

2025 PHISHINGBOX CYBERSECURITY MONTH GUIDE



phishingbox.com

WHAT IS CYBERSECURITY AWARENESS MONTH?

Cybersecurity Awareness Month is a national initiative led by CISA and the National Cybersecurity Alliance. Every October, organizations across the U.S. focus on building stronger security habits that reduce human risk.

This year's four core themes emphasize the basics of online safety:

-  **Use strong passwords**
-  **Turn on multifactor authentication (MFA)**
-  **Recognize and report phishing**
-  **Update your software**

With PhishingBox, you can engage employees through simulations, courses, and reinforcement (training) emails — making awareness practical and memorable.

Have questions? Reach out to customersuccess@phishingbox.com



HOW TO USE THIS GUIDE

PURPOSE

Use this guide to plan and launch Cybersecurity Awareness Month activities in PhishingBox. Follow the step-by-step plan of action below, or use the Library to build your own customized campaigns.

OPTION A — PHISHINGBOX'S RECOMMENDED PLAN OF ACTION

1. Create a Training Email Campaign
 - Use the Cybersecurity Month 2025 template (highlights the four CISA focus areas).
2. Enroll Learners Automatically
 - This training email will enroll recipients in the [Micro] Reporting Incidents course.
3. Reinforce with a Phishing Campaign
 - Later in the month, schedule a phishing simulation using Internal – Corporate VPN Expiration.

OPTION B — BUILD YOUR OWN

1. Go to Library → apply the "2025 Cybersecurity Month" content filter to view suggested items.
2. Pick activities per theme: phishing simulations, courses, and reinforcement (training) emails.
3. Create:
 - A phishing email campaign
 - A training email campaign
 - Course enrollments
4. Schedule across October.

NEED HELP?

Email customersuccess@phishingbox.com for assistance configuring Campaigns, choosing content, or tailoring the schedule for your organization.



PASSWORDS: YOUR FIRST LINE OF DEFENSE

Weak or reused passwords are the #1 way attackers break in. Training helps employees build strong habits that keep accounts secure.

PHISHING SIMULATIONS

- Generic – Password Reset
- Microsoft – Password Reset
- Central Medical – Account Compromised

COURSE OPTIONS

- **PhishingBox:** Password Security (Core)
- **Optiv:** Password Security (SecurityBytes), The Problem with Popular
- **Hook:** Passwords (PsySec Deep Dive), Passwords (Mike Fry the Cyber Guy)

REINFORCEMENT EMAILS

- Creating a Strong Password
- Password Management
- One Size Does Not Fit All
- Benefits of Single Sign-On & Password Lockers

Create a new password

You received this email because you requested a new password.

[CREATE A PASSWORD](#)

You will use your new password to log into:

If you didn't make this request or need assistance, please [contact us](#).

All rights reserved.



What You'll Learn Today:

Creating a Strong Password

Weak passwords are one of the easiest ways for cybercriminals to break into accounts. A strong password helps keep your information safe and secure.

[How to Build a Strong Password](#)



Use at least 12 characters

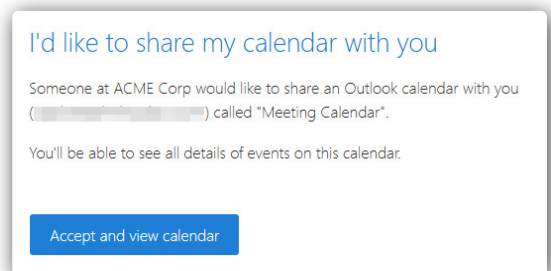


MFA: ADD A SECOND LAYER OF PROTECTION

Multifactor authentication (MFA) stops most credential theft. Employees should learn to recognize MFA prompts and avoid push notification scams.

PHISHING SIMULATIONS

- Microsoft – Calendar Invitation
- Google – Workspace Password Reset
- Generic – Verify Your Login
- Minisoft – 2FA Code



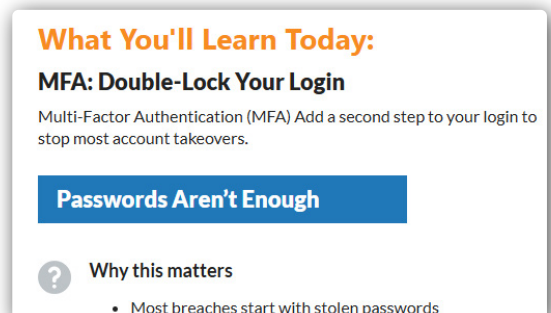
COURSE OPTIONS

- PhishingBox: Multifactor Authentication (Core)
- Optiv: Multi-factor Authentication (Rapid Awareness), Paul's Password Problem
- Hook: Multi-factor Authentication



REINFORCEMENT EMAILS

- MFA: Double-Lock Your Login
- MFA Push Notification Exploitation
- Authentication System Security





PHISHING: SPOT IT. STOP IT. REPORT IT.

Phishing remains the most common cyber threat. Teaching employees how to spot red flags — and report suspicious emails — reduces risk across your organization.

PHISHING SIMULATIONS

- Internal – Corporate VPN Expiration
- BEC – Purchase Order Gift Card Incentive
- PayPal – Claim Your \$5
- Venmo – Phone Number Changed

To John Taylor:

Please be advised that, effective immediately, we have terminated your corporate VPN access due to repeated violation of our Acceptable Use Policy. We regret having to take this action, but after numerous warnings regarding inappropriate use and access from unauthorized locations and devices, we have seen no change in your usage pattern. The manner in which you use our VPN service jeopardizes ACME Corp's reputation and security as safety of our customers' information.

If you believe that you received this message in error or are not responsible for inappropriate use, please reply to this email with your ACME Corp VPN username and password for further investigation.

Sincerely,

ACME Corp IT Department

COURSE OPTIONS

- **PhishingBox:** Phishing (Core), Phishing Attachments (Micro), Smishing (Micro)
- **Optiv:** Phishing Attachments (Rapid Awareness), Phishing Links (Rapid Awareness)
- **Hook:** Phishing (Quick Hit), Phishing (PsySec Deep Dive)



REINFORCEMENT EMAILS

- How to Spot & Avoid Phishing
- Is This Email Legitimate?
- Types of Phishing

What You'll Learn Today:

How to Spot & Avoid Phishing

Not even the best scammer can outsmart skepticism.

**Trust No one & Check
Everything**

1. **The Lure:** An enticing, yet flawed, email featuring any of these traits:



UPDATE SOFTWARE TO STAY SECURE

Unpatched systems are prime targets for attackers. Employees should always install updates from official IT channels — not from suspicious prompts.

AWARENESS FOCUS (NO PHISHING SIMS)

Campaign messages emphasize installing updates from trusted sources only.

COURSE OPTIONS

- **PhishingBox:** Update to Stay Safe (Micro)
- **Optiv:** Workplace Security (SACT), Your Role in Cybersecurity
- **Hook:** Safe Web Browsing (PsySec Deep Dive), Physical Security (Quick Hit)

REINFORCEMENT EMAILS

- The Power of Updating
- How to Spot Fake vs. Real Update Prompts
- Anti-Virus & Anti-Malware Defense

What You'll Learn Today:

The Power of Updating

Keep your hardware and software updated to stay as safe as possible.

Updating Best Practices



Enable auto-update features on secure networks, so patches will download and install without you needing to remember to do it manually.



What You'll Learn Today:

How to Spot Fake vs. Real Update Prompts

Cybercriminals often disguise malware as "update required" pop-ups or emails. Learning how to tell the difference keeps you safe and ensures you only install legitimate updates.

Key Differences to Watch For



Source of the prompt

Real updates come from your device's built-in updater or app