Phishing Awareness & Training Guide

THE IMPACT: Training our Team Members is a key part of our overall scam-prevention strategy. Ongoing cybersecurity education and realistic phishing simulations help our team recognize and stop suspicious activity while keeping everyone alert, prepared, and on their toes as scam tactics continue to evolve.

THE GAME PLAN:

MONTHLY TRAINING

Each month, Team Members with a company e-mail, excluding store accounts, will receive:

- A short cybersecurity training video focused on a specific security or phishing topic.
- A brief knowledge check at the end of the training.
- A simulated phishing email designed to mimic a real phishing attempt.
- Immediate feedback based on how they respond to the simulation.

Training topics will change throughout the year and may include phishing awareness, business email compromise, malicious links, password security, social engineering, QR code scams, AI-generated scams, and other emerging cybersecurity threats.

If You Receive a Phishing Simulation

Treat, the email as you would any suspicious email. If you correctly identify and report the simulation, you will receive confirmation that you successfully recognized and reported it.

If you interact with a simulated phishing email, a short Just-in-Time Training will explain what made the email suspicious, the phishing indicators and red flags that were present, and how to identify similar emails in the future. You will then complete a four-question knowledge check.

FREQUENTLY ASKED QUESTIONS

Questions	Answers
Are the training videos the same every month?	• No. Training topics will vary throughout the year and cover different cybersecurity risks.
How long does training take?	• Training is intentionally short and designed to fit into the workday. Most sessions can be completed in just a few minutes.
Is there a quiz?	• Yes. Each monthly training video includes a short knowledge check to reinforce key takeaways.
What happens if I click on a phishing simulation?	• You will receive a brief Just-in-Time Training explaining the warning signs you may have missed, followed by a four-question knowledge check.
Will I be in trouble if I fail a phishing simulation?	• No. The program is focused on awareness, education, and helping Team Members improve their ability to identify phishing attempts.
What phishing red flags should I look for?	• Watch for unexpected requests, urgent or threatening language, requests for passwords or sensitive information, suspicious links or attachments, and misspelled sender names or email addresses.
How do I report a suspicious email?	• Continue following Rally House's established process for reporting suspicious emails. If you are unsure whether an email is legitimate, report it rather than interacting with it.
Will phishing simulations be announced ahead of time?	• No. Simulations are designed to imitate real phishing attempts and may occur without advance notice.
Are phishing simulations safe?	• Yes. Simulations are generated through Abnormal AI as part of the security awareness program and do not pose a risk to your device or Rally House systems.