unity
unifying...

Meet Phish.

Something's fishy.

Phish is the sly blue fish behind every phishing email, text and call. This guide explains why businesses like yours are targeted, and the warning signs to look out for.



What is phishing?

Phishing is when someone pretends to be a person or organisation you trust, such as a supplier, your bank, Microsoft or even your boss, to trick you into clicking a link, sharing a password or sending money.

What Phish is after

Passwords
One login can open your email, files and accounts.

Money
Fake invoices and "new" bank details send payments to the wrong place.

Data
Customer and staff details are valuable to sell or use again.

Access
A way into your systems to cause disruption later.

Why small businesses get targeted

Busy teams
People are juggling a lot, so a quick click is easy.

Fewer checks
Payments and changes often rely on one person.

Supply chains
You're a route into bigger customers and suppliers.

The 5 red flags Phish hopes you'll miss

Unity World

If a message shows any of these signs, stop and check before you do anything.

1. **Unexpected invoices or payment requests**
   Especially a supplier "changing bank details".
2. **Password reset requests you didn't make**
   The link leads to a convincing fake login page.
3. **Delivery notifications for parcels you're not expecting**
   A "held" parcel, a small fee and a link to pay it.
4. **Urgent or threatening language pushing you to click quickly**
   "Act now or lose access." Pressure stops you thinking.
5. **Sender addresses or links that don't match who they claim to be**
   The name looks right, but the address or web link doesn't.

Not just email

Texts
A link plus urgency, often about a parcel, bank or refund.

Phone calls
A caller asking for codes, passwords or remote access.

QR codes
A code in an unexpected place leading to a fake page.

"Boss" requests
An urgent payment or gift cards, "just this once".



Your first habit: Stop. Spot. Report.

Stop before you click. **Spot** the red flags. **Report** it to your nominated person so everyone else is protected. Nobody gets in trouble for checking.