unity
unifying...

How protected is your business?

Twelve quick questions to find the gaps Phish could swim through. Be honest: “not sure” counts as a gap.



QUESTION	YES	NOT SURE	NO
Accounts			
1. MFA is switched on for email and Microsoft 365. A stolen password alone isn’t enough.	☐	☐	☐
2. Passwords are unique and kept in a password manager.	☐	☐	☐
3. Leavers’ accounts are closed straight away.	☐	☐	☐
People			
4. Staff know the common red flags. Invoices, resets, deliveries, urgency, mismatched senders.	☐	☐	☐
5. Everyone knows who to report a suspicious message to.	☐	☐	☐
6. Bank detail changes are always checked by phone.	☐	☐	☐
Systems			
7. Devices and software update automatically.	☐	☐	☐
8. Email filtering and security software are in place.	☐	☐	☐
9. Backups are tested, not just switched on.	☐	☐	☐
Readiness			
10. You know exactly what your IT provider covers for security. In writing, not just “we look after it”.	☐	☐	☐
11. You’d know what to do in the first hour after a click.	☐	☐	☐
12. You have Cyber Essentials, or know whether you need it.	☐	☐	☐

Your result: could Phish catch you?

Unity World

Count your “Yes” answers.

10–12
Phish would struggle to catch you. Keep it that way with regular reviews.

6–9
Phish could still find a way in. A few gaps are worth closing soon.

0–5
Phish could catch you. Let’s fix the biggest gaps first.



“Plenty more fish in the sea…”

Make sure yours isn’t one of them.

Book a review with a Unity advisor. We’ll look at your answers, find the gaps and give you a clear plan. **[unity.world/review]**