If It Feels Off, It Probably Is:

Everything Your Business Needs to Know About Cyber Red Flags

POWERED BY TEKIE GEEK

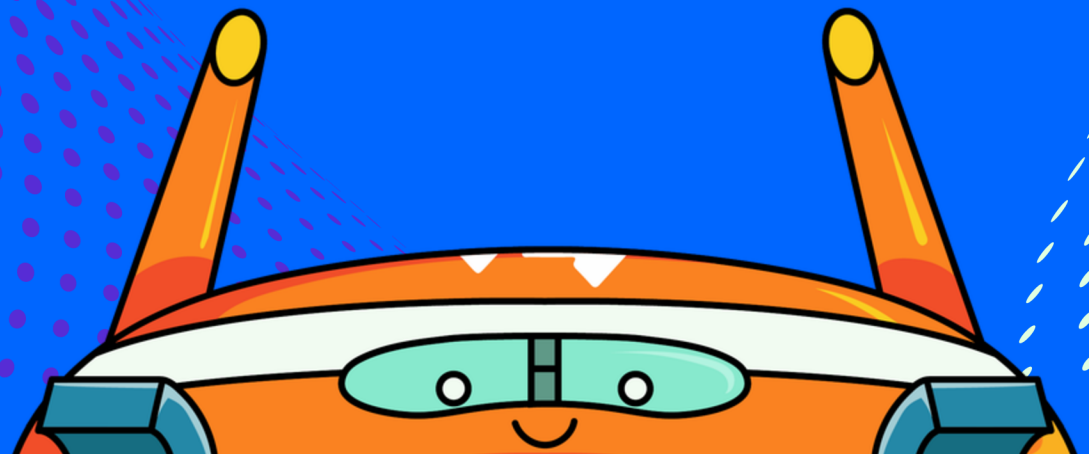


Table of Contents

1

Why Cybersecurity Awareness Matters

Cybersecurity is no longer just an IT concern—it is a business-wide responsibility. Businesses of all sizes and industries are increasingly targeted by cybercriminals, and employees are often the primary entry point for these attacks.

A single mistake, such as clicking a malicious link or sharing credentials, can lead to data breaches, financial loss, operational disruption, and reputational damage. Cybersecurity awareness training helps reduce these risks by preparing employees to recognize threats and act responsibly.

Protecting your business begins with educating your employees.

2

What Is Cybersecurity Awareness?

Cybersecurity is the practice of protecting IT infrastructure, systems, networks, and data from cyberattacks.

Cybersecurity awareness focuses on educating employees about cybersecurity best practices and helping them recognize indicators of cyber threats.

Cyber awareness training teaches employees how cyberattacks occur, what warning signs to look for, and how everyday actions—such as email use, password management, and file sharing—impact overall security.

An informed workforce is one of the most effective defenses against cyber threats.

3

Why Educating Employees Is Critical

Regardless of company size or industry, employee cybersecurity education is essential.

Well-trained employees help:

- Reduce the risk of cyberattacks and data breaches
- Minimize human error, including falling for phishing scams
- Strengthen internal security policies and procedures
- Reinforce confidentiality and data privacy
- Support compliance with regulatory and industry standards

Cybersecurity awareness training also demonstrates your commitment to protecting customer and employee data, building trust with clients and partners.

4

Understanding Phishing and Email-Based Attacks

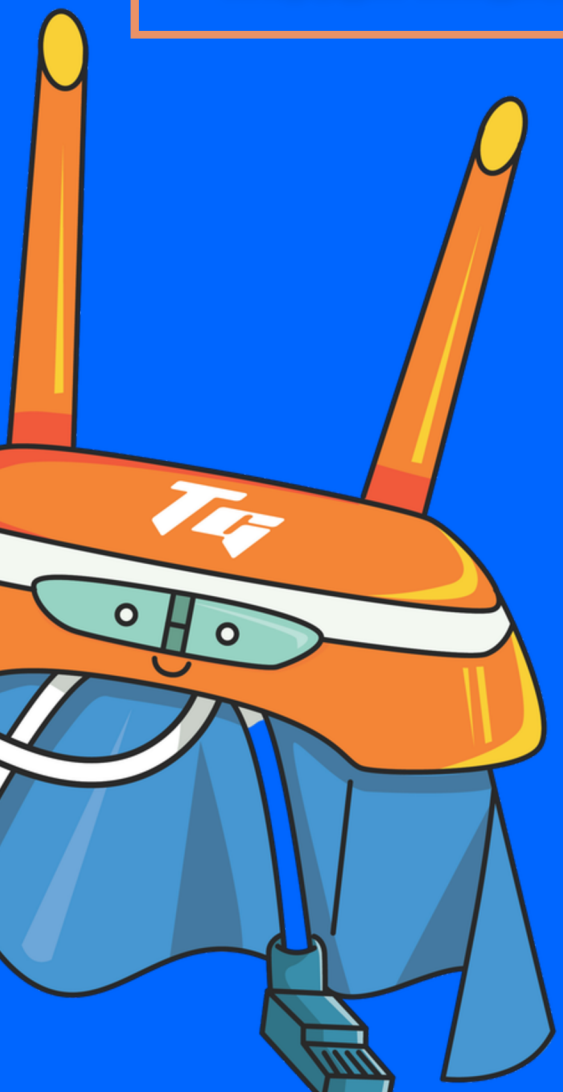
Phishing is one of the most common and damaging cyber threats facing businesses today.

These attacks are designed to trick employees into clicking malicious links, downloading harmful attachments, or sharing sensitive information.

Phishing emails often impersonate trusted sources such as vendors, executives, banks, or service providers. They may create urgency, request confidential information, or pressure employees to bypass standard procedures.

5

- *Common phishing tactics include:*
- *Fake login pages used to steal credentials*
- *Fraudulent invoices or payment requests*
- *Business Email Compromise (BEC)*
- *Malicious links or attachments that install malware*



Training employees to recognize phishing warning signs—such as suspicious sender addresses, unexpected requests, and urgent language—significantly reduces risk.

6

SOCIAL ENGINEERING AND HUMAN-BASED THREATS

Social engineering attacks rely on psychological manipulation rather than technical exploits. Cybercriminals may use emails, phone calls, text messages, or in-person interactions to trick employees into revealing confidential information.

Examples of social engineering include impersonating IT support, executives, or vendors, as well as pretexting and baiting tactics. Employee training helps staff identify these attacks and respond appropriately without compromising security.

8

CYBER AWARENESS EMPLOYEE TRAINING OPTIONS

Businesses can implement various types of cybersecurity training depending on their needs:

Security Awareness Training Covers password management, multi-factor authentication, phishing recognition, malware awareness, and physical security.

Compliance Security Training Supports regulatory requirements such as HIPAA, PCI, ISO, and Sarbanes-Oxley, focusing on secure data handling and confidentiality.

Social Engineering Training Educates employees on manipulation tactics and proper response strategies.

Simulated Phishing Attacks Tests employee awareness through mock phishing campaigns and reinforces learning.

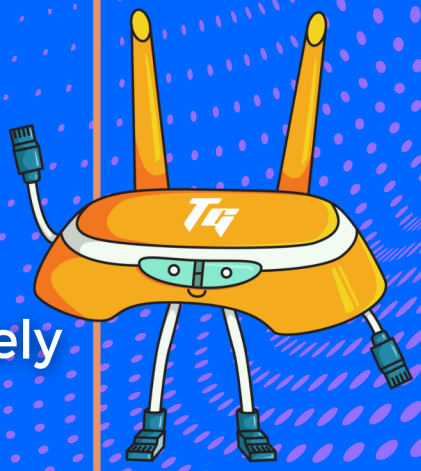
9

BEST PRACTICES EMPLOYEES SHOULD FOLLOW DAILY

Employees play a key role in maintaining cybersecurity.

Best practices include:

- Using strong, unique passwords
- Enabling multi-factor authentication
- Verifying unexpected requests
- Reporting suspicious emails immediately
- Following company security policies



Consistent habits greatly reduce cybersecurity risk.

10

HOW TEKIE GEEK SUPPORTS EMPLOYEE CYBERSECURITY TRAINING

Cybersecurity starts with employees, and effective training strengthens your first line of defense.

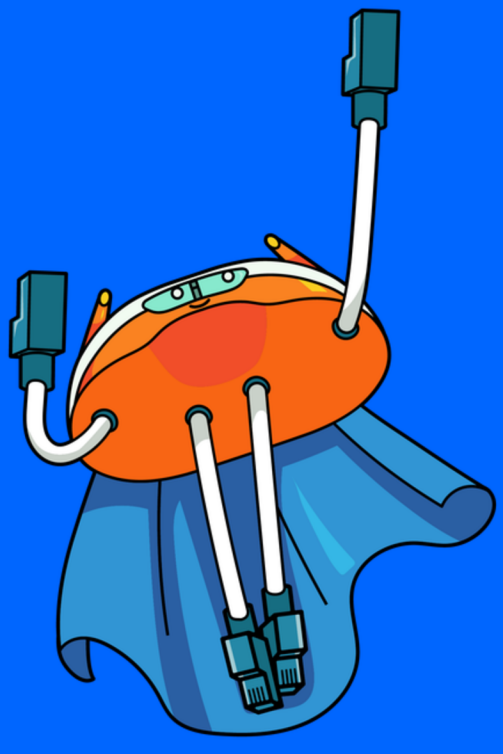
Tekie Geek helps businesses navigate the evolving digital landscape by providing cybersecurity education, awareness training, and managed IT services tailored to organizational needs.

11

BUILDING A SECURITY-FIRST CULTURE

A strong cybersecurity posture depends on informed and vigilant employees. Technology alone is not enough to protect a business from today's cyber threats.

By investing in employee cybersecurity awareness and training, businesses reduce risk, protect sensitive data, and build a culture of security.



Tekie Geek is here to guide your business through the challenges of the digital age by empowering employees with the knowledge and tools they need to stay secure.

Educated employees create stronger, more secure businesses.