DIRECTIVE TECHNOLOGY

CYBERSECURITY TIP SHEET

How to Spot a Fraudulent Phishing Email

A practical checklist for your team

Phishing Is the #1 Way Businesses Get Breached

More than 90% of cyberattacks start with a phishing email. Modern phishing is well-written, branded, and personalized — gone are the days of obvious typos and Nigerian princes. Training your team to pause before they click is the single highest-impact security investment you can make.

Red Flags to Look For

- Sender address that almost matches a real domain (micros0ft.com, amaz0n-billing.com)
- Urgent or threatening language — 'your account will be closed in 24 hours'
- Requests for credentials, wire transfers, gift cards, or tax information
- Generic greetings like 'Dear Customer' on accounts that know your name
- Unexpected attachments, especially .zip, .iso, .htm, or password-protected files
- Links whose visible text doesn't match the actual URL (hover before clicking)
- Replies to threads you were never part of, or invoices you didn't request

The 10-Second Verification Rule

If a message asks you to do something with money, credentials, or sensitive data, stop and verify through a second channel before acting. Call the sender at a known phone number — never one provided in the email. Ten seconds of verification can prevent a six-figure loss.

What to Do If You Click

- Disconnect the device from Wi-Fi and Ethernet immediately
- Notify your IT or security team — speed of response limits damage
- Change passwords for any accounts entered, from a clean device
- Watch bank, payroll, and email accounts for unauthorized activity

Build a Phishing-Resistant Culture

Directive Technology runs realistic phishing simulations and ongoing security awareness training that turns your staff into your strongest layer of defense — not your weakest link.