Phishing Attacks: How to spot and avoid them

A phishing scam happens when a cyber criminal pretends to be someone else to gain information. Commonly they do this by sending fake emails designed to look like they're from a trusted source. The aim is to make you click on malicious websites or attachments, so that you share sensitive data or download malware.

It is crucial that small businesses protect themselves by fully educating their staff about the threat of phishing.

Spotting phishing scams is not always easy, which is exactly how the scammers keep going, but here are some ways to avoid falling prey to phishing attacks:

Always double-check emails asking for money – or offering a prize!

If you receive an email asking for an invoice to be paid, always check this thoroughly before sending any money – even if you recognise the sender (phishing emails nowadays often look authentic). Similarly, don't be tempted by the promise of prizes. If you receive a message in your inbox telling you you've won a competition you don't remember entering, step away.

Be suspicious. Is it odd that the sender is contacting you?

If you have been contacted out of the blue, been offered a deal that seems too good to be true, or been given contact details that are very vague, it is possible that the email is a scam. If an email doesn't look quite right, it probably isn't. If you're not sure, check the sender address or just hover over the link before clicking on it to see where it leads to. If you don't recognise the address or it's full of odd looking symbols, avoid it like the plague!

Check for spelling mistakes and poor grammar

Scammers often use email addresses that are very similar to those of colleagues or clients, with just a subtle difference in the email address. As well as always checking the email address, look out for any uncharacteristic errors in spelling or grammar within the email itself. If there are lots of grammatical errors and language that sounds very old-fashioned, it's almost always going to be from a scammer.

Stay informed

Education is everything, and that goes for you and your staff members. New scams are being developed every day, so it pays to sign up to regular updates and guides that will keep you in the loop. Cyber Security training for all IT users is also highly recommended so you can be confident that everyone knows what to look out for.

Be aware of your social media presence

Scammers often 'stalk' their victims on social media so that they can gain data to deceive them with (e.g. name, job, friends, employment background, interests and contact details). Think about tweaking your online accounts so that any information that could be used against you is kept safe

Keep your technology up-to-date

Keep your web browser up to date. It might seem like a pain having to keep installing new patches on your internet browser, but updates are there for a reason. Providers release patches in response to phishing attacks and loopholes, so don't ignore messages to update.

Download the full guide

You can avoid phishing scams by making sure you – and your team – are prepared for an attack and know what to look out for.

We've written a guide to tell you everything you need to know. Download today and keep your business safe from phishing.

About Dragon IS

Dragon IS, based in Milton Keynes, is an IT support company and cyber essentials certified supplier. Established over a decade ago, we specialise in working with small and medium sized businesses.

For more advice, please contact:

Lionel Naidoo
CEO
Dragon Information Systems
lionel@dragon-is.com

0330 363 0055