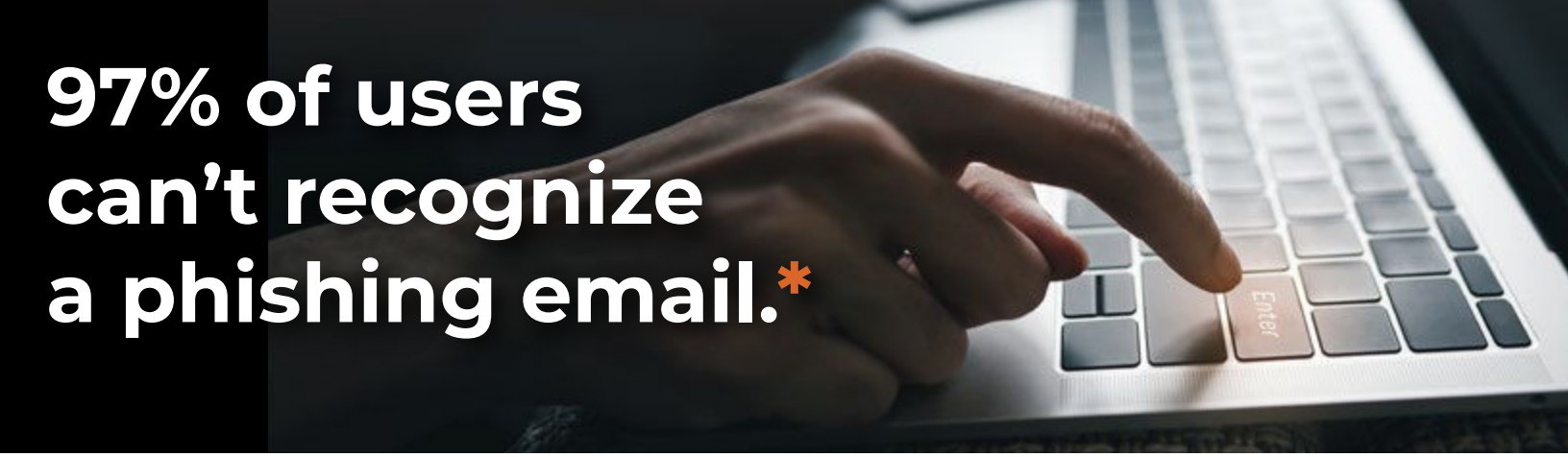

97% of users can't recognize a phishing email.*

Stop Cyber Attacks in Their Tracks With Security Awareness Training

Your employees are your first line of defense against attacks. Make sure they know what to look for. GRF can help you create an engaging, custom employee training program to help reduce your risk. Just call us and we'll manage the rest! Start up is quick and easy...and best of all, affordable!

CPAs & ADVISORS

- **Ongoing 12-Month Training & Monthly Deep Dives**
- **Phishing Simulations**
- **Automated, Actionable Reporting**

How Our Training Works

Our program uses a positive approach that includes humor, repetition, and the latest research in neuroscience to train the part of the brain that houses threat recognition and response.

Experts You Can Trust

- ✓ Our cybersecurity team includes certified ethical hackers (CEHs), certified fraud examiners (CFEs), and certified information system auditors (CISAs)
- ✓ You'll work with experts with specialized cyber security skills, knowledge, and technological resources to provide you with optimal solutions

Contact Us

Melissa Musser,
CPA, CITP, CISA
Partner & Director,
Risk & Advisory Services
mmusser@grfcpa.com

Darren Hulem,
CISA, CEH, Security+
Supervisor, IT &
Risk & Advisory Services
dhulem@grfcpa.com

Source: Security Boulevard, technology publisher for the IT security industry

Contact us for a live demonstration today!

grfcpa.com/security-consultation

Cybersecurity Awareness Training

What is Security Awareness Training?

Security awareness training reduces the risk of breaches and cyber attacks. Attackers send phishing emails to end users daily, and while spam filters and email security features can be set up, there will always be the risk of malicious emails getting through to user inboxes. By incorporating a formal training program, your end users will learn good habits for identifying malicious emails, what to do if received, and how to report incidents that may occur.

Why is it Important?

While the most important outcome of training is to reduce the risk of breaches to the organization, there are multiple benefits, including the reduced risk of downtime and improved compliance. Many compliance programs, such as PCI, DSSS, HIPAA, ISO 27001, and GDPR require employee training. Training reduces the risk of cyber attacks, which are a main cause of downtime for organizations.

Our Approach

At GRF, we provide white glove service to cybersecurity awareness training, which includes everything from setting up recurring training and phishing simulations, to providing actionable reports. We are ready to help you reach your cybersecurity program objectives today.

GRF's Cybersecurity Solutions

We are dedicated to safeguarding the integrity of our client's information technology systems. Our service approach is systematic and heavily focused on timely, responsive, and clear communications. Our practical, right-sized solutions are based on your organizational context to address your most important issues. For more information, visit www.grfcpa.com/accounting-services/cybersecurity-and-privacy-risk-solutions/

CPAs & ADVISORS

Security Best Practices

1. Update devices and applications regularly
2. Use a VPN when working on public networks
3. Lock your workstation when not in use
4. Utilize strong password and MFA where available
5. Communicate incident response procedures to employees
6. Be aware of potential phishing and social engineering attacks
7. Train employees on what to look for from malicious actors