FCI

CYBERSECURITY AWARENESS

CYBERSECURITY AWARENESS TRAINING

Train your people before attackers do.

Phishing simulations and cybersecurity awareness training are essential for testing employee awareness and strengthening security practices — but most solutions come with operational headaches. Microsoft 365 solves this natively.

30+
years serving financial services

40,000+
endpoints under management

$5
per user/month (Defender Plan 2)

THE CHALLENGE

Most phishing simulation tools create more problems than they solve.

Cybersecurity Awareness Training and Phishing Campaigns are essential for testing employee awareness and strengthening cybersecurity practices, but they often come with operational challenges and risks. With most solutions, firms conducting phishing simulations must whitelist specific domain names in their email systems to ensure that simulated phishing emails reach users. This process can be complex and risky, as improperly configured email filters could expose the organization to actual phishing attacks.

Most third-party phishing software options are legacy systems that are not user-friendly or easy to configure. To avoid whitelisting, some newer tools require integration with Microsoft 365, which introduces additional risks and complexity, making them less appealing for modern security needs.

DOMAIN WHITELISTING RISK

Improperly configured email filters can expose the organization to real phishing attacks.

LEGACY SYSTEMS

Most third-party options are outdated, not user-friendly, and difficult to configure.

INTEGRATION COMPLEXITY

Newer tools require Microsoft 365 integration, introducing additional risks.

SEPARATE USER MANAGEMENT

Managing users in a separate system adds administrative burden and potential sync issues.

MICROSOFT ATTACK SIMULATION TRAINING

Microsoft 365 addresses these challenges — natively.

Microsoft 365 offers phishing simulation and cybersecurity awareness training directly within its platform. These features do not require domain whitelisting, eliminating operational burdens and associated risks, providing a streamlined, secure, and cost-effective solution for reducing employee errors and maintaining regulatory compliance.

> "A major advantage of using the Microsoft 365 solution is that all users are already integrated, eliminating the need to manage users in a separate system."

Phishing Simulation

Run realistic phishing campaigns against your own users using Microsoft's built-in payload library. No domain whitelisting required — simulations run natively within your Microsoft 365 environment.

Awareness Training

Assign cybersecurity awareness training modules directly to users. Over 70 built-in training modules covering phishing, social engineering, password hygiene, and more.

RESOURCES

Learn more about Microsoft Attack Simulation Training.

You can view the Microsoft documentation at learn.microsoft.com/en-us/defender-office-365/attack-simulation-training-get-started.

This page includes a demo that you can view directly at www.microsoft.com/en-us/videoplayer/embed/RWMhvB?postJsllMsg=true.

LICENSING

~$5

per user / month — Microsoft Defender for Office 365 Plan 2

The Plan 2 license is included with the Microsoft 365 E5 license. A 90-day free trial is available for organizations that want to evaluate the platform before committing.

CONFIGURATION

Set it up once — it runs for the year.

Everything is configured through the Microsoft Defender portal — a single console for simulations, training, automations, and reporting. No additional software to install, no agents to deploy, no third-party integrations to maintain.

Both elements are designed to be configured once and left to run. The phishing simulation uses an automation that repeats every month on its own — nobody needs to log in to launch each campaign. The awareness training is assigned once per year as a standalone campaign. When a user fails a phishing simulation, Microsoft automatically assigns them remedial training — so ongoing education happens without any manual intervention.

WHERE TO GO

Access the Attack Simulation Training console.

Open the Microsoft Defender portal at security.microsoft.com. In the left navigation pane, go to:

> **Email & collaboration → Attack simulation training**

This opens the Attack simulation training dashboard. From here you will use three tabs:

Simulations	Automations	Training
Launch one-time phishing simulations manually.	Set up recurring phishing campaigns that run on a schedule.	Create awareness training campaigns and assign modules to users.

RECURRING PHISHING SIMULATION

Configure once — phishing campaigns run every month automatically.

Use the Simulation Automations feature to create a phishing campaign that repeats every month on its own. Once configured, there is nothing to do — no monthly login, no manual launch. The system sends a new simulated phishing email to all users each month, rotating payloads automatically. Users who fail are assigned remedial training immediately.

Where to go: Attack simulation training → **Automations** tab → **Simulation automations** → click **+ Create automation**

THE WIZARD WALKS THROUGH THESE PAGES:

1

Automation Name

Give the automation a descriptive name — for example "Monthly Phishing Simulation." The description field is optional but helpful for internal documentation.

2

Select Social Engineering Techniques

Choose one or more techniques from the MITRE ATT&CK framework: Credential Harvest, Malware Attachment, Link in Attachment, Link to Malware, or Drive-by URL. You can select multiple — the system rotates through them.

3

Select Payloads & Login Page

Choose from Microsoft's built-in payload library or create custom payloads. Select **Randomize** to automatically rotate different payloads each month — this keeps simulations unpredictable and realistic.

4

Target Users

Select **Include all users** or pick specific groups. All Microsoft 365 users are already available — no separate user list to manage or sync.

5

Assign Training

Enable automatic training assignment for users who fail the simulation. Select **"Assign training for me (Recommended)"** — Microsoft will pick relevant modules based on what the user fell for.

6

Simulation Schedule

Set the schedule to **Randomized** or **Fixed**. For monthly cadence, set recurrence to **Monthly** with interval **1**. Choose a start date and optional end date. Click **Submit** — simulations will launch automatically each month.

ANNUAL AWARENESS TRAINING

Assign one annual training campaign — remedial training happens automatically.

Training campaigns assign awareness training modules directly to users — independent of phishing simulations. Create one campaign per year for baseline compliance training. You do not need to create monthly campaigns — when a user fails a phishing simulation, the automation you configured above assigns them remedial training automatically. The annual campaign ensures every employee completes their foundational training; the monthly simulations handle everything else.

Where to go: Attack simulation training → **Training** tab → **Training campaigns** → click **+ Create new**

THE WIZARD WALKS THROUGH THESE PAGES:

1 **Campaign Name**

Name the campaign — for example "Annual Cybersecurity Awareness Training 2026." Add an optional description for your records.

2 **Select Training Modules**

Click **Add Training** to open the module library. Choose from over 70 built-in modules covering phishing recognition, social engineering, password security, safe browsing, data handling, and more. Check the boxes next to each module you want and click **Add**.

3 **Target Users & Schedule**

Select **All users** or specific groups. Set a start date and a training due date — Microsoft offers **7, 15, or 30 days** for users to complete their assigned modules.

4 **Notifications & Submit**

Enable reminder emails for users who haven't completed training. Set the notification frequency and customize the message. Review your settings and click **Submit** to launch the campaign.

ANNUAL VERIFICATION

Verify, adjust, and maintain — every year.

Setting up phishing simulations and training is not a one-time task. Regulators, home offices, and cyber insurance carriers expect ongoing evidence that your firm's awareness program is active and effective. An annual review ensures the system is working and that participation is where it needs to be.

Participation Rates

Review completion rates for both phishing simulations and training campaigns. Identify users who have not participated and follow up.

Simulation Results

Analyze click rates, credential submissions, and reporting rates across all monthly simulations. Look for trends — are users improving over time?

Training Completion

Confirm all users have completed their assigned training modules. Generate completion reports for compliance documentation.

Payload Effectiveness

Review which phishing payloads had the highest click rates. Adjust the payload mix to keep simulations realistic and challenging.

New Hire Coverage

Verify that new employees are automatically included in both simulation automations and training campaigns.

Evidence Package

Export reports showing simulation results, training completion, and improvement trends. This is the evidence regulators and insurers want to see.

THE QUESTION THEY WILL ASK

Can you show us evidence that your employees are being tested and trained on cybersecurity awareness?

Ready to set up cybersecurity awareness training for your firm?

FCI works with broker-dealers & branch offices, insurance carriers & agencies, and RIAs. Call us to discuss implementation — there is no commitment until you decide to engage.

PHONE

973-227-8878

WEB

fcicyber.com