

Phishing Red Flags

AI removed the spelling mistakes. It can't remove what the attacker needs from you. If you see any of these, don't trust it.

The 7 red flags that still work

- **The sender is almost right.** Check the actual address, not the display name. `microsoft-help.co` is not Microsoft.
- **There's a deadline.** "Within 24 hours", "before end of day". Urgency is there to stop you thinking.
- **It's generic, or oddly personal.** "Dear customer", or a message that knows a surprising amount about you.
- **The link goes elsewhere.** Hover (computer) or press and hold (phone) to see the real address.
- **It asks for something it shouldn't.** A password, a one-time code, a payment, new bank details, your ID.
- **There's a threat or a prize.** Lose access, pay a fine, miss a delivery. Or win something, or get a refund.
- **You weren't expecting it.** An invoice, a shared file or a password reset you didn't ask for.

Read a link in 5 seconds

Read the address **from right to left**, starting just before the first single `"/`. That part is who you're really talking to.

`https://αphαtechs.al/login` real ·
`https://αphαtechs.al.secure-login.com` fake ·
`https://αIphαtechs.al` fake (capital i)

It's not only email

- **SMS:** "Parcel on hold, pay €1.99". Open the courier's app instead.
- **QR codes:** check the address your phone shows before you open it.
- **WhatsApp:** a "new number" from a colleague or relative? Call the old one.
- **Phone calls:** the bank or IT never needs your code. Hang up and call back.

62%

of breaches involve the human element (Verizon DBIR 2026)

44%

of AI-assisted initial access is phishing (Verizon DBIR 2026)

24/7

Alphatechs security operations, 30-minute response

• UNVERIFIED



```
> trust = 0; verify --all
```

Clicked? Do this now

1. **Don't hide it.** Speed matters more than pride.
2. **Entered a password?** Change it from another device, starting with your email.
3. **Entered card details?** Call your bank on the number on your card.
4. **Opened a file?** Disconnect from the network.
5. **Tell IT** straight away, even if you're not sure.

The rule that beats all 7

Trust nothing: not the sender, not the link, not the deadline. **Verify everything:** open the app or type the address yourself, or call a number you already have.

Report suspicious messages to

Why Alphatechs

24/7 security operations with a 30-minute response, penetration testing, and Sphere TI, our own threat intelligence platform. Built by a team that defends businesses in one of Europe's most targeted countries.

Take the Next Step

Are your company's passwords already exposed? Get a free Exposure Report at sphereti.com