CICADA | RESOURCES

LESSON 02 OF 04 · 7 MIN · ESSENTIAL

The anatomy of a phishing email

What to check when the email looks right, what QR codes change, and what to do if you've already clicked.

It looks like email you already get

Phishing copies the shape of normal work: a shared document, a voicemail, a delivery, an invoice, a password expiry. The link may go to a convincing login page, or the attachment may be an HTML file that opens locally and asks for your password.

Check the actual sender address, not just the display name. Hover or long-press a link before clicking. Look at the reply-to. Ask whether you were expecting this specific document from this specific person.

The clues that survive good forgery

- A lookalike domain: `supplier.co` instead of `supplier.com`, or an extra word.
- A reply-to address that differs from the sender.
- An unexpected attachment, especially ZIP, ISO or HTML.
- A QR code used to “log in” or “verify”, it moves the attack to your phone, away from email filters.
- A login page reached from a link, asking for your existing password.
- Pressure to act before you can think.

If you've already clicked

Don't hide it. Disconnect the device from Wi-Fi, tell IT or your provider, and change the affected password from a different device. Check for new inbox rules, forwarding addresses and active sessions. If you entered a code, assume the account is compromised until proven otherwise.

Reporting quickly is the single most useful thing an employee can do.

> **REPORT, DON'T JUST DELETE**
>
> A deleted phishing email teaches nobody. Reporting it lets your provider block the sender and warn everyone else who received it.

Key takeaways

- ✓ Check the real sender address, link destination and reply-to.
- ✓ Unexpected attachments and QR codes deserve extra suspicion.
- ✓ If you clicked, disconnect and report immediately.
- ✓ A no-blame report culture is a security control.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.