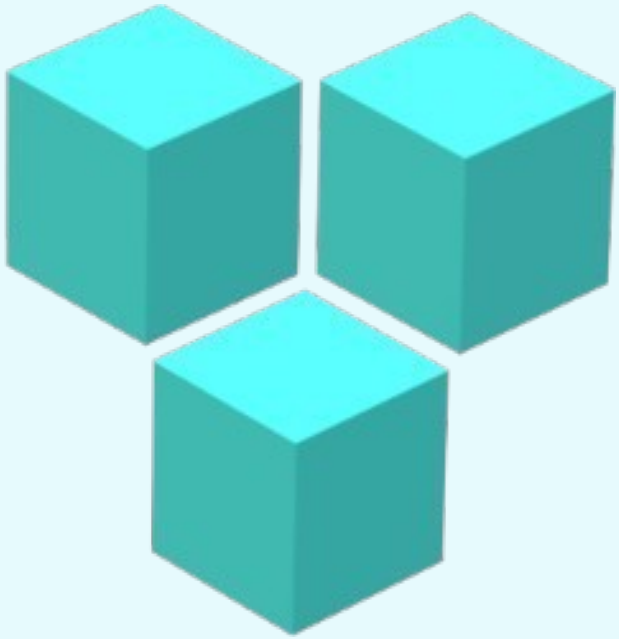

# SofTouch Systems

## How to Spot a Phishing Email

A Simple Guide for Texas Small Businesses

**No-Surprise IT:** Predictable. Proactive. Proven.

© 2025 SofTouch Systems — All Rights Reserved


# How to Spot a Phishing Email

A Simple Guide for Texas Small Businesses

SofTouch Systems  No-Surprise IT © 2025

Cybercriminals don’t break in, they log in.

Phishing emails are the #1 way attackers steal passwords, plant malware, and gain access to a company network. The problem isn’t that people are careless… it’s that phishing emails look more legitimate than ever.

This guide shows your team the exact red flags that reveal a phishing attempt, before they click.

# 1. Check the Sender — It’s Not Who You Think

Attackers spoof familiar names, companies, and even coworkers.

## Red Flags

Display name looks right, but the email address is wrong

(“John from HR” john.hr.support@outlook.com)

Misspellings in the domain

(micorsoft.com, amozon-services.com)

Free email providers for business messages

(Gmail, Yahoo, Hotmail)

Unexpected messages from services you don’t use

## Quick Test

If the sender’s email doesn’t match the company’s real domain → stop.

# 2. Urgency, Pressure, or Fear = Phishing

Phishing relies on emotional manipulation.

### Common Phrases

“Your account will be deleted in 24 hours.”

“Immediate action required.”

“Payroll error — confirm details now.”

“We detected suspicious login attempts. Click to secure your account.”

### Quick Test

If an email tells you to act NOW, take a breath → it’s likely fake.

# 3. Unexpected Attachments or Links

Attackers disguise malware and credential theft inside harmless-looking files.

### Red Flags

PDF, ZIP, HTML attachments you weren’t expecting

“View document” or “Download invoice” with no context

Tracking numbers when you didn’t order anything

Embedded links that redirect multiple times

### Quick Test

Hover your mouse over any link. If the URL is strange, shortened, or unrelated → don’t click.

# 4. Poor Spelling, Grammar, or Formatting

Phishing emails used to be full of bad English, now they’re written by AI.

But subtle mistakes still give them away.

### Red Flags

Odd phrasing or robotic tone

Wrong capitalization or punctuation

Brand logos slightly distorted

Colors or fonts that don’t match the real company

### Quick Test

If something feels “off,” trust your gut → slow down.

## 5. Requests for Passwords or Personal Info

Legitimate companies never ask for sensitive information over email.

### Immediate Deal-Breakers

“Verify your username and password.”

“Send us your Social Security Number.”

“Enter your 2FA code here.”

“Confirm your direct deposit information.”

### Quick Test

If the email asks for anything sensitive → delete it.

## 6. Strange or Unexpected Attachments

Files are the #1 delivery method for ransomware.

### High-Risk File Types

.zip

.html

.exe

.xlsm (macro-enabled Excel)

.iso

.img

“Scanned document” attachments you didn’t request

### Quick Test

If you aren’t expecting it → don’t open it.

## 7. Payment, Invoice, or Banking Changes

This is where small businesses lose money, fast.

### Red Flags

“Update our banking info before sending payment.”

“New invoice attached.”

“We’ve switched accounts, wire funds here instead.”

These attacks impersonate real vendors, clients, or internal staff.

### Quick Test

Always verify payment changes by phone, not email.

## 8. Mismatched Sender vs. Message

If Microsoft emails you about your Dropbox subscription, that’s a scam.

Attackers often mix brands, terms, and products.

### Quick Test

If the sender and the message don’t align → stop.

## 9. Unexpected MFA Alerts

If you receive a 2FA code you didn’t request:

Your password has already been stolen, and the attacker is trying to log in.

### Immediate Steps

Do not approve the request

Change your password immediately

Alert your IT provider

## 10. Trust Your Instincts

If an email feels odd,  even slightly,  it's safer to assume it's malicious until proven otherwise.

Business owners get breached because of hesitation, not overreaction.

When in doubt: Don't click. Forward it to your MSP/IT team.

# QUICK REFERENCE

## The Phishing Red Flag Checklist

✔ Sender email doesn't match the company

✔ Urgent or threatening message

✔ Unexpected attachment or link

✔ Poor grammar or formatting

✔ Requests for passwords

✔ Payment or bank change requests

✔ Too-good-to-be-true offers

✔ Strange login or MFA alerts

✔ Impersonation of leadership (CEO fraud)

✔ Email feels "off"

If any one box gets checked → treat the email as a phishing attempt.

## How STS Helps Protect You

Phishing succeeds when businesses rely on guesswork.

STS eliminates that risk with:

1Password Enterprise Password Manager

Multi-Factor Authentication (MFA) enforcement

Email filtering and threat scanning

Real-time monitoring & alerts

Dark web credential audits

Employee training & testing

Automated backup & recovery

24/7 security-first support

Your people are your frontline, SofTouch Systems is the shield behind them.

## Download This Guide as a PDF

## Want to Protect Your Business from Phishing?

Book a FREE 15-Minute Email Security Audit and see exactly where attacks can succeed.

→ **IT AUDIT**

SofTouch Systems

Simplifying technology, maximizing results.