E-Guide

The Rise of Spear Phishing Attacks & Email Fraud

ComputerWeekly.com

In this E-Guide:

Spear phishing attacks are sophisticated, targeted, costly and increasing in popularity among cyberattackers. In fact, almost half of UK firms have been hit by phishing attacks, a recent report shows. Download this e-guide to learn about the rise of phishing and email security, today.

Four in 10 leading banks failing on email fraud protection

Warwick Ashford, Security Editor

One-third of leading UK challenger banks have failed to implement a vital email protocol that protects consumers from email fraud, while 8% of traditional banking institutions have also neglected this fundamental defence system.

This is the finding of an analysis of the email security defences of the top 10 traditional and challenger banks by data-driven cyber security firm Red Sift, despite increased cyber attacks targeting financial institutions and increased competition in the sector.

The domain-based message authentication, reporting and conformance (Dmarc) protocol is the only sure-fire way to prevent email spoofing, which for too long has been blamed on the user being duped by social engineering, the security firm said.

Red Sift believes that implementing Dmarc is a strong indicator of an organisation's overall willingness to adopt adequate cyber security measures to protect its consumers.

While 67% of traditional banks have implemented Dmarc and configured it to reject all spoof email, the study found that 25% have implemented the government-endorsed tool but have not configured it for full protection.

And although two-thirds of challenger banks have implemented Dmarc, only 25% have configured it to reject all spoof email.

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

Randal Pinto, COO at Red Sift, said: "As challenger banks continue to disrupt the sector with digital banking service innovations, we wanted to assess the cyber security health of the whole sector to understand whether new entrants into the market were factoring in the likely threat impact as part of the product innovation process and if this was driving traditional providers to up their security game.

"However, the results are not encouraging. Only a quarter of challenger banks, and 67% of established banking institutions, have deployed the highest level of email fraud protection to prevent fake emails reaching customers' inboxes."

The traditional banking sector has struggled to keep pace with an ever-changing cyber threat landscape, said Pinto. "Reliance on ageing computer systems to maintain vast global banking empires is causing all manner of problems when it comes to ensuring organisation security," he said.

"We have recently seen UK retail banks, including Santander, Royal Bank of Scotland, Barclays and Tesco Bank, having to limit or shut down their systems due to attack. Analysis of these types of attack shows it is basic systems such as email that are being duped, accounting for significant losses, mainly via phishing.

Read more about Dmarc

- Lack of Dmarc email validation puts brands and customers at risk.
- US government making progress on Dmarc implementation.
- Dmarc email validation – we're doing it all wrong.

"We saw £354m of UK money lost to authorised push payment scams last year alone, so we are calling for both long-established and new challenger banks to implement basic email security defences in order to safeguard customer data, finances and loyalty."
In March 2019, another study revealed that email security in UK government organisations is lagging far behind that of central government, with less than one-third implementing Dmarc.

The study showed that only 28% of gov.uk domains have been proactive in implementing the Dmarc protocol. However, this finding is in sharp contrast to central government departments, where 89% have implemented Dmarc, according to the National Cyber Security Centre (NCSC).

Attackers sending fake emails purporting to be from the government has been one of the biggest problems in UK cyber security, according to the NCSC. But much of it is preventable by adopting the Dmarc protocol, which helps to authenticate an organisation's communications as genuine by blocking emails pretending to be from government.

Dmarc is also an effective tool for preventing domain impersonation attacks, which are the most common and most harmful kind of phishing attacks.

Government departments with Dmarc that are using Mail Check are blocking 35% more spoofed emails than those not using Mail Check, achieving a more secure Dmarc configuration, according to an NCSC blog post.

UK government organisations' email security lagging

Warwick Ashford, Security Editor

Only 28% of gov.uk domains have been proactive in implementing the Domain-based Message Authentication, Reporting and Conformance (Dmarc) protocol, a study has revealed.

This finding is in sharp contrast to central government departments, where the majority have implemented Dmarc, according to the National Cyber Security Centre (NCSC).

Dmarc is a key component of the NCSC's Active Cyber Defence (ACD) initiative, which aims to protect the UK from high-volume commodity attacks.

Once enabled, Dmarc provides an email validation system designed to detect and prevent email spoofing, ensuring that email senders and recipients can better determine whether or not a given message is from a legitimate sender. If an email is from an untrusted source, and Dmarc is fully enabled, administrators can decide whether the email should be placed in quarantine or rejected.

Attackers sending fake emails purporting to be from the government has been one of the biggest problems in UK cyber security, according to the NCSC. But much of it is preventable by adopting the Dmarc protocol because it helps authenticate an organisation's communications as genuine by blocking emails pretending to be from government.

Dmarc is also an effective tool for preventing domain impersonation attacks, which are the most common and most harmful kind of phishing attacks.

Lack of preparation leaves door open for phishing attacks

The UK Government Digital Service (GDS) issued guidance advising government organisations to implement the Dmarc email authentication and reporting protocol in preparation for the retirement of the Government Secure Intranet (GSI) platform in March 2019.

The GSI has enabled government organisations to communicate securely at low protective levels since 1996, but just weeks before its retirement less than a third of gov.uk domains have enabled Dmarc themselves ahead of the deadline, according to analysis of more than 2,000 email domains by data security company Egress.

This means that nearly three-quarters are not following the minimum standard requirements suggested by GDS to authenticate email messages.

Nearly three-quarters of government organisations are not following minimum standard requirements suggested by GDS to authenticate email messages

This highlights a lack of preparation by the majority of email administrators at government organisations in readying themselves for the domain migration, which, in effect, leaves domain users open to phishing attacks.

The number of public sector organisations that have not yet set up Dmarc to assure their email network's ability to withstand phishing attacks is "quite startling" according to Neil Larkins, chief technology officer at Egress.

"With only weeks left before the GSI framework is retired, it's critical that organisations heed the advice laid out by GDS," he said.

Further analysis by Egress revealed that of the 28% of government organisations that have set up Dmarc, 53% have the policy set to "do nothing". This means email buffering and business email compromise (BEC) cannot be prevented for these domains, and spam and phishing messages go straight into the recipient's inbox, regardless of whether the message has been sent from a trusted sender or not.

Any organisation using a default gov.uk Dmarc setting will also not be taking advantage of the "reject email" policy, said Egress. This means less than 14% of organisations are using Dmarc effectively if they want to stop phishing attacks, according to Egress.

Central government shores up email defences effectively

In central government, however, Dmarc has been implemented by the majority of departments, according to the NCSC.

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

"Our world-leading ACD programme was launched two years ago, but 89% of central government departments have already implemented Dmarc and 95% are using the NCSC's Mail Check service," an NCSC spokesperson told Computer Weekly.

The NCSC's approach has been to focus on the primary domains of central government departments which are the most valuable to phishers, the spokesperson said, adding that gov.uk domains using Mail Check were much more likely to reach a Dmarc policy of "reject" or "quarantine" (blocking) to protect recipients from spoofed email from domains.

"We believe our unique bold and interventionalist approach is making the UK an unattractive target to criminals or nation states"

NCSC spokesperson

The Mail Check service, which is also part of the ACD programme, works by assessing an email server's configuration and providing guidance on the implementation of various email security protocols, most notably Dmarc.

Government departments with Dmarc that are using Mail Check are blocking 35% more spoofed emails than those not using Mail Check to achieve a more secure Dmarc configuration, according to an NCSC blog post.

"The ACD programme intends to increase our cyber adversaries' risk and reduces their return on investment, and it is for organisations to understand their own risk and act accordingly," said the NCSC spokesperson.

“We are proud that Dmarc is available to organisations and believe our unique bold and interventionalist approach is making the UK an unattractive target to criminals or nation states.”

Read more about Dmarc

- Lack of Dmarc email validation puts brands and customers at risk.
- US government making progress on Dmarc implementation.
- Dmarc email validation – we’re doing it all wrong.

Four in 10 leading banks failing on email fraud protection

UK government organisations’ email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

Nine email security features to help prevent phishing attacks

Kevin Tolly, Founder

As long as email exists, phishing attacks will too. In the world of IT, that probably means forever. So to keep pace with hackers, IT security professionals and email security vendors need to constantly reassess their email system features to help prevent phishing attacks.

Whether you're looking for a new email security system or making a wish list of features to hand your current vendor for phishing protection, here's a checklist of key product features to consider.

The following list was created using The Tolly Group's background in email security, along with input from email security vendors. While not comprehensive, this email security checklist should help ensure you have your anti-phishing bases covered.

1. Review the existing configuration

While IT professionals have a tendency to look beyond their existing environments for new features and functions or to new vendors to help solve technology problems, they often don't have to look that far. The quickest path to potential improvement is to first review your existing email security system configuration. If you're still running on defaults, your system definitely isn't optimized.

2. Harden logins to protect credentials

The goal of phishing is most often to retrieve and compromise users' credentials. If you can't stop 100% of phishing attacks, you can at least reduce their effectiveness by hardening the login process.

Many applications offer two-factor authentication, where a text is sent to a person's registered mobile number, for example, to help assure the right user is logging in. Similarly, many systems provide reports of anomalous logins or login attempts. While this might be outside your purview as an email security professional, encouraging credential protection can be a secondary but effective method to guard against phishing attacks.

3. Verify threat intelligence networks

First and foremost, your email security needs to be smart and know about threats as soon as they arise. Threat intelligence services -- also called platforms or networks -- provide this information, so be sure to check your vendor's offerings to see if it has its own threat intelligence network. If so, make sure you know how extensive it is.

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

Also, ask your vendor if it leverages other resources, such as FireEye, Lastline or others.

The quickest path to potential improvement is to first review your existing email security system configuration.

4. Mailbox intelligence

While mailbox intelligence is a fairly straightforward feature, it can save you from a lot of trouble.

If you're like me, you get a lot of emails. Your email security system may apply some intelligence to the message flow and determine who your normal correspondents are -- either by name or by company. The first email from anyone is more likely to carry a phishing attack and probably deserves closer inspection by the email security system than a message from a known person.

5. Deep link inspection

While some phishing attacks are evident just from the look of an email, the more insidious ones may not become evident until the link is probed. Be sure your email security system will follow links and inspect not just the source email but the target link in the message.

Every link in an email is potentially a phishing site, and with deep link inspection, the email system opens the link in its own sandbox to make sure it isn't malicious. Then, malicious links are removed or blocked.

6. Multilayer email security

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

As with any security system, more layers usually provide more protection. Look for products that can provide multiple layers of security. Look for email security products that check links at least twice -- first when they enter the email system and again if or when they are clicked by a user. It is certainly possible for an email to contain a harmless link when it enters the system, but it can be turned into a phishing site a few minutes or hours later.

The opposite is also true. Links can be malicious when they enter an email system, but they could be identified and resolved by the time a user clicks through a few hours later. A system that doesn't check a second time would be likely to label the now-clean site malicious, which produces a false positive. False positives slow down users who may need to contact a security admin so the message can be manually cleared or whitelisted.

7. Web and document isolation

What if your email security system can't determine whether a given site or document is legitimate or phish bait? There will always be that no-man's land where a document is potentially good or potentially malicious.

Symantec, for example, practices isolation, a capability it attained from its acquisition of Fireglass in 2017. The isolated site is presented in read-only mode. As a result, it's easier to see what the site is without entering any data. Another option is for the security manager to configure the feature to allow users to override isolation and proceed.

Similarly, you can isolate an attachment. For example, if a user opens a Microsoft Word or Excel attachment, it can actually open in an isolated container rather than on the user's system. If the email happens to contain a malicious macro, that macro can't infect or attack the end user's computer.

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

8. Platform-specific

Many of the files and links related to email can reside on a cloud service like Google Drive, Dropbox or Microsoft OneDrive. While these applications often integrate into the user's computer interface, they may have special requirements for file scanning or threat isolation.

Some of these cloud products might require special application code for the email security system to query and analyze those files. It's always a good idea to note any platform-specific requirements and match them up to what the vendor is offering.

9. Reporting and analytics

You will certainly want to know how effective your email security system is at isolating and neutralizing phishing attacks. For this, you will need a comprehensive set of reporting and analytics tools. Make sure your system can provide a real-time dashboard, as well as historical reporting capabilities and data export functions in the event you want to generate a custom analysis of your threat response information.

Then what?

Is there more that you can do? There's always more, but starting with this checklist should improve your email security protection and your awareness of where the industry is moving.

Firms urged to protect against spear phishing

Warwick Ashford, Security Editor

Brand impersonation is being used in 83% of spear phishing attacks, making it the most popular form of this type of targeted attack, research shows.

These attacks are designed to impersonate well-known companies and commonly-used business applications and are well designed as an entry point to harvest credentials, carry out account takeovers and steal personally-identifiable information (PII), according to a report by security researchers at Barracuda Networks.

Using carefully-designed templates that impersonate top brands, scammers send an email claiming that the targeted individual's account has been frozen and providing a link to reset the account password. The link typically takes victims to a legitimate-looking phishing website designed to harvest login credentials.

Microsoft and Apple are the most-impersonated brands in spear phishing attacks, the researchers said, based on an analysis of 360,000 spear phishing emails in a three-month period.

Spear phishing attacks are designed to evade traditional email security, including gateways and spam filters. They are typically sent from high-reputation domains or already-compromised email accounts and do not usually include malicious links or attachments,

enabling them to bypass most traditional email-security techniques rely on blacklists and reputation analysis, the report said.

The attacks also typically use spoofing techniques and include zero-day links hosted on domains that have not been used in previous attacks or that have been inserted into hijacked legitimate websites. As a result, they are unlikely to be blocked by link-protection technologies.

The attackers also take advantage of social engineering tactics in their attacks, including urgency, brevity and pressure, to increase the likelihood of success, the report said.

Read more about spear phishing

- In November 2018, dozens of US Democratic National Committee (DNC) email addresses were targeted in a spear phishing campaign.
- A cyber espionage group dubbed Whitefly has been identified as the perpetrators behind Singapore's largest data breach to date that used malware distributed through spear phishing emails.
- Email is the number one entry point for data breaches, which includes targeted email attacks such as business email compromise and spear phishing.

The second most popular form of spear phishing attacks, accounting for 11% of attacks monitored, are blackmail scams, which include sextortion attacks.
In these attacks, scammers typically claim to have a compromising video, images or other content allegedly recorded on the victim's computer. They threaten to share this content with the targeted individual's email contacts, unless they pay up.

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

With about 1 in 10 emails being a sextortion attack, employees are twice as likely to be the target of blackmail than business email compromise (BEC), which accounted for just 6% of attacks monitored.

Although BEC attacks – also known as CEO fraud, whaling and wire-transfer fraud – make up only a small proportion of spear phishing attacks, they have resulted in more than $12.5bn in losses since 2013, according to the FBI.

In BEC attacks, scammers usually impersonate an executive, partner or another trusted person in an email by compromising their email account, requesting a wire transfer or personally-identifiable information from finance department employees or others with access to sensitive information.

Business email compromise attacks

According to the Barracuda research, Gmail accounts are used to launch 30% of business email compromise attacks.

The study shows that spear phishing attacks are timed to exploit security weaknesses and other potential vulnerabilities around holidays and other events, such as tax season. The week before Christmas, the number of spear phishing attacks spiked to more than 150% above average, the study shows.

"Hackers know the end of the year is a flooded with a lot of activity, including email communications, and try to take advantage by launching attacks at distracted and busy employees. IT and security staff resources are typically stretched at the holidays, as many people take vacation time, and they may not be as vigilant or have as much time to monitor potential phishing attacks," the report said.

Preventing spear phishing attacks, the report said, requires the right combination of technology and user security training.

In the light of the fact that scammers are adapting email tactics to bypass gateways and spam filters, the report recommends that organisations consider purpose-built technology that does not rely on looking for malicious links or attachments, but uses machine learning to analyse normal communication patterns and spot anomalies.

The report also recommends deploying technology that uses artificial intelligence to recognise when accounts have been compromised and that remediates in real time by alerting users and removing malicious emails sent from compromised accounts.

In light of the fact that domain spoofing is one of the most common techniques used in impersonation attacks, the report recommends using the Domain-based Message Authentication, Reporting and Conformance (Dmarc) email authentication and reporting protocol. Dmarc authentication and enforcement can help stop domain spoofing and brand hijacking, while Dmarc reporting and analysis helps organisations accurately set enforcement, the report said.

Other recommendations include using:

- Multifactor authentication (MFA) to provide an additional layer of security.
- Training to help employees recognise and report attacks.
- Regular proactive searches to detect emails with content known to be popular with hackers.
- The right combination of technologies and business policies to ensure emails with confidential, personally-identifiable and other sensitive information are blocked and never leave the company.

Almost half UK firms hit by phishing attacks

Warwick Ashford, Security Editor

Phishing attacks aimed at stealing legitimate user credentials have been used in the past 24 months to compromise 45% of UK organisations, according to research on behalf of cyber security firm Sophos.

Just over half (54%) of more than 900 IT directors polled in Western Europe said they had identified instances of employees replying to unsolicited emails or clicking on links contained within them, revealed a poll conducted by Sapio Research.

The study revealed that larger businesses are most likely to have been compromised by phishing attacks, despite also being most likely to conduct phishing and cyber threat awareness training.

Although organisations in the UK fell victim to phishing attacks at a similar rate to those in France (49%) and the Netherlands (44%), those in Ireland performed significantly better. Just 25% of Irish respondents said they had fallen victim to phishing in the past two years.

Across all respondents, 56% of companies employing between 500 and 750 people were identified as phishing victims in the past two years, while two-thirds (65%) had identified instances of employees replying to unsolicited emails or clicking on links contained within them.

By comparison, just 25% firms with fewer than 250 people and 36% of organisations with between 250 and 499 employees had been compromised by phishing in the same period.

Half of firms with fewer than 250 people offered training to help employees spot attacks, compared with 78% of those with between 500 and 1,000 people. And 79% of UK companies conduct regular cyber threat awareness training already, while 18% said they plan to offer it in the future.

Adam Bradley, UK managing director at Sophos, said criminals are adept at using social engineering to exploit human weakness, so while well-trained employees are an excellent deterrent, even the best user can slip up.

“Organisations need to ensure employees remain vigilant to the threat posed by phishing attacks and ongoing training should be part of that to spot check employees and ensure they respond correctly and continue to follow the guidelines they’ve been given.”

According to Bradley, phishing is one of the most common routes of entry for cyber criminals. “As organisations grow, their risk of becoming a victim also increases as they become more lucrative targets and provide hackers with more potential points of failure.

“Given the frequency of these attacks, organisations that don’t have basic infrastructure in place to spot people engaging with potentially harmful emails and whether their systems are compromised are likely to encounter some really significant problems,” he said.

Organisations should block malicious links, attachments and imposters before they reach users’ inboxes, said Bradley, and use the latest cyber security tools to stop ransomware and other advanced threats from running on devices even if a user clicks a malicious link or opens an infected attachment.

Four in 10 leading banks failing on email fraud protection

UK government organisations’ email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

Four in 10 leading banks failing on email fraud protection

UK government organisations' email security lagging

Nine email security features to help prevent phishing attacks

Firms urged to protect against spear phishing

Almost half UK firms hit by phishing attacks

Read more about phishing

- Phishing attacks hidden by custom fonts.
- Phishing at centre of cyber attack on Ukraine infrastructure.
- How to create an internal phishing campaign from scratch.
- Phishing remains top fraud enabler, RSA reports.