PHIN

8 TIPS

for going beyond insurance requirements

1 Short & Digestible Content

No one wants to watch a 45-minute presentation on data security. It's boring and information overload. **Keep training ~5 minutes or less** to reduce work disruptions and ensure information retention.

5 mins

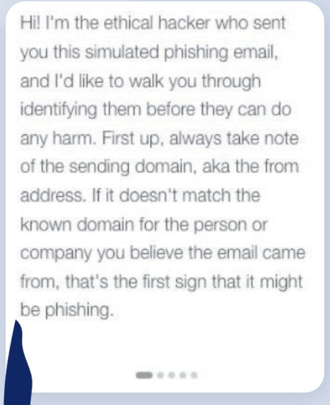
2 Make it Relevant

Training should include **real-life examples** and information that's relevant to both the user's work and personal life.

The user will be more engaged and it will help them put the pieces together of **why it's important to them.**

3 Train Frequently

Once-a-year training sucks. **#sorrynotsorry** It forces the content to be too long to retain information and it doesn't keep training top of mind. Threats evolve constantly, so users will have **serious security knowledge gaps throughout the year.**



Hi! I'm the ethical hacker who sent you this simulated phishing email, and I'd like to walk you through identifying them before they can do any harm. First up, always take note of the sending domain, aka the from address. If it doesn't match the known domain for the person or company you believe the email came from, that's the first sign that it might be phishing.

4 Give Real Time Feedback

If users click a phishing simulation and are punished with an irrelevant training video 2 weeks later, they're not actually learning anything. **Give your users immediate feedback** on the email they clicked, so they know exactly what they did wrong and can **improve for next time.**

5 Everybody Gets Trained

Your executive team does not get a free pass. They need to be the role models for the rest of your company. If they don't care about keeping their business secure, why should your employees?

VIP

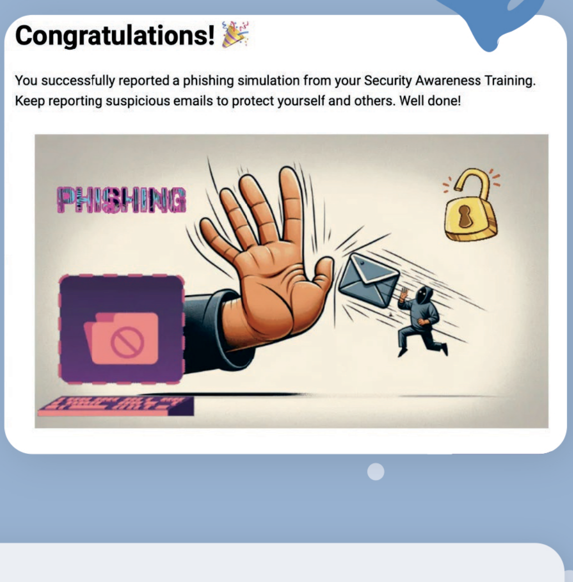
Users who are most at risk of an incident:

- Have access to critical data
- Are click-happy
- Fail to complete training assignments
- Are suppliers or business partners
- Are leaving the company
- VIPs/Executives

Source: Proofpoint's 2024 State of the Phish

6 Measure Behavior Change, Not Just Completion

Don't just report on who has completed their training. **Analyze how end-user behavior is changing** (or staying the same) so you can improve the training experience for your users. Remember: the goal isn't to check the box, it's to secure your business.



Congratulations! 🎉

You successfully reported a phishing simulation from your Security Awareness Training. Keep reporting suspicious emails to protect yourself and others. Well done!

7 Make It Fun!

Include gamification and ways to better engage users! Celebratory GIFs are a fun way to **reward users** when they accurately **report phishing simulations.** Plus, the training content itself **doesn't have to be boring**—people can still learn from cartoon shows and music videos.

8 Celebrate Success, Don't Just Punish Mistakes

Build a leaderboard or other system to **reward users** who complete their training on time, perform well on assessments, and accurately identify phishing simulations. **Ensure users aren't scared to report** if they've accidentally clicked a phish — this will help you react more promptly to an attack and mitigate a breach.

LEARN MORE

Sure, it sounds like a lot more work than just checking a box.
But not when Phin can do it all for you!

PHIN