Phishing field guide

How to spot a scam email, check a link without clicking it, and what to do when one gets through.

Phishing is an email (or text) that pretends to be someone you trust so you'll sign in, pay or open something. Filters catch most of them. The ones that get through are made to look real, so the last line of defense is you.

A real-looking example

From Accounts Payable <billing@yourvendor-invoices.com> 1
Subject URGENT: Overdue invoice #48213, service stops today 2

Hello,

Our records show invoice #48213 is 30 days past due. To avoid interruption, payment must be received **by 5:00 PM today**. 2

Please review the invoice here: View Invoice (Secure Document) 3

You will need to sign in with your work email to open it. 4

Note: our bank details have changed. Please use the new account listed in the document. 5

1. **The sender's address doesn't match.**
   The name looks right, but the address is a lookalike, not the vendor's real one.
2. **Rush and a threat.**
   "Today", "service stops", "urgent". Pressure is there to stop you from checking.
3. **A link to a "secure document".**
   Shared files and invoices are the most common bait.
4. **It asks you to sign in.**
   A real invoice doesn't need your email password to open.
5. **New bank details.**
   Always confirm by phone, on a number you already have.

Check a link without clicking it

- [ ] **On a computer:** rest the mouse on the link (don't click). The real address shows at the bottom of the window.
- [ ] **On a phone:** press and hold the link to preview the address. Don't tap Open.
- [ ] **Read the address right to left** from the first single slash. The last two parts before it are who really owns the site.

> **Which site is this, really?**
> In **yourbank.com.secure-login.net/account** the real site is **secure-login.net**, not your bank. Anything to the left is decoration a scammer can type.

Lookalike tricks to watch for

- Swapped letters: **rn** for **m**, **1** for **l**, **0** for **o** (rnicrosoft, paypa1).
- Extra words: yourbank-support.com, yourbank-secure.net.
- A real company's name in front of a strange ending: yourbank.co, yourbank.info.
- Your own boss's name with a personal email address.

What to do with a suspicious email

1. **Don't click, reply or open attachments.**
   Even "unsubscribe" links can be traps.
2. **Forward it to check@scan.fluxlabs.net.**
   You'll get a free verdict back by email in a few minutes.
3. **Or use the Report button in your email program**
   if your business has one, so it's pulled from everyone's inbox.
4. **Clicked or typed something already?**
   Call your IT support now. Fast is what matters, not blame.