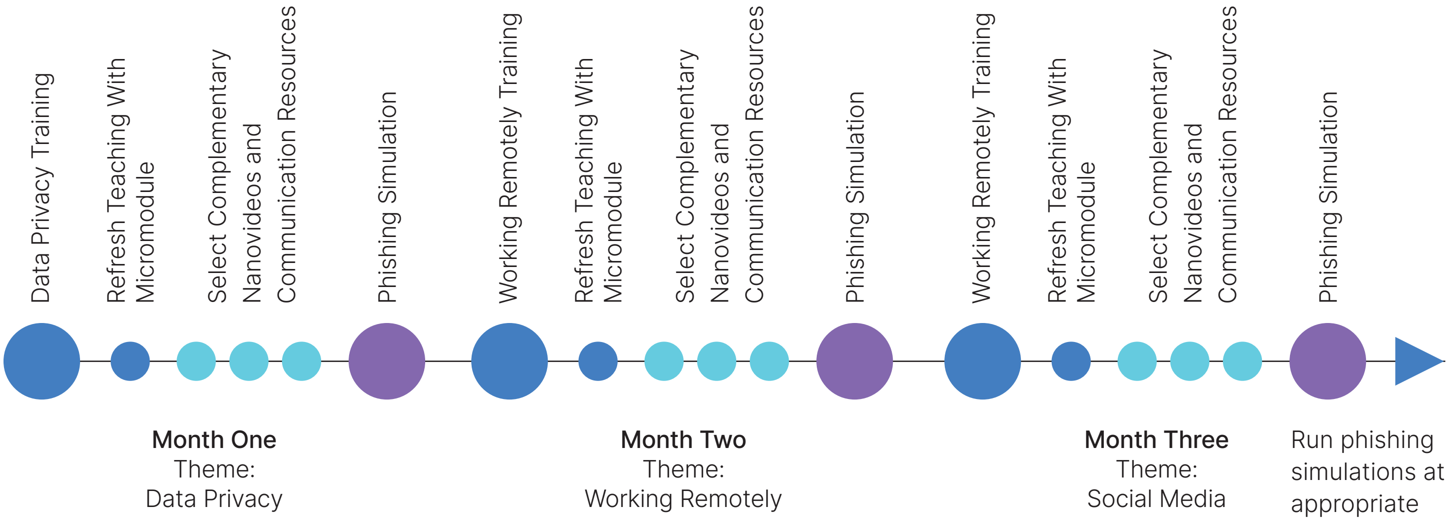
Figure 1: The time between training modules can be days or weeks, depending upon your onboarding process.

Build a Security Culture With Continuous Engagement

Throughout the year, it's good practice to check in with employees and provide quick learning opportunities that help foster a culture of security awareness. Sending fresh new content every month can help keep employees interested and engaged. It's important that training is appropriately targeted to the right role and that it is easy to digest, understand, and implement. Don't overwhelm your employees with large blocks of training in one sitting.

Below is an example campaign that can be broken down into one topic, or a collection of topics, to make a theme each month. Corresponding phishing simulations, tailgating at office door simulations, clean desk spot checks, and other types of tests can also be included, combined with the distribution of communication resources that help reinforce key teachings.

The following example takes place over a three-month period; however, the idea is that different themes would continue throughout the year. This is a snapshot of three months of a year-long program. If a monthly frequency is too much for your organization, consider building the same model, but space it out quarterly, rather than monthly.



Run phishing simulations at appropriate intervals that align with training plan.

Figure 2: Snapshot of three months of a year-long program.

Theme Your Awareness and Training to Different World and Regional Events and Holidays

Connecting your training and awareness to industry themes or holidays is a great way to reinforce key teachings. Your employees may also read about these topics in other publications or on social media, which helps to reinforce the importance of cybersecurity.

Here are some key holidays or noted observances that you can build a campaign around:

October Is Cybersecurity Awareness Month

Cybersecurity Awareness Month is an internationally recognized campaign held each October to help the public learn more about the importance of cybersecurity.

The National Institute of Standards and Technology provides some helpful tips, themes, and resources that you can use during this month.

Black Friday and the Holiday Season

Black Friday and Cyber Monday kick off the holiday shopping season in the U.S. In fact, 30% of all retail sales occur between Black Friday and Christmas Day. Since the advent of Cyber Monday, brick and mortar, and e-commerce stores alike, stand to generate a significant portion of their annual revenue over this shopping “holiday” weekend.

FortiGuard Labs has observed more and more scams involving counterfeit websites that appear to be legitimate e-commerce sites. These sites may look safe, but if you aren’t paying attention, they can steal your payment (and possibly payment information) through a purchase you thought was legitimate. Fake e-commerce sites are quickly becoming the latest threat to consumers, and they cover a wide range of products to lure potential buyers.

Run campaigns leading up to this time frame to educate your employees about this threat and how they can easily fall prey to these sites. Read more on the Fortinet blog.

Data Privacy Day/Data Protection Day

Data Privacy Day, or Data Protection Day, as it’s known in Europe, is recognized on January 28 every year. The purpose of the day is to raise awareness and promote privacy and data protection best practices.

This is a great time to focus your training on data security and privacy. If you’re looking for more resources about this topic, many regions and governments have specific in-country campaigns that organizations can leverage.

Tax Season

Cyber criminals are out in force, eager to prey on the stress and uncertainty surrounding the tax season. Attacks may take the form of phishing email campaigns or even phone calls from people claiming to be from the IRS or a collection agency. Stolen data may also equip these scammers with personal information, including Social Security numbers, making them appear legitimate even when they aren’t.

In addition to phishing campaigns implemented through a “spray and pray” model, which sends thousands of emails in the hopes that at least one person will fall victim, spear-phishing attacks are also on the rise.

Leading up to tax season, run campaigns to ensure that your employees don’t get distracted and fall prey to a more sophisticated spear-phishing attack. Spear-phishing attacks can be more difficult to detect than phishing attacks because they come in the form of targeted, personalized emails that often sound like they were sent from someone who knows the recipient.

Others:

- Voting
- Vacations
- Public Health Emergencies such as COVID-19 or vaccines
- States of Emergencies such as flooding, wildfires, and so on

Phishing Simulation

Phishing simulation is an important tool to reinforce security awareness and training focused on email-based threats such as phishing, spear phishing, impersonation, business email compromise, and email-based ransomware attacks.

Phishing simulation should be an ongoing activity (at least bimonthly) across your entire employee and user base, though topics and frequency may vary. In addition, phishing simulation or testing should incorporate training as well as learning content that activates at time of click of a test email.

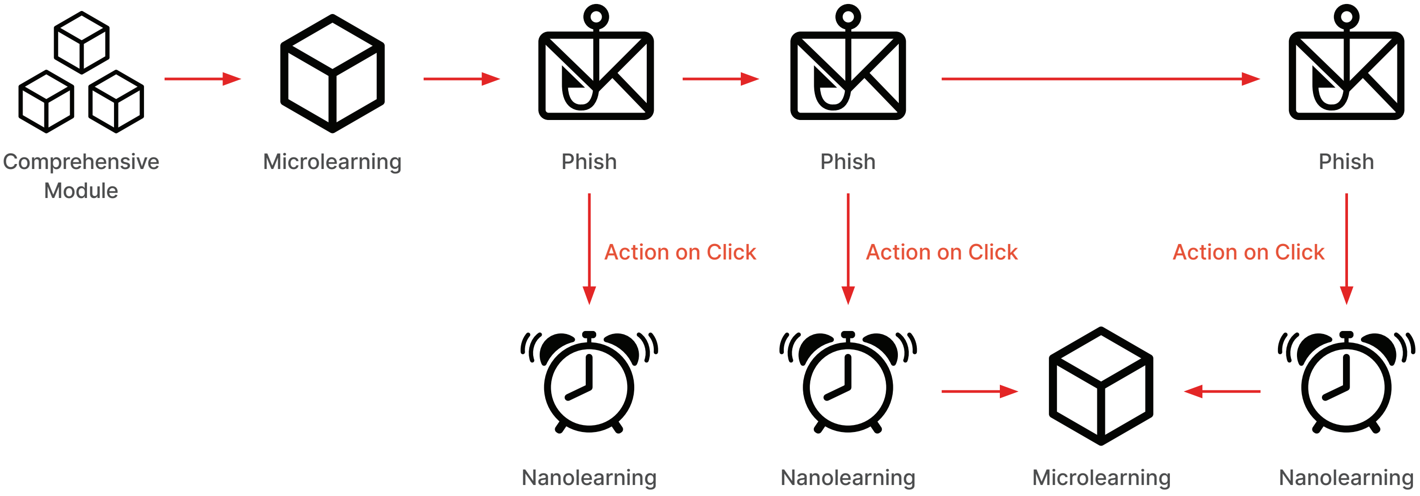


Figure 3: Constructing a phishing “campaign.”

When establishing a phishing simulation program, your approach shouldn’t necessarily be to test all employees against the same phishing emails. You will want to take a more thoughtful approach that considers a few vantage points, such as:

- Are there any groups or departments of employees or users that should be tested on lesser/greater frequency or on different topics or tactics?
- What tactics are most important to test on to reinforce vigilance against? For example, if your organization gets emails purportedly from the CEO wanting them to take action, you should test your employees and users on similar test emails.
- Be sure to perform testing that incorporates simulated suspicious links and attachments together and separately.
- Consider phishing topics that relate to activities only employees would seemingly be aware, such as announcements of payroll or human resources changes, password resets, training outage notices, internal newsletters, etc. Astute attackers will create emails that try to emulate these internal communications, so it’s good to test your employees and users against them too.
- Consider creating a specialized phishing testing and education campaign for repeat clickers or employees who consistently click on phishing test emails.

As your phishing testing campaigns end, be sure to review performance and other metrics to determine how your organization is doing. Your analysis should take on various vantage points, such as how your campaigns are performing, how individual groups are performing across campaigns, what tactics employees and users seem to be having trouble identifying successfully, and what individuals are serially clicking on tests and require additional training and reinforcement.

Don't Forget Remediation Training

Make remediation training positive, not punitive.

As part of a continuous training and awareness life cycle, you can check in with employees to determine if what they are being taught is helping and is changing behaviors. The check-ins can be signaled by several actions:

- Poor performance on quizzes and assessments
- Accidentally clicking on phishing simulation emails
- Data or privacy breaches
- Poor performance on other types of tests, such as spot desk checks, tailgating simulations, and so on

If employees perform poorly on any of these items, then microvideos or nanovideos are great assets to send targeted reminders of what to do in each applicable scenario. It's important that remediation training is not presented as teaching a lesson, which can be perceived as a negative form of reinforcement. Instead, remediation training should be supportive and uplifting, to create engagement with employees. The goal is to reeducate and reinforce key teachings, not administer punishment.

"Even in the midst of binding time constraints, look for opportunities to revisit, review, and restate."[2]

About the Fortinet Security Awareness and Training Service

The Fortinet Security Awareness and Training Service brings timely and current awareness of today's cybersecurity threats and helps make an organization's employees cyber aware and able to recognize and help stop attacks. Purpose built to address the needs of SMBs and enterprises, the service provides a turnkey offering that includes an intuitive administrator interface for campaign building, monitoring, and reporting, end-user learning modules, reinforcement micromodules or nanomodules, and awareness resources.

Learn more

[1] Steve Glaveski, Where Companies Go Wrong with Learning and Development, Harvard Business Review, October 2, 2019.

[2] Robert F. Bruner, Repetition is the First Principle of All Learning, ResearchGate, August 2001.

December 30, 2021 9:59 AM

1376807-0-0-EN