unity
unifying...

What happens after a click?

One click can give Phish a way in. This guide shows how quickly it moves from click to compromise, and exactly what to do straight away.



From click to compromise

THE BAIT
09:02
A "supplier" emails to say their bank details have changed.

THE BITE
09:05
It looks urgent and the team is busy. The link gets opened.

THE HOOK
09:06
A password is typed into a fake page. Phish has the keys.

THE CATCH
09:40
A payment goes to Phish, and customers get fake emails too.

A fictional example.

The damage that can follow

Financial
Payments sent to the wrong account, and the cost of putting things right.

Operational
Locked accounts, lost files and time spent recovering instead of working.

Data loss
Customer and staff information exposed or stolen.

Reputation
Customers receive scam emails from your real address.

I’ve clicked. What now?

Clicked, replied or typed a password by mistake? Speed matters more than blame. Work through this checklist straight away.

Incident response checklist

- [ ] **Tell your nominated person or IT provider immediately.**
  The sooner they know, the more they can stop. Nobody gets in trouble for reporting.
- [ ] **Disconnect the device from the network if you opened a file.**
  Unplug the cable or switch off Wi-Fi. Don’t turn it off unless told to.
- [ ] **Change the password you entered, from a different device.**
  And anywhere else that password is used.
- [ ] **Check MFA is switched on for that account.**
  Look for sign-ins or MFA prompts you don’t recognise.
- [ ] **Call your bank straight away if money or bank details were involved.**
  Use the number on your card or statement.
- [ ] **Check your sent items and email rules.**
  Attackers often set up forwarding rules or send emails as you.
- [ ] **Warn colleagues and, if needed, customers.**
  So nobody else takes the same bait.
- [ ] **Write down what happened and when.**
  Keep the message. Don’t delete it, as it helps the investigation.
- [ ] **Report it to the police’s fraud reporting service if money was lost.**
  Forward suspicious emails to report@phishing.gov.uk and texts to 7726.