

# Breach Secure Now: Empowering Your Cyber Security

Take a proactive approach with cyber security education and phishing

Ransomware is an epidemic, and email phishing scams continue to be the attack vector of choice for cybercriminals. However, technology alone *cannot* provide adequate security defense, as web and internet users need assistance in avoiding evolving security threats.

Recent security reports reveal that 95% of data breaches are caused by user error. Without proper training to spot and avoid falling victim to phishing attempts, we humans will continue to be the weakest link in protecting our systems and critical data.

Breach Secure Now with CMIT Solutions helps to transform our weak links into strong defenses.

### **User-Focused**

Breach Secure Now is a robust security platform that protects you by providing customized ongoing security awareness training and simulated phishing campaigns.

# **Cybersecurity Training:**

- User-Focused
- Flexible User Subscriptions
- Monthly Newsletter
- Revolutionary Training Tools

# With the widespread adoption of cloud storage platforms, it was only a matter of time before cybercriminals began exploiting cloud services in their schemes. Be cautious of emails, phone calls, or text messages claiming that your cloud account has expired or been compromised. Instead of clicking on any links or responding to unsolicited phone calls, research the company and contact them directly using the information provided on their official website. #CyberCat #cloud See Less THE ADVENTURES OF CYBER CAT This seems like a case for Storage solution. This seems like a case for Detective Mittens! The message is unsolicited, asis for my credentials, and the sender; email address doesn't match the sender sender.

## Why use Breach Secure Now?

- Rich training modules that encourage user engagement and security practices
- Consistent platform enhancements based on user feedback and market trends
- · Real-world security training modules, including weekly micro-training emails
- Flexible phishing campaigns to keep users refreshed on effective security



# Training Syllabus

# Lesson 1

- Password Best Practices
- Multi-Factor Authentication
- Password Managers
- Social Engineering

# Lesson 2

- Malware and Ransomware
- Worms and Cryptoworms
- Connected Networks
- IoT Devices
- Phishing and Vishing
- SLAM Method
- Artificial Intelligence

# Lesson 3

- PII (Personally Identifiable Information)
- Physical Security
- Device Security
- Backup and Remote Wiping
- Spear Phishing
- Critical Infrastructure Attacks
- Dark Web
- Social Media

# Lesson 4

- Importance of Cybersecurity Awareness
   Training
- Insider Threats (Intentional and Unintentional)
- Reporting Incidents
- Updating Software

