**Q:** We have a good password policy.

**FAQs: Ask a Hacker**

*A friendly Q&A with your least favourite guest*

**A:** And I have good software. One cracked password is all I need. You sure no one’s using "Password" or "iloveyou"? Because I’m betting, they are.

**Q:** Our staff are trained not to click dodgy links.

**A:** Until they’re tired, rushed, under pressure, or the email looks like it is from their boss. Your training is good - I’m just better at Monday mornings.

**Q:** We outsource all our IT - they handle security.

**A:** Brilliant! So, when I get in through them, do I get a loyalty card? Do they have things like ISO 27001 or DSPT - or just a nice logo and a mate who built their website? Because when it goes wrong, nobody says, “Oh no, that was the supplier’s data.” It’s your name in the headlines.

**Q:** All our devices are encrypted.

A: Sweet. But if I send a malicious link and someone clicks it before the screen locks - encryption doesn’t matter. You lock the door *after* I’m already on the sofa.

**Q:** We only use secure cloud storage now.

**A:** Right - and nobody ever drags files to their desktop “just for now”? Or uses their personal Dropbox because it’s easier? I love a rebel.

**Q:** Our staff get annual cyber training.

**A:** So do I! Every time someone sends me an email chain with login details or forwards a dodgy link “just in case.” You’ve trained them - but have you *tested* them lately?

**Q:** We’re just social care - who’d come after us?

**A:** Honestly? No one. Not you, anyway. I don’t even know who you are - I’m scanning the internet for vulnerabilities, not names. Outdated software, forgotten plug-ins, exposed logins... I don’t pick targets, I pick doors that are already open. Yours just happens to be one of them.

**Q:** We’ve got two-factor authentication - you can’t get in.

**A:** Love that for you. But if I send a flood of login attempts, will someone just approve one to make it stop? Or if I call pretending to be IT and ask for the code? 2FA is great - until your people help me bypass it.

**Q:** We’ve got strict controls - no one can install anything.

**A:** Until someone begs for “just this one tool” because they need it for a report. Controls are great - but so are exceptions. I only need one little “yes” and I’m in with a party hat.

**FAQs: Ask a Hacker**

*Round-up with your least favourite guest*

Look, nothing is ever 100% secure - and that’s fine. But here’s the thing: policies, tick-box training, and shiny tech tools like 2FA or encryption are only part of the picture. If people aren’t following them, or if you’re not regularly testing how well they work in real life, they’re just decoration. You’ve got to build a culture that thinks before clicking, double-checks dodgy emails, and doesn’t treat DSPT like a once-a-year paperwork job.

And **don’t** forget your suppliers - they’re part of your digital front door.

Think of me like a burglar walking down a street looking for my next target. If I see a window left open, an unlocked side gate, or a neighbour who’s clearly not watching - I’ll give it a try. But if everything looks well-maintained, doors locked, lights on, and maybe a barking dog in the background? I’ll just move on to someone easier.

Hackers, we’re lazy - don’t make it easy.