Cyber Security Awareness: What Everyone Should Know

Business Success Symposium

September 9, 2025

Steve Wingate

- 25+ Years Experience in IT
- 15+ Years Experience in Information/Cyber Security
- Certifications CISM, CISSP, GCIH, CEH, GSEC, SSAP, MCP, GCIA, GCISP

How easy is it to lose $1.4 million?

Legit email address = gb868@email.com

Hacker's address = gp8668@email.com

- The user's account was compromised allowing the hacker over 10 days to monitor normal activity and patterns.
- When the hacker saw a transfer request for $1.4 million, they intercepted the response, changed the account number and "boom" they were $1.4 million richer.

Why Cybersecurity Matters

Protect customer data, your data and company resources

Protect operations, production, and supply chain integrity

Reduce reputational risk, financial loss, regulatory penalties

Top Cyber Threats

Phishing & Social Engineering

Ransomware Attacks

Insider Threats

Supply Chain Vulnerabilities

Legacy and Unpatched Systems

Quiz Time!

You receive an email from 'IT Support' asking you to reset your password immediately. What should you do?

A) Click the link and reset your password right away

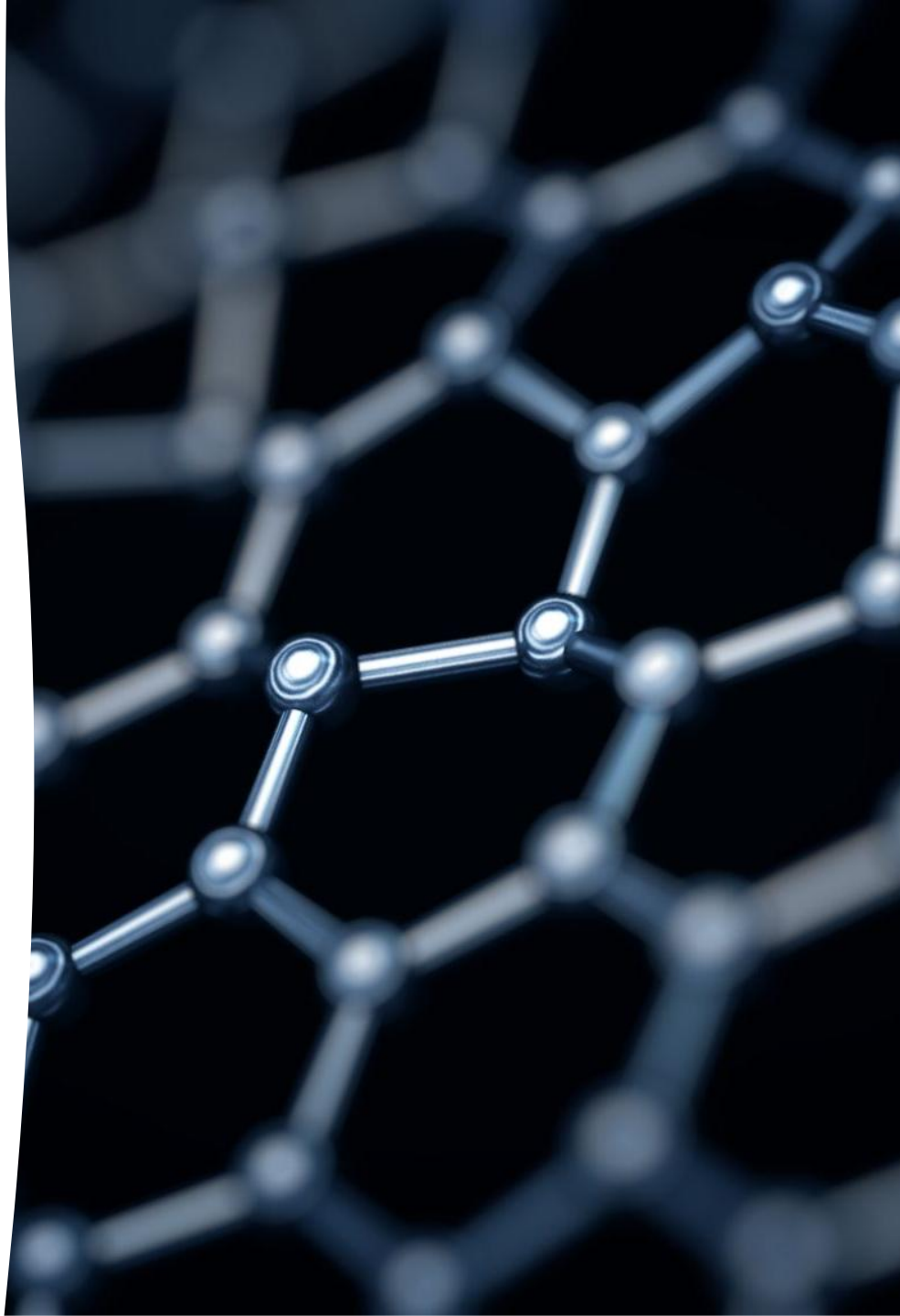
B) Forward the email to a coworker to see if it's real

C) Report the email using your company's phishing button or to IT

D) Reply to the email asking for verification

Fundamental Cyber Hygiene

- Use strong passwords & Multi-Factor Authentication
- Recognize and report phishing attempts
- Regular patching and updates
- Network segmentation for critical systems
- Backup & recovery plans
- Secure remote access practices
- Vendor security oversight



Emerging Risks: Artificial Intelligence (AI) & Large Language Models (Chat GPT)

Prompt Injection Attacks – tricking AI into leaking sensitive data

Misinformation & Fabricated Sources – AI may produce convincing but false content

Data Privacy – inputting sensitive business/patient/manufacturing data can create risks

Shadow AI Use – employees using AI tools outside of company-approved platforms

Staying Safe with AI Tools

- Never input sensitive or regulated data (Personal/health related, financial, proprietary)
- Verify AI outputs against trusted sources before acting
- Use company-approved AI platforms with security controls
- Train staff to recognize risks of sharing confidential info with public AI tools
- Incorporate AI use into security policies and awareness training

Real-World Scenarios

- Hospital ransomware locks medical records, delaying treatment
- Attack on OT network halts factory production line
- Vendor compromise spreads malware into both sectors
- AI-generated phishing emails/texts used to target staff

Quiz Time!

Which of the following is the most secure password practice?

A) Use your pet's name with your birth year (e.g., 'Bella1990')

B) Use the same password across all accounts so it's easy to remember

C) Use a password manager to create and store unique passwords

D) Add '123!' to the end of your current password when asked to update

Building a Cyber-Aware Culture

- Consistent training and phishing simulations
- Leadership support and visible involvement
- Clear reporting paths for suspicious activity
- Reward and recognize secure behavior

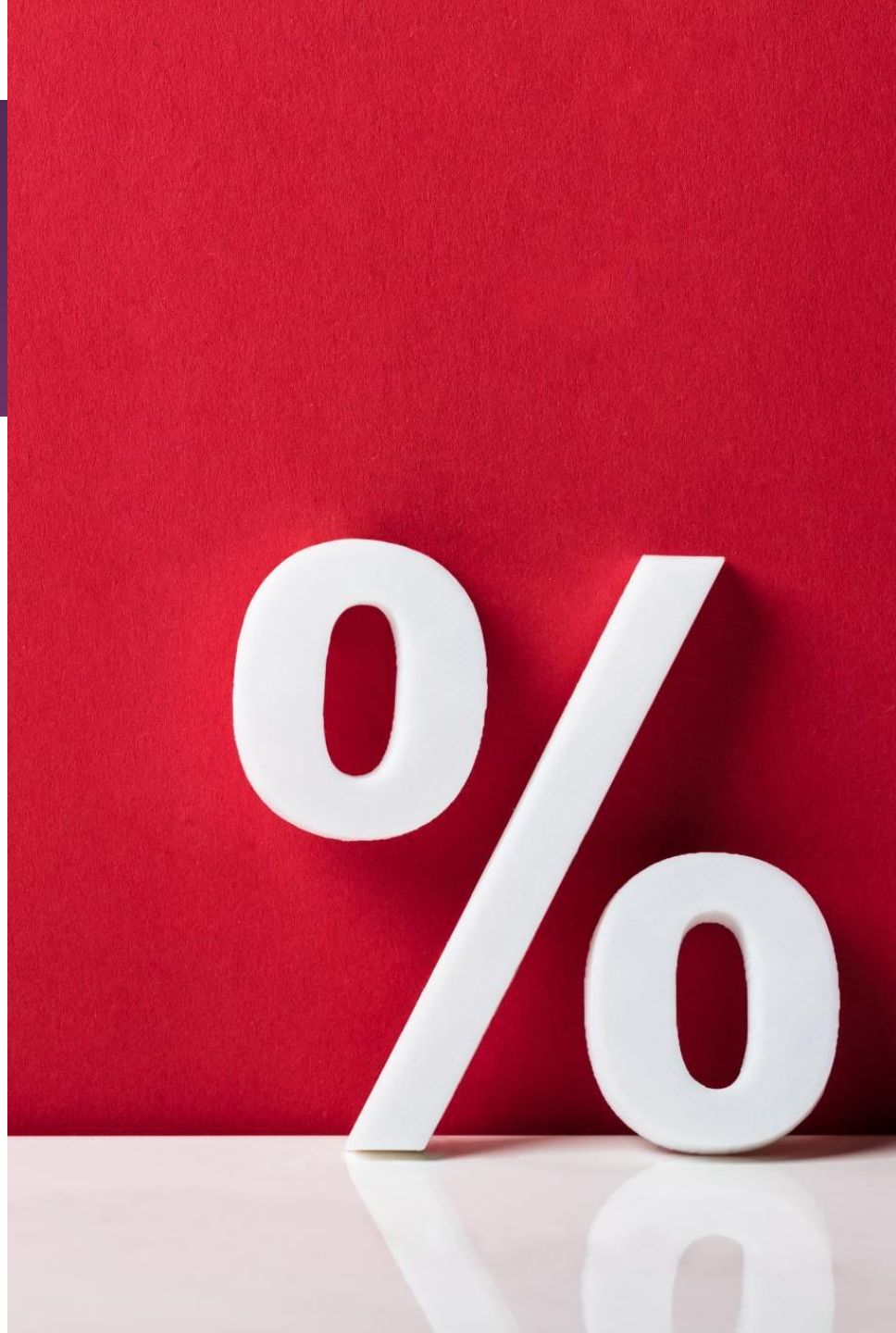
Simple Takeaways by Role

Enable	All Staff: Enable MFA, report suspicious messages
Patch	IT/Security: Patch, secure access, segment networks
Support	Leaders: Support training, enforce vendor checks
Verify	If it doesn’t look right, report it or ask someone. Don’t take on unneeded risk.
Lock down	Stay aware of your surroundings, protect your devices, protect your own data and the data you are entrusted with.

Quiz Time

What percentage of cyberattacks begin with phishing?

A) 20%
B) 50%
C) 90%



Sample Phishing Emails & Texts

Email: 'URGENT – Your account is locked. Click here to verify your login.'

Email: 'HR Update: New benefits plan details attached.'

Text: 'Your package delivery failed. Reschedule now: [malicious link]'

Text: 'Bank Alert: Unusual activity detected. Reply YES to secure your account.'

Security Made Easy

1. If you don't know who it is from, don't click on it.

2. If you know who it is from but it's not normal - don't click on it.

3. If you were not looking for it, don't click on it.

4. If you buy it, keep it updated.

5. If you are done with it, remove all your data and get rid of it.

6. Slow down, pay attention and if you are not sure don't click on it.

7. Just because you are on a mobile device, you are not protected.

Wrap Up

Cybersecurity is everyone's responsibility

Stop, Think, and Act with awareness

Questions?

Resources

Security Training
https://www.knowbe4.com/homescourse
- Password is homecourse

Freeze Your Credit
https://www.usa.gov/credit-freeze

Cyber for Children
https://www.knowbe4.com/resources/kits/childrens-cybersecurity