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.

Email 1

Subject Line: Keep these cybersecurity cheat sheets handy

Hi [First Name],

Here are a few resources to help keep you safe both in and out of work as we kick off Cybersecurity Awareness Month.

📌 **You clicked a scam. Now what?**

📌 **What to do if you're experiencing any of these Cyber Attack Warning Signs**

📌 **10 Security Tips for [Industry]**

Save them somewhere you'll see often, share them with your team, and/or print them out (11x17) and hang them around the office!

[Signature]

Note: *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!*

Email 2

Subject Line: Protect your family and friends, not just your employer

Hi [First Name],

Cybercriminals don't just target you at work. They target you when you're shopping, traveling, helping your parents, running a business, scrolling social media, or just trying to hire someone to fix the roof.

That's why we're sharing **Internet Survival Guides** for:

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

Each guide covers scams that commonly target that demographic, warning signs to watch for, and what to do if something goes wrong.

[Button: Download your Internet Survival Guides →]

Use the ones most relevant to you, and send another to someone you care about.

[Signature]

Note: *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!*

Email 3

Subject Line: Congratulations to your cybersecurity MVPs 🏆

Some people have been absolutely crushing their cybersecurity training, and they deserve a shoutout.

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

These team members have been consistently completing their security awareness training on time ***and*** accurately reporting simulated phishing emails.

Why does that matter? Because the habits you practice during training are the same ones that can help you recognize a real attack.

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

[Signature]

Note: *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!*

Email 4

Subject Line: 'Tis the season for scams

Hi [First Name],

Not only is the holiday spirit about to ramp up, but so are scams 👎

Over the next few months, be extra cautious of:

- **Fake delivery notifications** claiming there's a problem with your package
- **Too-good-to-be-true deals** from fake stores and websites that mimic real stores
- **Gift card scams** asking you to buy gift cards or send the numbers
- **Fake purchase alerts** claiming there's an unauthorized charge on your account
- **Fake charities** asking for donations after major events or during the holidays
- **Travel scams** offering suspiciously cheap flights, rentals, or vacations
- **Boss impersonation scams** asking you to urgently send money, change payment information, or buy gift cards

Urgency is one of a scammer's favorite tools. Before clicking, paying, or sharing information, slow down and verify the request another way.

For more tips on spotting holiday scams, or to share with family and friends, **download this short guide.**

[Signature]

Note: *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!*

Email 5

Subject Line: Why do you need security awareness training?

Hi [First Name],

We get it. Cybersecurity training probably isn't the highlight of your month. So why do you have to do it?

Because cybersecurity isn't just about protecting company computers. **The same skills that protect you at work can protect you everywhere else.**

Spotting a suspicious email can protect your company's data — but it can also keep someone from stealing your personal bank credentials.

That's why we use **Phin Security** to give you short, ongoing security awareness training and realistic phishing simulations. It's not about trying to trick you or expecting you to become an expert. It's about giving you regular practice so you can recognize when something doesn't look right and know what to do about it—both in and out of work.

Learn more about our security awareness program here, and don't hesitate to reach out with questions!

[Signature]

Note: *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!*