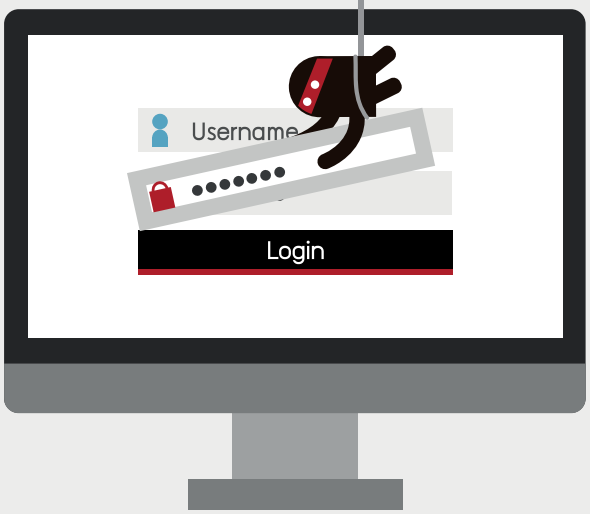
blackfoot Newsflash

Protect your business and reputation from phishing



For end customers, phishing means anything from an annoyingly cluttered inbox to the distress of identity theft or account takeover. However for your business, phishing translates into potential brand and reputational damage, particularly if it undermines your customers' trust and willingness to do business with you in the future. Phishing could also mean additional operational expense if in-bound customer service calls increase due to a phishing attack conducted in your name.

We explain a couple of methods to help prevent phishing e-mails purportedly coming from your business. These methods also help to improve the delivery of your e-mails generally. When you have implemented these methods, you have the chance to pro-actively reassure your customers.

About SPF and DKIM

The basic premise of phishing – sending e-mails purporting to be genuine to dupe unsuspecting recipients – exploits the anonymity of the internet. Or as the caption to the famous New Yorker cartoon read, 'on the internet, nobody knows you're a dog.' Consequently, nearly all abusive or phishing e-mails carry fake sender addresses, which may not be obvious to the end customer from the address displayed in the 'from' or 'sender' field of the e-mail. If the fake sender address is your own domain, customers might be more easily duped into believing the message is genuine.

The sender policy framework (SPF) is an open standard specifying a technical method to prevent sender address forgery. SPF allows you to specify which mail servers you use to send e-mail from your domain. The receiving mail server can check whether the message complies with what you have published as an SPF record in your domain name system (DNS) zone. If the e-mail comes from an unknown server, it can be considered a fake. For further information on how to create an SPF record, please see the appendix. DomainKeys Identified Mail (DKIM) allows you to identify yourself as the legitimate originator of your e-mails whilst they are in transit. DKIM attaches a new domain name identifier to each e-mail which validates that it is authentic via cryptography. The adoption of DKIM is growing and many mail systems will fully trust properly signed messages, providing increased deliverability. For further information on DKIM, please see the appendix.

Both SPF and DKIM make it easier for receiving servers to recognise and filter out fake sender addresses. These methods also help the delivery of genuine e-mails as more recipients tighten their restrictions to prevent spam.

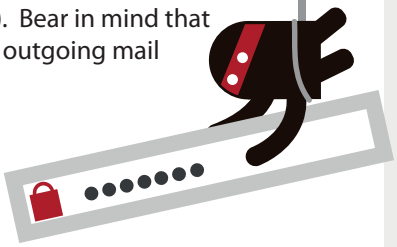
In summary

Phishing is an industry issue as old as the internet. Phishers continue because it works, otherwise they would have long since moved on to other scams. In this way, phishing is always likely to exist in some form. The effective implementation of SPF and DKIM described in this newsflash raises the bar against phishing, and helps protect your business from the brand, reputational and operational fallout.

For further information on SPF and DKIM, please visit www.openspf.org and www.dkim.org, or e-mail us at info@blackfootuk.com

How to implement SPF

The following are some considerations when creating an SPF record:



List all your outgoing mail servers – SPF advertises your domain's mail servers, so consider which are used to send mail (e.g. mail and web servers, servers at ISPs and other third party service providers). Bear in mind that only the final mail server is relevant, so if your organisation routes internal mail through an outgoing mail server for onward distribution, only list the outgoing mail server in SPF.

List all your domains – include all the domains you use, bearing in mind that domains you do not use could still be abused by fraudsters (see 'publish null records for domains that do not send mail' below).

Assess the impact of changes – Understanding who sends mail, from where, using which domains, and via which mail servers will allow you to determine the impact of changes. For example it may be necessary to review use of your own email from public places, or provide stronger authentication for such users.

Publish null SPF records for domains that do not send mail – to prevent fraudsters spoofing domains that do not send mail, specify those particular domains with a null record (e.g. 'v=spf1 –all').

Test your SPF records – use a testing tool to ensure that your new SPF records are valid before making changes to DNS.

Publish your SPF record in the correct DNS server – SPF is based on DNS lookups, so create SPF records on the correct DNS server. To find out which are the 'authoritative' DNS servers for your domain, perform a 'whois' lookup.

Allow for DNS caching during testing – if you are using a testing tool to look up your SPF record in DNS, ensure that change has propagated. It may be easier to paste the SPF record into the testing tool so any changes are seen immediately.

Monitor mail – examine mail server logs for rejected mail and review bounced mail.
For further information on SPF, please visit http://www.openspf.org

How to implement DKIM

Implementing DKIM is relatively straightforward, especially if SPF has already been implemented:

- **Identify all domain names and mail servers used for sending mail**
- **Generate/export public keys for each of these**
- **Request a DNS change from your domain name administrator to publish the DKIM information**
- **Enable the use of DKIM on the mail servers once the DNS change has propagated**
- **Test the use of DKIM**
- **Monitor and address delivery failures**
- **Protect the private keys**

For further information on DKIM, please visit http://www.dkim.org

How to validate the changes

The following tools may help you to validate the changes to your DNS records as a result of implementing SPF and DKIM:

http://www.appmaildev.com/en/dkim

http://www.kitterman.com/spf/validate.html

blackfoot

BLACKFOOT UK LIMITED
Tel: 0845 805 2409 E-mail: info@blackfootuk.com
Web: www.blackfootuk.com