PHISHING AWARENESS TRAINING

A comprehensive guide to recognize and respond to phishing threats in 2025. Protect your organization, data, and yourself.

⚠ SECURITY IS EVERYONE'S RESPONSIBILITY

July 2025

Table of Contents

1. Introduction
2. Phishing in 2025: Key Statistics
3. What is Phishing?
4. Why Everyone Is a Target
5. Main Types of Phishing Attacks
6. Real-World Phishing Case Studies
7. Anatomy of a Phishing Email
8. Business Email Compromise (BEC)
9. Ransomware and Phishing
10. Identifying Phishing Attempts
11. Prevention Strategies & Best Practices
12. Reporting and Responding to Phishing
13. Employee Training and Awareness Programs
14. Takeaways & Action Steps
15. Resources & Further Learning

July 2025

Introduction: The Evolving Threat Landscape

Phishing attacks are the most common cause of data breaches in 2025, with over 90% of cyberattacks beginning with a phishing email.

> Recent developments—like AI-powered attacks—mean that phishing has become harder to detect, more targeted, and increasingly sophisticated.

- Attack volume has increased by 173% compared to previous years
- The human element is present in 68% of all breaches
- Average cost of a phishing breach is now $4.88 million
- Training can reduce phishing incidents by up to 86%

This training arms you with current knowledge and practical guidance to protect yourself and your organization.

July 2025

Phishing in 2025: Key Statistics

91%

of cyberattacks begin with a phishing email

64%

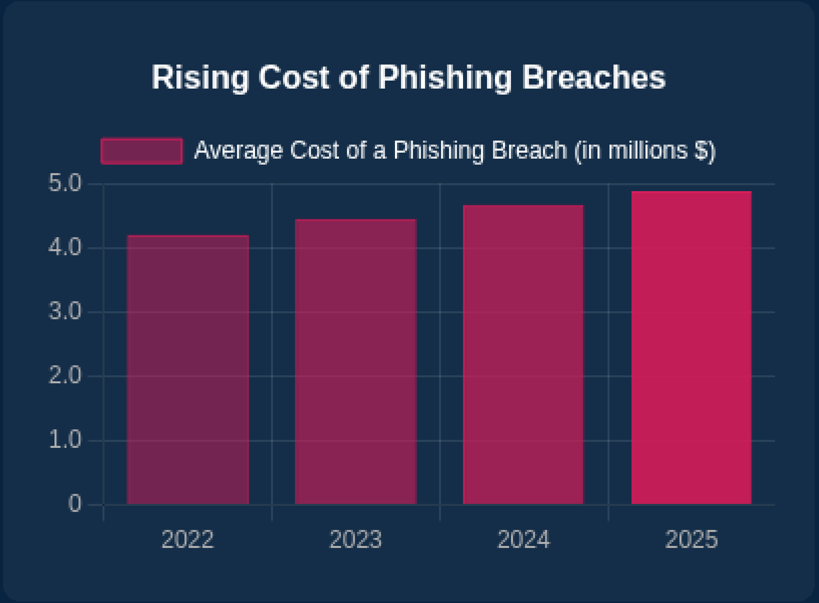
of businesses faced BEC attacks in 2024 (avg. loss: $150,000)

80%

of phishing campaigns aim to steal credentials

86%

reduction in phishing incidents with effective training



Sources: Hoxhunt 2025 Phishing Trends Report, IBM Cost of a Data Breach Report, APWG, KnowBe4

July 2025

What is Phishing?

Phishing is a type of cyberattack that uses deceptive communications to trick individuals into revealing sensitive information or taking harmful actions like downloading malware.

> In 2025, phishing has evolved from simple email scams to sophisticated multi-channel attacks that can be difficult to detect without proper training.

- **Email Phishing**: Fraudulent emails appearing to come from legitimate sources
- **Smishing**: SMS text messages containing malicious links
- **Vishing**: Voice calls designed to extract personal information
- **Quishing**: QR code phishing that increased by 25% in past year
- **Social Media Phishing**: Scams through social platforms and messaging apps

The term "phishing" originated in the 1990s, referencing how attackers use "bait" to "fish" for sensitive information from unsuspecting victims.

Why Everyone Is a Target

Attackers exploit fundamental human psychology to trick individuals regardless of position, technical knowledge, or awareness level.

> No one is immune. Phishing attacks are successful because they target universal human traits rather than technical vulnerabilities.

Authority

People tend to comply with requests from perceived authority figures (bosses, IT department, executives)

Urgency

Time pressure limits critical thinking and encourages immediate action without verification

Fear

Threats of negative consequences trigger emotional rather than logical responses

Curiosity

Natural desire to investigate interesting links, attachments, or unusual messages

Recognizing these psychological triggers is the first step toward building resilience against social engineering attacks.

⚠ SECURITY THREAT LANDSCAPE

Types of Phishing Attacks

Email Phishing

Mass-targeted emails impersonating legitimate organizations to steal data

Spear Phishing

Highly targeted attacks customized for specific individuals or organizations

Whaling

Targets high-value executives and C-level employees specifically

Business Email Compromise

Impersonates executives to request fund transfers or sensitive data

Vishing

Voice phishing over phone calls to trick victims into sharing

Smishing

SMS-based phishing that exploits mobile messaging to deliver

Quishing

Uses malicious QR codes to direct victims to fraudulent websites

Clone Phishing

Replicates legitimate emails with malicious modifications

Real-World Phishing Case Studies

Facebook & Google BEC Scam

$121 Million Lost

A Lithuanian man impersonated a hardware vendor using fake invoices with convincing business documents. Even tech giants with sophisticated security weren't immune.

Children's Healthcare of Atlanta

$3.6 Million Stolen

A scammer impersonated the CFO and convinced the hospital's accounts payable department to update banking information for a legitimate construction vendor.

Treasure Island Homeless Charity

$625,000 Diverted

Attackers compromised the charity's email system, manipulated a legitimate invoice, and changed wire transfer instructions to their own accounts.

Medicare & Medicaid Fraud

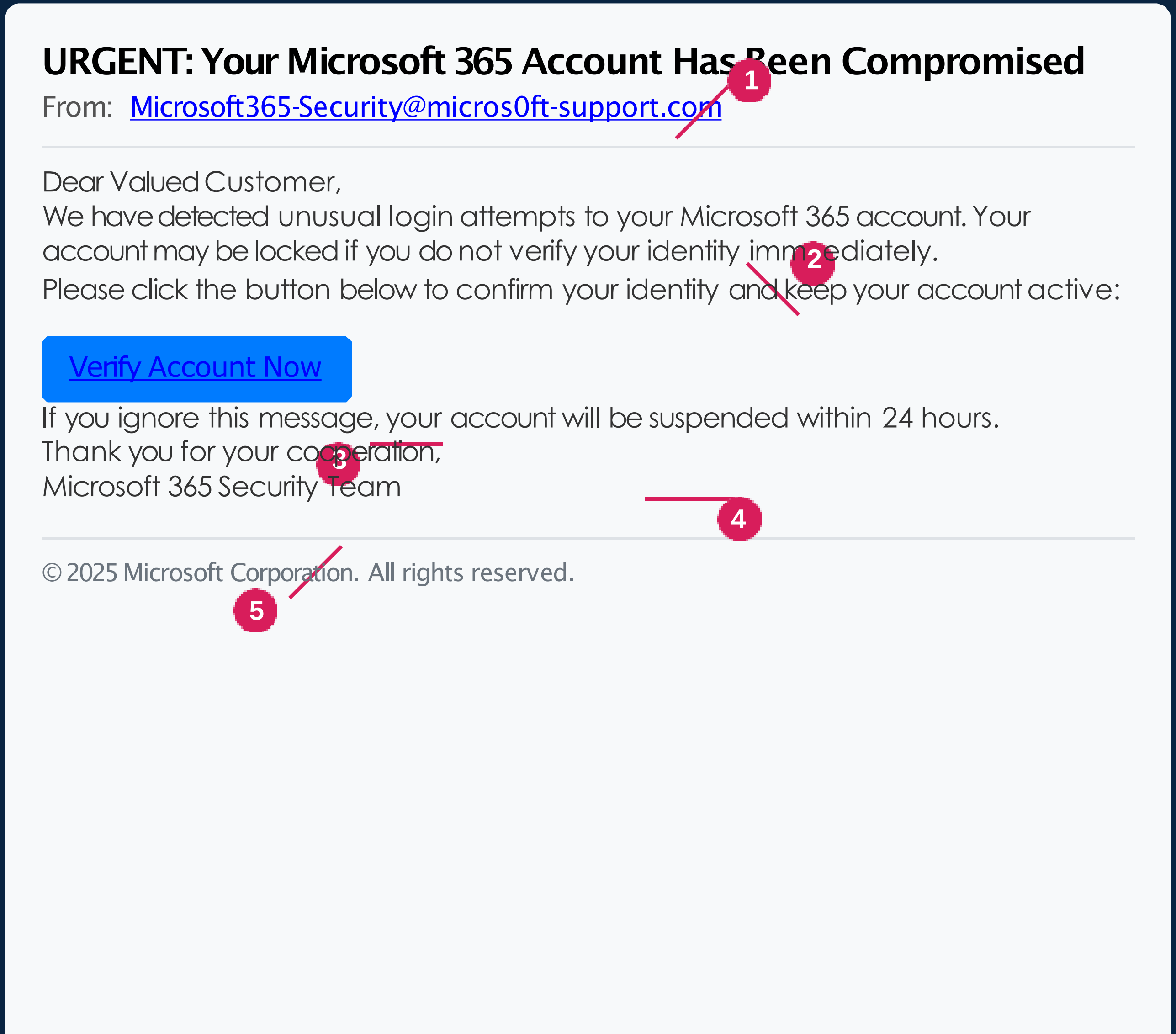
$11.1 Million Drained

Cybercriminals impersonated trusted entities with spoofed emails, convincing five state Medicaid programs to divert payments to fraudulent accounts.

Key Insight

These incidents demonstrate that no organization is immune to phishing attacks—regardless of size, industry, or security maturity. Attacks targeting payment systems and financial transfers are particularly devastating.

Anatomy of a Phishing Email



URGENT: Your Microsoft 365 Account Has Been Compromised

From: Microsoft365-Security@micros0ft-support.com

Dear Valued Customer,
We have detected unusual login attempts to your Microsoft 365 account. Your account may be locked if you do not verify your identity immediately.
Please click the button below to confirm your identity and keep your account active:

Verify Account Now

If you ignore this message, your account will be suspended within 24 hours.
Thank you for your cooperation,
Microsoft 365 Security Team

© 2025 Microsoft Corporation. All rights reserved.

1. Suspicious Domain

Misspelled domain names (micros0ft vs microsoft) or unusual subdomains are common in phishing attempts.

2. Urgency & Fear

Creating urgency with words like "immediate" or "urgent" pressures users into acting without thinking.

3. Suspicious Links

Hover over links before clicking. The actual destination is often different from what the button or text suggests.

4. Threats or Consequences

Threats of account suspension or other negative consequences are common manipulation tactics.

5. Generic Greeting/Signature

Vague sender information or generic greetings instead of your actual name can indicate a mass

Business Email Compromise (BEC)

BEC is a sophisticated email scam where attackers impersonate trusted individuals or companies to trick victims into transferring funds or revealing sensitive information.

> According to the FBI, businesses lost over $2.7 billion to BEC scams in 2022 — more than 25% of all cybercrime-related financial losses that year.

- Typically contains no malware, malicious links, or attachments
- Often targets finance departments, executives, or employees with payment authority
- Leverages social engineering and extensive research of target organizations
- Creates urgent scenarios demanding immediate action (payments, wire transfers)

BEC attacks bypass traditional security measures because they rely on impersonation rather than technical exploits. 75% of organizations experienced at least one BEC attack last year.

Ransomware & Phishing

54%

of ransomware infections begin with a phishing email

22.6%

increase in ransomware payloads in phishing attacks since 2024

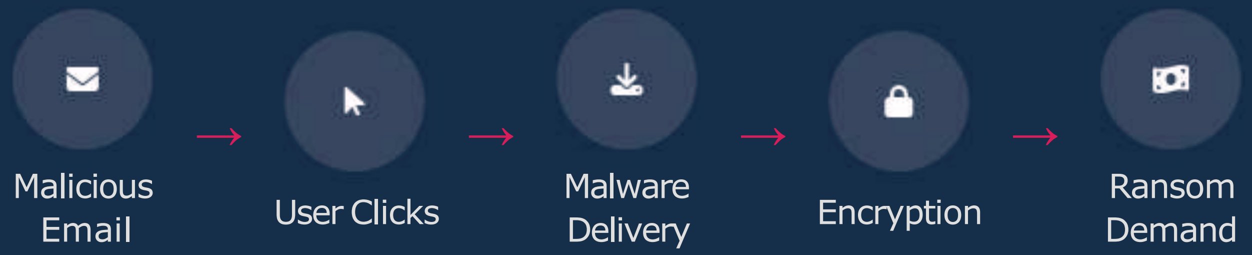
$4.88M

average cost of a phishing-related ransomware breach in 2025

92%

of polymorphic ransomware attacks utilize AI to evade detection

How Phishing Delivers Ransomware



Malicious Email → User Clicks → Malware Delivery → Encryption → Ransom Demand

Prevention Strategies

- Implement regular phishing awareness training and simulations
- Deploy advanced email filtering with AI-powered detection
- Keep all systems and software regularly patched and updated
- Maintain secure, offline backups of all critical data
- Implement strict access controls and network segmentation
- Block macros and executable attachments by default

Identifying Phishing Attempts

Know the warning signs of phishing emails to protect yourself and your organization from social engineering attacks.

> When in doubt, verify through official channels - never use contact information provided in the suspicious email.

✉ **Sender Details:** Examine the sender's email address carefully. Look for slight misspellings or domain variations.

🔗 **Suspicious Links:** Hover over links before clicking. The displayed text and actual URL destination should match.

⚠ **Urgency & Pressure:** Be wary of emails creating a sense of urgency or threatening negative consequences.

📄 **Unexpected Attachments:** Never open attachments you weren't expecting, especially executable files.

Trust your instincts. If an email seems suspicious, it probably is. Take the time to verify before taking any action.

Prevention Strategies & Best Practices

Implementing a multi-layered defense approach provides the most effective protection against phishing attacks.

Technical Controls

Deploy email filtering, DMARC/SPF/DKIM authentication, and secure email gateways to block malicious messages before delivery.

Account Security

Enforce Multi-Factor Authentication (MFA) on all accounts and implement strong password policies with regular rotation.

System Management

Regularly patch and update all systems, applications, and browsers to address known vulnerabilities.

Employee Training

Conduct regular phishing simulations and security awareness training to build a security-minded culture.

Effective security requires a balanced approach combining technology, policies, and human awareness in a continuous improvement cycle.

> Organizations with ongoing security awareness programs see an

How to Report & Respond to Phishing

STOP: Don't Click or Respond

Never click suspicious links, download attachments, or reply to suspected phishing emails. Even checking unsubscribe links can confirm your email is active.

REPORT: Notify Security

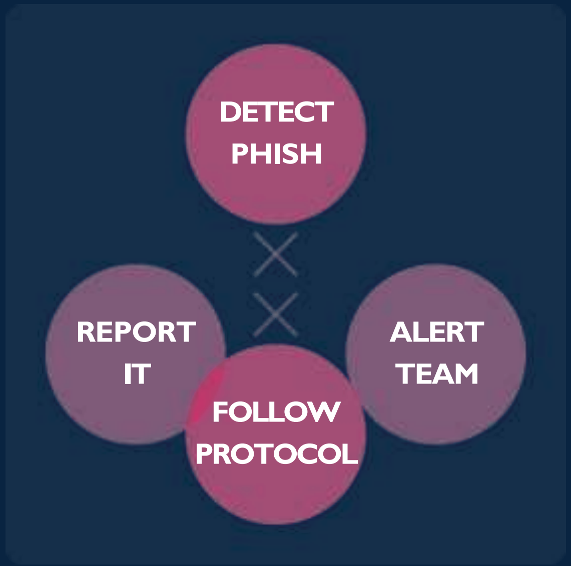
Use your email client's "Report Phishing" button or forward the suspicious email to security@company.com. Include why you think it's suspicious.

ALERT: Inform Colleagues

If appropriate, alert teammates through proper channels about the phishing attempt. Many attacks target multiple employees simultaneously.

FOLLOW: Incident Response

Follow your company's incident response plan if you've already clicked a link or provided information. Speed is critical to minimize damage.



Quick response to phishing incidents dramatically reduces the risk of data breaches and financial loss. Always prioritize reporting.

⚠IF YOU'VE ALREADY CLICKED

If you've already interacted with a suspicious email, immediately disconnect from the network, change your passwords from a different

Resources & Further Learning

CISA Phishing Resources

The Cybersecurity & Infrastructure Security Agency provides free phishing awareness materials, tip sheets, and training resources at cisa.gov/secure-our-world

KnowBe4 Security Training

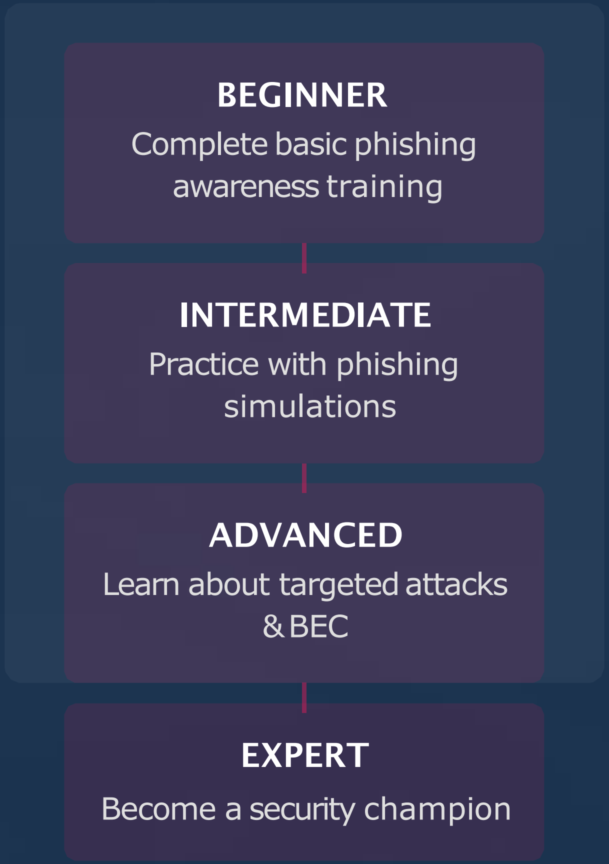
Access our company's KnowBe4 phishing simulation platform for interactive training modules and self-paced courses at company.knowbe4.com

SANS Security Awareness

SANS offers free resources including the "Ouch!" newsletter and security awareness toolkits at sans.org/security-awareness-training

Internal Security Portal

Visit our company's internal security portal for policies, procedures, previous phishing examples, and downloadable quick reference guides at security.company-intranet.com



BEGINNER
Complete basic phishing awareness training

INTERMEDIATE
Practice with phishing simulations

ADVANCED
Learn about targeted attacks & BEC

EXPERT
Become a security champion