FIRST UNDERWRITERS INSURANCE BROKERS

Phishing Recognition Guide

How to Spot, Stop, and Report Phishing Attacks

Phishing is the #1 way cybercriminals gain access to business systems. This guide teaches your team how to recognize phishing emails, text messages, and phone calls before they cause damage. Share it with every employee as part of your security awareness program.

A single click on a phishing link can lead to ransomware, data breaches, wire fraud, and business interruption. Training your team to recognize phishing is the most cost-effective security investment you can make.

91%
of cyberattacks start with a phishing email

$4.76M
average cost of a phishing-related breach

3.4B
phishing emails sent every single day

Part of: Cyber Security Essentials for Small Business

Free resource series from First Underwriters Insurance Brokers
www.firstunderwriters.com | (425) 242-5357

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

What Is Phishing?

Phishing is a social engineering attack where criminals impersonate trusted entities to trick people into revealing sensitive information, clicking malicious links, downloading malware, or transferring money. Phishing attacks exploit human psychology — urgency, fear, curiosity, and trust — rather than technical vulnerabilities.

Types of Phishing Attacks

1. **Email Phishing**

   Mass emails impersonating banks, vendors, or services (Microsoft, PayPal, shipping companies). The most common type. Typically contains malicious links or attachments.

2. **Spear Phishing**

   Targeted attacks using personal information about the recipient (name, job title, recent activities). Much harder to detect because the email appears personally relevant and legitimate.

3. **Business Email Compromise (BEC)**

   Attacker impersonates a CEO, CFO, vendor, or business partner to request wire transfers, payment changes, or sensitive data. Often uses a spoofed or look-alike email domain. Causes the largest financial losses.

4. **Smishing (SMS Phishing)**

   Phishing via text message. Often impersonates delivery services, banks, or government agencies with urgent messages containing shortened links that are difficult to verify.

5. **Vishing (Voice Phishing)**

   Phone calls from attackers impersonating IT support, banks, government agencies, or vendors. Caller ID can be spoofed to show legitimate numbers. Often creates urgency to act immediately.

6. **QR Code Phishing (Quishing)**

   Malicious QR codes placed in emails, flyers, or even physical locations that redirect to phishing sites or trigger malware downloads when scanned.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Anatomy of a Phishing Email

Every phishing email contains recognizable patterns. Train yourself to pause and check for these red flags before clicking any link, opening any attachment, or responding to any request.

Suspicious Sender Address

The display name may say "Microsoft Support" but the actual email address is something like support@micros0ft-secure.xyz. Always check the full email address, not just the display name.

Urgency and Threats

"Your account will be suspended in 24 hours" or "Immediate action required." Legitimate organizations rarely threaten account closure via email with tight deadlines.

Generic Greetings

"Dear Customer" or "Dear User" instead of your actual name. Legitimate services that have your account typically address you by name.

Suspicious Links

Hover over any link before clicking. The displayed text may say "microsoft.com" but the actual URL points to "m1crosoft-verify.com" or a completely unrelated domain. Never trust the link text alone.

Unexpected Attachments

Invoices you didn't expect, shipping notices for orders you didn't place, or documents requiring you to "enable macros" or "enable editing" are classic malware delivery methods.

Spelling and Grammar Errors

Professional organizations have editorial processes. Multiple typos, awkward phrasing, or inconsistent formatting are warning signs. However, AI-generated phishing is increasingly error-free.

Mismatched Branding

Slightly wrong logos, incorrect color schemes, unusual formatting, or missing elements that the real company would normally include. Compare against legitimate emails from the same sender.

Requests for Sensitive Information

Legitimate companies will never ask for passwords, Social Security numbers, credit card details, or login credentials via email. Ever.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Phishing Email Examples

Study these common phishing patterns. The more examples you see, the faster you will recognize real attacks. Each example below includes annotated red flags to help you identify the techniques attackers use.

Example 1: Credential Harvesting

From: security-alert@micros0ft-account.com

Subject: Unusual sign-in activity on your account

We detected unusual sign-in activity on your Microsoft account. Someone may have accessed your account without your permission. Please verify your identity immediately by clicking the button below.

[Verify Your Account Now]

If you don't verify within 24 hours, your account will be permanently suspended.

RED FLAGS:

- Spoofed sender: "micros0ft" with a zero instead of 'o', fake domain
- Creates urgency with 24-hour deadline and account suspension threat
- Generic message — no account name, no specific sign-in details
- Link button likely redirects to a credential-harvesting fake login page

Why This Works

Credential harvesting emails are the most common type of phishing. They exploit the fear of losing access to an important account. The attacker creates a fake login page that looks identical to the real one. When you enter your username and password, those credentials go straight to the attacker.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Business Email Compromise

BEC attacks are the most financially damaging form of phishing. Unlike mass email campaigns, these are carefully targeted and researched. The attacker studies the company's leadership, communication style, and payment processes before striking.

Example 2: CEO Fraud / Executive Impersonation

From: j.smith.ceo@company-mail.net

Subject: Urgent — Wire Transfer Needed Today

Hi Sarah,
I'm in a meeting and can't talk. We need to process a wire transfer of $47,500 to finalize an acquisition. The details are attached. Please handle this before 3pm today and confirm when done.
Keep this confidential until the deal closes.
Thanks, John Smith, CEO

RED FLAGS:

- Look-alike domain: "company-mail.net" instead of the real company domain
- Requests urgency and secrecy — classic BEC manipulation tactics
- CEO impersonation with "can't talk" to prevent voice verification
- Wire transfer request with artificial deadline; always verify by phone

BEC by the Numbers

The FBI reports BEC losses exceeding $2.9 billion per year in the U.S. alone. The average BEC incident costs $125,000. These attacks succeed because they exploit trust and authority rather than technology. Always verify payment requests through a separate phone call.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

More Attack Examples

Example 3: Vendor Invoice Fraud

From: accounts@vendor-payments-portal.com

Subject: Updated Banking Information — Invoice #4892

Dear Accounts Payable,
We have changed our banking details effective immediately. Please update your records and direct all future payments to the new account below:
Bank: First National Trust | Routing: 071923456 | Account: 89012345
Please apply this change to the outstanding invoice #4892 ($23,400). If you have questions, reply to this email.

RED FLAGS:

- Unsolicited banking change request — the #1 vendor fraud technique
- Uses a fake portal domain, not the vendor's real email address
- Asks you to reply to THIS email rather than calling the vendor directly
- Legitimate vendors announce banking changes via formal letter and phone confirmation

Smishing (Text Message) Examples

USPS: Your package cannot be delivered due to an incorrect address. Update your information at: usps-delivery-update.com/track/7839

Fake USPS link — real USPS uses usps.com only. Don't click shortened or unfamiliar URLs.

Chase Bank: We detected unauthorized activity on your account ending in 4892. Verify now: chase-secure-alert.com or call 1-800-555-0147

Fake Chase domain and spoofed phone number. Call the number on the back of your card instead.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

The S.T.O.P. Method

When you receive any unexpected email, text, or call requesting action, use the S.T.O.P. method to protect yourself and your organization:



S — Stop

Pause before reacting. Phishing relies on getting you to act impulsively. Take a breath. If a message creates a sense of panic or urgency, that itself is a red flag.

T — Think

Ask yourself: Was I expecting this? Does the request make sense? Would this person or organization normally contact me this way? Does anything look off about the sender, formatting, or content?

O — Observe

Check the sender's full email address (not just display name). Hover over links without clicking. Look for the red flags covered in this guide. Compare against known legitimate communications.

P — Protect

If anything seems suspicious, do NOT click, reply, or provide information. Report the message using your company's reporting process. If in doubt, verify through a separate, known channel (call the sender using a number you already have, not one from the suspicious message).

Remember: No Legitimate Organization Will...

Ask for your password or full Social Security number via email, text, or phone.
Threaten to close your account unless you click a link within hours.
Ask you to bypass your company's normal approval processes for payments.
Tell you to keep a transaction or request secret from your colleagues or manager.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

How to Report Phishing

Reporting phishing attempts is critical. Even if you didn't click, reporting helps your IT team block threats for the entire organization and improves your email filters over time.

1. **Don't Click, Reply, or Forward**

   Do not interact with the suspicious message in any way. Don't forward it to colleagues to "warn them" — this can spread the threat.

2. **Use the Report Phishing Button**

   Most email platforms (Outlook, Gmail) have a built-in "Report Phishing" or "Report Junk" button. Use it. This trains your organization's email filters and alerts IT.

3. **Forward to Your IT/Security Team**

   If no report button is available, forward the suspicious email to [phishing@yourcompany.com] or notify [IT Help Desk / Security Contact] directly.

4. **Delete the Message**

   After reporting, delete the message from your inbox. Empty your deleted items folder as well.

What to Do If You Clicked

If you accidentally clicked a link, opened an attachment, or provided information, act quickly. Speed matters — the faster you respond, the less damage an attacker can do.

1. **Disconnect immediately**

   Disconnect your device from the network (turn off Wi-Fi, unplug ethernet). This limits the attacker's ability to move through your network.

2. **Report to IT right away**

   Contact [IT Help Desk / Security Contact] immediately. Be honest about exactly what happened — what you clicked, what information you entered, and when. There is no penalty for reporting honestly.

3. **Change your passwords**

   If you entered credentials on a phishing site, change that password immediately (from a known clean device). Change it everywhere you use that same password.

4. **Monitor your accounts**

   Watch for unusual activity on the affected accounts. Enable alerts for login attempts and transaction notifications where available.

5. **Document what happened**

   Write down the timeline: when you received the message, when you clicked, what you entered, and what happened afterward. This helps the incident response team.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

How to Verify Links & URLs

Learning to read URLs is one of the most valuable skills for avoiding phishing. Attackers rely on the fact that most people don't check where a link actually goes.

How to Hover-Check a Link

- On a computer: hover your mouse over the link WITHOUT clicking. The actual URL appears in the bottom-left corner of your browser or in a tooltip.
- On a phone: press and hold the link (don't tap). A preview of the URL will appear.
- In email: right-click the link and select "Copy link address" to inspect it in a text editor.

Spotting Fake URLs

LEGIT:	`https://login.microsoft.com/account`
FAKE:	`https://login.micros0ft-secure.com/account`
FAKE:	`https://microsoft.com.login-verify.xyz/account`
FAKE:	`https://secure-login.com/microsoft/account`

> **The Domain Name Rule**
>
> The REAL destination is determined by what comes immediately BEFORE the first single slash (/). In "microsoft.com.login-verify.xyz/account" the real domain is login-verify.xyz, NOT microsoft.com. Everything before the domain is a subdomain that anyone can create to look legitimate.

URL Red Flags Checklist

- Misspelled company names (micr0soft, arnazon, paypa1, app1e)
- Extra words or hyphens in the domain (microsoft-security-verify.com)
- Unusual top-level domains (.xyz, .top, .buzz, .click) for major companies
- IP addresses instead of domain names (http://192.168.1.50/login)
- Extremely long URLs with random characters designed to hide the real domain
- URL shorteners (bit.ly, tinyurl) in official-looking emails — legitimate companies use their own domains

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Wire Fraud & Payment Scams

Business Email Compromise (BEC) and wire fraud cause more financial damage than any other type of cybercrime. The FBI reports over $2.9 billion in losses from BEC in a single year. These attacks specifically target employees who handle payments, invoices, and financial transactions.

Common BEC Scenarios

CEO / Executive Impersonation

Attacker poses as the CEO or CFO, emails an employee in finance with an urgent, confidential wire transfer request. Often happens when the executive is known to be traveling or in meetings.

Vendor Payment Redirect

Attacker sends an email appearing to come from a known vendor, requesting updated banking details for future invoice payments. All subsequent legitimate payments go to the attacker's account.

Attorney Impersonation

Attacker poses as outside legal counsel handling a confidential acquisition or settlement. Uses urgency and secrecy to pressure the target into making a payment without normal approval processes.

Payroll Diversion

Attacker impersonates an employee and emails HR/payroll requesting a change to their direct deposit bank account. The employee's next paycheck goes to the attacker.

> **The Golden Rule for Wire Transfers & Payment Changes**
>
> ALWAYS verify any request to send money, change payment details, or redirect invoices through a SEPARATE phone call to a KNOWN number (not a number from the email). This single step prevents the vast majority of BEC losses. Build this verification into your standard accounts payable procedures.

This guide is for informational purposes only and does not constitute professional cybersecurity advice.

Quick Reference Card

Print this page and keep it at your desk as a daily reminder.

Top 10 Phishing Red Flags

1. Unexpected email requesting urgent action
2. Sender address doesn't match the claimed organization
3. Generic greeting ("Dear Customer") instead of your name
4. Links that don't match the displayed text (hover to check)
5. Requests for passwords, SSN, or financial details
6. Threats of account suspension or legal action
7. Unexpected attachments, especially .zip, .exe, or macro-enabled files
8. Too-good-to-be-true offers or prize notifications
9. Pressure to bypass normal procedures or keep things secret
10. Spelling errors, awkward grammar, or mismatched branding

S Stop | **T** Think | **O** Observe | **P** Protect

Report Phishing To:

Email: [phishing@yourcompany.com] | Phone: [IT Help Desk number]
Or use the "Report Phishing" button in your email client.

Does Your Cyber Insurance Reward Security-Aware Teams?

First Underwriters helps businesses find coverage that recognizes your security investments.

www.firstunderwriters.com | (425) 242-5357

This guide is for informational purposes only and does not constitute professional cybersecurity advice.