THREATNEXIS

Phishing Defense & Employee Training

A Practical Security Guide for Small Business Owners

FREE EDITION | threatnexis.com

2025 Edition · Suitable for businesses with 1–250 employees

91%	**$4.9M**	**82%**
of cyberattacks begin with a phishing email	average cost of a business email compromise attack	of breaches involve a human element — training works

---

What's Inside This Guide

- Why phishing is your biggest threat
- How to recognize phishing emails
- Common attack types explained simply
- Step-by-step employee training guide
- Phishing response checklist
- Quick wins you can implement today
- Employee quiz questions
- Resources and next steps

1. Overview

Phishing is the single most common way cybercriminals break into small business networks. It requires no sophisticated hacking tools — just a convincing email, a distracted employee, and one click. The result can be devastating: stolen credentials, ransomware infections, fraudulent wire transfers, and regulatory penalties.

The good news? With the right awareness and training, phishing is also one of the most preventable threats your business faces. You don't need a dedicated security team or an enterprise budget. You need educated employees, practical processes, and a few smart technical controls.

This guide gives you everything you need to understand phishing, train your team, and reduce your risk — starting today.

2. Why This Matters

Let's be direct: phishing attacks are not just a big-company problem. In fact, small businesses are increasingly targeted precisely because attackers know they often lack the security controls and trained staff that larger organizations have.

REAL-WORLD SCENARIO
A law firm employee receives an email that appears to be from a client requesting a wire transfer to a new account. The email looks legitimate — same name, similar email address. The employee processes the transfer. $85,000 is gone. This is Business Email Compromise (BEC), and it's happening to small businesses every day.

The Business Impact

Financial Loss	Operational Disruption	Reputation Damage
• Stolen funds • Ransomware payments • Recovery costs • Legal fees • Regulatory fines	• System downtime • Data recovery delays • Lost productivity • Client service failures • Staff distraction	• Client trust erosion • Public disclosure • Breach notifications • Contract losses • Business closure risk

3. Risks Addressed

This guide helps you reduce risk from the following threats:

Attack Type	Description	Risk Level
Email Phishing	Generic mass-sent emails designed to steal credentials or install malware	HIGH
Spear Phishing	Targeted emails personalized for a specific employee or organization	CRITICAL
Business Email Compromise	Impersonation of executives or vendors to authorize fraudulent payments	CRITICAL
Smishing	Phishing via SMS text messages linking to malicious sites	HIGH
Vishing	Voice phishing — phone calls impersonating IT support, banks, or vendors	MEDIUM
Whaling	Phishing attacks specifically targeting executives and owners	CRITICAL
Clone Phishing	Duplicating a legitimate email with a malicious link substituted	HIGH

4. How to Recognize a Phishing Email

The most effective defense against phishing is a trained employee who can spot suspicious emails before clicking. Here are the warning signs every team member should know:

The 10 Red Flags of Phishing

1 Sender Address Doesn't Match
The display name says "Microsoft Support" but the actual email address is support@microsoft-helpdesk.xyz. Always check the real sending address, not just the display name.

2 Urgent or Threatening Language
"Your account will be suspended in 24 hours!" Attackers create urgency to pressure victims into acting before thinking. Slow down. Verify.

3 Requests for Credentials or Sensitive Data
Legitimate organizations never ask for your password, Social Security number, or banking information via email.

4 Unexpected Attachments

An invoice from a vendor you don't recognize, a resume from someone you didn't recruit, or a shipping notice you weren't expecting can all be malware delivery vehicles.

5 Suspicious Links
Hover over links before clicking. If the URL destination doesn't match the expected website domain, do not click. Watch for lookalike domains like "apple-support.net" or "microsoft365-login.com."

6 Generic Greetings
"Dear Customer" or "Dear User" instead of your name suggests a mass phishing campaign without personalization.

7 Poor Grammar or Spelling Errors
While attackers are improving, many phishing emails still contain obvious errors in grammar, punctuation, or awkward phrasing.

8 Mismatched Branding
Logos that look slightly "off," incorrect company colors, or outdated email templates are signs the sender may be impersonating a real brand.

9 Unexpected Password Reset Requests
If you receive a password reset request you didn't initiate, do not click the link. Go directly to the website instead.

10 Too Good to Be True
Prize notifications, unexpected refunds, or lottery winnings are classic social engineering tactics. If it sounds too good, it is.

SECURITY MINDSET
Think of email like a stranger handing you a package at your front door. Would you open it before verifying who sent it and why? Your inbox deserves the same caution.

5. Step-by-Step Employee Training Guide

You don't need a Learning Management System or a big training budget to train your team effectively. Here's a practical approach you can implement in your business right now.

Step 1: Start with Leadership Buy-In

Security training only works when leadership takes it seriously. If the owner or manager dismisses security awareness as “just an IT thing,” employees will too.

- Hold a brief all-hands meeting to explain why phishing training matters
- Share a real-world example (ideally from your own industry)
- Make it clear that everyone — including leadership — participates
- Reinforce the message: clicking a phishing link isn’t a firing offense — hiding it is

Step 2: Teach the Basics

Provide every employee with a simple, plain-English overview of phishing. Cover these core topics in a 30-minute session:

1. What is phishing and why attackers use it
2. The 10 red flags of a phishing email (see Section 4)
3. What attackers are trying to steal or accomplish
4. What to do if you receive a suspicious email
5. How to report suspicious emails to the right person

Step 3: Establish Clear Reporting Procedures

Every employee must know exactly what to do when they receive a suspicious email. Create a simple process:

Action	What to Do
STOP	Do not click any links, open attachments, or reply to the email
REPORT	Forward the email to your designated security contact or IT support immediately
FLAG	Mark the email as phishing/spam in your email client (Microsoft 365 has a built-in Report button)
NOTIFY	If you accidentally clicked a link or entered credentials, tell your IT/manager immediately — speed matters
DOCUMENT	Note the date, time, sender, and subject line for the incident record

Step 4: Reinforce Training Regularly

One training session is not enough. Human memory fades. Reinforce security awareness consistently:

- Send monthly “Security Tip of the Month” emails to all staff
- Share phishing examples when you see them in the news or receive them yourself
- Post security awareness reminders in team chat tools (Slack, Teams)
- Conduct brief annual refresher training (30 minutes is sufficient)
- Review and discuss any suspicious emails the team flags

Step 5: Test Your Team (Simulated Phishing)

The most effective training tool is a simulated phishing test — a safe, fake phishing email sent to employees to see who clicks. This is not about punishment; it's about identifying gaps and reinforcing learning.

- Free tools: GoPhish (open source, requires setup)
- Low-cost tools: KnowBe4, Proofpoint Security Awareness Training, Cofense
- Run simulations quarterly at a minimum
- Provide immediate, supportive education to anyone who clicks
- Track your click rate over time — it should decrease

6. Phishing Defense Checklist

Use this checklist to measure and improve your organization's phishing defenses. Priority levels indicate where to focus first.

☐	Action Item	Priority	Effort
PEOPLE & AWARENESS			
☐	Conduct initial phishing awareness training for all employees	High	Low
☐	Create and share a written phishing reporting procedure	High	Low
☐	Designate a security contact / incident reporting point of contact	High	Low
☐	Train employees to verify wire transfer requests via phone	High	Low
☐	Run at least one simulated phishing test this quarter	Medium	Medium
☐	Schedule recurring monthly security awareness communications	Medium	Low
☐	Conduct annual phishing awareness refresher training	Medium	Low
TECHNICAL CONTROLS			
☐	Enable Multi-Factor Authentication (MFA) for all email accounts	High	Low
☐	Enable Microsoft 365 anti-phishing policies (if applicable)	High	Low
☐	Configure external email warning banners in Microsoft 365	High	Low
☐	Enable Safe Links and Safe Attachments in Microsoft Defender	High	Low
☐	Set up DMARC, DKIM, and SPF records for your email domain	High	Medium
☐	Block automatic email forwarding rules to external domains	High	Low
☐	Review email administrator accounts for suspicious access	Medium	Low

7. Common Mistakes to Avoid

⚠ **Treating Security Training as a One-Time Event**
A single 30-minute training session will not protect your business. Phishing tactics evolve constantly, and human memory fades. Build a consistent, ongoing awareness program.

⚠ **Blaming Employees Who Click**
Shaming or punishing employees who fall for phishing attacks creates a culture of fear and silence. When employees are afraid to report mistakes, breaches go undetected far longer. Create a no-blame reporting culture.

⚠ **Trusting the Display Name**
Attackers routinely set display names to impersonate real people. Train employees to always verify the actual email address — not just the name shown.

⚠ **Assuming IT Will Catch Everything**
Email filtering is essential, but no filter catches 100% of phishing emails. Humans are the last line of defense. Technology and training must work together.

⚠ **Ignoring Unusual Payment Requests**
Any unusual request involving wire transfers, gift card purchases, or changes to bank account information should require verbal confirmation via a known phone number — not a reply to the requesting email.

⚠ **Skipping Simulated Phishing Tests**
You cannot know how prepared your team is without testing them. Simulated phishing is the most valuable training investment you can make.

8. Employee Quiz: Test Your Knowledge

Use these quiz questions to reinforce employee training. Review answers together as a team to maximize learning.

Q1. You receive an email from “PayPal Support” asking you to verify your account or it will be suspended. The email includes a link. What should you do?

A) Click the link and log in to verify your account
B) Delete the email and forget about it

C) Do not click the link. Go directly to PayPal's website by typing the address in your browser, and report the email to your security contact.

D) Forward the email to a coworker to ask their opinion

✓ **Correct Answer: C**

Q2. An email arrives from your CEO asking you to urgently purchase $500 in Amazon gift cards for a client. She says she's in a meeting and can't talk. What do you do?

A) Purchase the gift cards immediately since it's urgent

B) Reply to the email asking for more information

C) Call your CEO directly on her known phone number to verify the request before taking any action

D) Forward the request to the accounting department

✓ **Correct Answer: C**

Q3. Which of these is a warning sign of a phishing email?

A) The email is from someone you know

B) The email uses your first name

C) The email address domain looks slightly different from the real company (e.g., support@micros0ft.com)

D) The email has a company logo

✓ **Correct Answer: C**

Q4. You accidentally clicked a link in a phishing email. What should you do first?

A) Restart your computer and hope nothing happened

B) Delete the email

C) Immediately tell your manager or IT contact what happened

D) Change your password for that account later when you have time

✓ **Correct Answer: C**

9. Quick Wins: Act Today

You don't need a project plan to start improving your phishing defenses. Here are five things you can do today:

01	Enable MFA on all Microsoft 365 / Google Workspace accounts. This single control stops 99.9% of automated credential attacks.
02	Enable the "External Email" warning banner in Microsoft 365 so employees see a yellow flag on every email from outside your organization.

03	Send your team a 5-minute email today sharing the Top 10 Phishing Red Flags from this guide.
04	Create a simple reporting process: designate a security contact and tell your team who to forward suspicious emails to.
05	Check your email domain's DMARC record at mxtoolbox.com/dmarc. If you don't have one, ask your IT provider to set it up.

10. Resources & Next Steps

Free Tools & Resources

- CISA Stop Ransomware Guide: cisa.gov/stopransomware
- Google Phishing Quiz: phishingquiz.withgoogle.com
- MxToolbox DMARC Checker: mxtoolbox.com/dmarc
- GoPhish (Open Source Phishing Simulator): getgophish.com
- Microsoft Secure Score: security.microsoft.com

Recommended Reading

- NIST Cybersecurity Framework for Small Business (NIST SP 1800-25)
- FTC Cybersecurity for Small Business: ftc.gov/smallbusiness
- IC3 Business Email Compromise Guide: ic3.gov

THREATNEXIS INSIGHT

The single most effective cybersecurity investment a small business can make is employee awareness training. Technology can be bypassed. An educated employee is your strongest defense.

SEO & Content Strategy Reference

Primary Keyword:

- phishing defense for small business

Secondary Keywords:

- how to train employees to avoid phishing
- phishing awareness training small business
- business email compromise prevention
- employee cybersecurity training
- phishing red flags email

SEO Title:

- Phishing Defense for Small Business: Employee Training Guide [2025]

Meta Description:

- Protect your small business from phishing attacks. Free guide includes how to recognize phishing emails, employee training steps, phishing defense checklist, and quiz questions.

SEO Slug:

- /small-business-phishing-defense-employee-training-guide

People Also Ask:

- How do small businesses protect against phishing attacks?
- What is the best phishing awareness training for employees?
- What are the red flags of a phishing email?
- How much does phishing training cost for small businesses?
- What should employees do if they receive a phishing email?

Internal Linking Suggestions:

- Microsoft 365 Security Hardening Guide
- Multi-Factor Authentication Setup Guide
- Business Email Compromise Prevention Playbook
- Cyber Insurance Readiness Checklist
- Small Business Incident Response Plan

Monetization Opportunities:

- Premium Phishing Defense Toolkit (upsell from this guide)
- Phishing Simulation Campaign Service
- Employee Security Awareness Training Package
- Virtual CISO Consulting Engagement
- Annual Security Awareness Campaign Retainer