How to use these templates:

These templates are written for a weekly cadence to be sent to your end-users.

Be sure to update anything highlighted before sending out.

- Anything highlighted yellow requires a link. There will be a placeholder link to content, but we recommend you whitelabel the content.
- Anything highlighted blue requires your personalized information.

Slack/Teams Message 1

📌 Here are a few quick resources to help keep you safe both in and out of work.

Save this message, share with friends, and/or print them out (11x17) and hang them around your office.

⚠️ **Reminder:** If you think you clicked something suspicious, entered information somewhere you shouldn't have, or notice your computer acting strangely, don't panic or try to hide it. **Contact [MSP/IT Team] at [Support Contact] right away.** The sooner we know, the sooner we can help!

[Attach 3 guides]

Slack/Teams Message 2

👨‍👩‍👧 **Protect your family and friends, not just your employer**

Cybercriminals target people everywhere—not just at work.

That's why we're sharing **Internet Survival Guides** for all types of people.

👨‍👩‍👧 Parents, Caregivers & Families
📱 Kids & Teens
👴 Adults 60+
🎓 Young Adults
💼 Small Business Owners
✈️ Travelers
🏠 Homeowners

Each guide covers common scams, warning signs to watch for, and what to do if something goes wrong.

[Attach all internet survival guides]

Slack/Teams Message 3

🏆 **Shoutout to our cybersecurity MVPs!**

These team members have been crushing their security awareness training:

🏆 [Employee Name]
🏆 [Employee Name]
🏆 [Employee Name]

They've consistently completed their training on time and accurately reported simulated phishing emails. The best way to get better at recognizing cybersecurity attacks is by building better habits.

Keep reporting anything that looks suspicious, even if you're not 100% sure. We'd much rather investigate something harmless than miss something dangerous.

Slack/Teams Message 4

As the holidays get closer, scams are going to be ramping up. Keep an eye out for these common scams.

One thing most of them have in common? **Urgency.**

Before clicking, paying, or sharing information, slow down and verify the request another way.

⚠️ **Reminder:** If you think you clicked something suspicious, entered information somewhere you shouldn't have, or notice your computer acting strangely, don't panic or try to hide it. **Contact [MSP/IT Team] at [Support Contact] right away.** The sooner we know, the sooner we can help!

[Attach scam guide]

Slack/Teams Message 5

🤔 **Why do you need security awareness training?**

Learning to spot suspicious emails, scams, impersonation attempts, and other warning signs can help protect both company data **and your own personal accounts, money, and information.**

That's why we use Phin Security for short, consistent training and realistic phishing simulations. The goal isn't to trick you or turn you into a cybersecurity expert—it's to build healthy cyber habits, so you know when something doesn't look right and how to take action.

You can learn more about the training you're enrolled in here.