FREEMAN CLARKE

Minimising the Phishing Threat

A CEO's Checklist

Every day we meet businesses who have lost thousands of pounds due to phishing emails. They rarely discuss this openly, and their losses are normally painful and disruptive rather than catastrophic. But it really is incredibly common.

Phishing attacks or "Business Email Compromise" scams are emails sent to users to trick them into giving up login details, transferring funds or running a malicious program. These emails are carefully crafted to look real and they sometimes appear to be from a legitimate source (the email may be to a member of your staff and may appear to come from you!).

30% opened

Phishing attacks are becoming increasingly sophisticated and prevalent. According to a respected 2015 report 30% of phishing messages were opened by targets, with 12% clicking on the attachment.

To address the threat requires actions which span different parts of your organisation: IT, finance and HR. Following is a CEO's checklist.

1. Plan how you would deal with this kind of problem? Agree who has authority to make decisions and manage the situation on the spot.
2. Establish that financial authorisation by email is not sufficient, no matter who it is from - a further check is always necessary (eg phone call to FD on a specific number).
3. Register similar domain names to yours. Often emails come from similar looking domains, in a hurry it's easy to mistake eg waddingtons.com vvading-tons.com
4. Ensure phishing is properly covered in the IT Security Policy (and make sure it's communicated and understood).
6. Check whether your insurance covers you for phishing - it may not.
5. Staff training should cover the following explicitly:
   - staff should check important instructions directly with the authoriser
   - staff should never go to a bank website or similar by clicking a link in an email
   - staff should be suspicious and check wording and style of incoming emails carefully.
7. Send test phishing emails to staff periodically to test their training.
8. Can the Board member accountable for IT answer 100% positive on the technical list below?

See our IT Director checklist over the page

FREEMAN CLARKE

A technical checklist for the Board member accountable for IT:

7 POINT technical checklist

1. Have your IT staff set DMARC, DKIM and SPF records in the company's email domain DNS records?
2. Are IT security systems in place? For example Microsoft's Advanced Threat Protection and Open DNS.
3. Are Anti-Virus systems up to date and managed centrally? (Is there evidence that the systems are up to date?)
4. Are there multi-scanning systems in place for Anti Spam/Malware, for example Symantec.cloud in front of Exchange Server/Office365?
5. Does the email system use good spam filtering systems, anti-virus systems and black/white lists and is a third party black list used?
6. Are all PCs protected with Anti-Virus, Anti-Malware and Anti-Spyware software and is it kept up to date? (Is there evidence it is up to date?)
7. Is the email system set up to sanitize email attachments, i.e. block executable attachments, links and other malware/virus payload files?

contact@freemanclarke.co.uk
0203 020 1864
www.freemanclarke.co.uk

FREEMAN CLARKE