# How to Spot a Phishing Email

A plain-English guide to catching the bad guys before you click.

We all get them. The sudden alert that your account is locked, an unexpected invoice for a service you didn't buy, or a rushed email from your "boss" asking for a quick favor. Cybercriminals are getting smarter, and their fake emails—known as **phishing**—are designed to look exactly like the real thing.

The goal? To trick you into handing over your passwords, downloading malicious software, or sending them money. Let's break down the three most common phishing traps and exactly what red flags you need to look out for.

## 1. The "Urgent Password Reset"

This is the oldest trick in the book. The scammer tries to create a sense of panic so you act before you think. They usually pretend to be a service you trust, like Microsoft, Google, or your bank.

**From:** IT Support <**admin@micro-soft-security.com**>

**To:** Employee

**Subject:** **URGENT:** Your Account Will Be Suspended in 24 Hours

---

**Dear Customer,**

We have detected unusual sign-in activity on your account. To prevent immediate suspension, you must verify your identity.

**Please click the link below to log in and secure your account:**

**Verify Account Now**

Thank you,
IT Security Team

> 🚩 **Red Flags to Spot:**
>
> - **The Sender Address:** Look closely at the "From" address. It says "micro-soft-security.com". Real Microsoft emails come from *@microsoft.com*. Scammers use look-alike domains.
> - **Artificial Urgency:** Phishing emails often threaten account suspension or use words like "URGENT" to rush you.
> - **Generic Greeting:** "Dear Customer" or "Dear Employee" is a major warning sign. Legitimate services usually know your name.
> - **The Hidden Link:** If you were to hover your mouse over that blue button (without clicking!), the little popup at the bottom of your screen would show a strange website address, not a real login page.

## 2. The "Fake Invoice"

This tactic targets your fear of being charged for something you didn't buy, or tries to trick accounts payable departments into paying a fraudulent bill. The danger here often lies in a malicious attachment.

**From:** Billing Department <billing@xyz-logistics-llc.com>

**To:** You

**Subject:** Invoice #9932 Overdue

**Attachment:** **Invoice_9932.pdf.exe** (1.2 MB)

---

Hi,

Please find attached the overdue invoice for your recent shipment. As per our terms, please process this payment immediately to avoid late fees.

If you have questions about these charges, **open the attached document** for full details.

Regards,
Accounts Receivable

> 🚩 **Red Flags to Spot:**
>
> - **Weird File Extensions:** The attachment is named *.pdf.exe*. An ".exe" is an executable program, not a document. Opening this will install malware on your computer. Also beware of unexpected .zip or .docm files.
> - **Vague Details:** They don't mention what you bought, when you bought it, or even your company's name. They want you to be confused so you open the attachment to investigate.
> - **Unexpected Sender:** If you don't recognize the vendor, don't open their attachments.

## 3. The "Spoofed Boss" (CEO Fraud)

Also known as Business Email Compromise (BEC). Scammers impersonate a CEO, director, or manager and email a junior employee. They rely on the fact that most employees want to quickly please their boss.

**From:** Sarah Jenkins <**ceo.sarah.jenkins@gmail.com**>

**To:** You

**Subject:** Quick request - Are you at your desk?

---

Hey,

**I am stuck in a board meeting right now and can't take calls.** I need you to do a quick task for me.

I need to send some client gifts today. Can you **purchase five $100 Apple gift cards** and reply to this email with the scratched-off codes on the back? I will expense you back before the end of the day.

Thanks,
Sarah
Sent from my iPhone

🚩 **Red Flags to Spot:**

- **The Email Address:** The display name says "Sarah Jenkins" (your real boss), but the email is a random Gmail address. The boss would use their official company email.
- **The "I'm Busy" Excuse:** Scammers always say they are in a meeting or on a plane. This is to stop you from picking up the phone and calling them to verify the request.
- **Gift Cards or Wire Transfers:** No legitimate business transaction requires you to buy iTunes, Apple, or Amazon gift cards. If someone asks for gift cards, it is a scam 100% of the time.

## The 5 Golden Rules of Phishing Defense

- **Stop and Breathe:** Phishing relies on panic and urgency. Slow down.
- **Check the Sender:** Always expand the "From" address to see the actual email, not just the display name.
- **Hover, Don't Click:** Hover your mouse over links to preview the actual destination URL before clicking.
- **Verify Independently:** If a boss asks for an unusual wire transfer or gift card, call them on a known number to confirm.

- **Report It:** Don't just delete it. Use your company's "Report Phishing" button so IT can protect everyone else.