SECURITY ADVISORY • PHISHING EMAIL AWARENESS

Even if the email looks real It might still be *a scam*.

01 ANATOMY OF A PHISHING EMAIL

TODAY, 9:14 AM

FROM: Microsoft Security <security@rnicrosoft.com> 1

SUBJECT: **Account suspended in 24 hours** 2

Dear customer, 3

Your account will be suspended if you don't verify your password in the next 24 hours: 4

Verify Account Now → 5

Account_Notice.zip 6

1. Lookalike domain
2. Urgency
3. Generic greeting
4. Asks for credentials
5. "Verify" button
6. Unexpected attachment

STOP

If you're not 100% sure, **don't click.**

02 HOW TO VERIFY IF IT'S A SCAM

Did you expect this email?
If NO, and it's asking you to click, log in, or send something, treat it as untrusted by default.

Don't act. Pause and verify
The attacker counts on you reacting fast. Pause before clicking, replying, or opening attachments.

Inspect the sender and every link.
Hover over the email and link. Even if the link looks real, it could be masked. Don't trust it.

Verify through a separate channel
Don't reply or use any contact info from the email. Type the company's URL yourself or call directly.

Report it, then delete.
Forward to your IT support or use the "Report" button. Then empty it from trash.

Email: hello@blackswancyber.co.uk
Phone: 01246 927142

BLACK SWAN
CYBER SECURITY SOLUTIONS