Inside Track Research Note

In association with

So long, and thanks for all the phish

How to avoid that hook at the end of a fraudster's line

Freeform Dynamics, 2017

About this Inside Track

The research upon which this Inside Track is based was independently designed and analysed by Freeform Dynamics Ltd. Data was gathered via an online survey executed in collaboration with a mainstream IT news site. 330 responses were gathered from IT professionals across a range of industry sectors, geographies and organisation sizes. The study was sponsored by Sophos.

Introduction

Phishing is the attempt to obtain personal, private, or commercial assets – usually information or funds – by impersonating a trustworthy source. Fraudsters commonly use email phishing scams to trick their prey, but messaging apps, social media, fake websites and phone calls can also be part of the picture.

Mass-mailing phishing attacks appear to be subsiding, but this shouldn't lull business and IT managers into a false sense of security, as attackers are now focusing their efforts on spear-phishing campaigns. Using cleverly crafted messages and a range of exploits to bypass traditional email security measures, it's estimated that perpetrators have already tricked unsuspecting businesses out of $5 billion[1].

This *Temperature Check* of 330 IT professionals reveals that attackers are regularly impersonating senior managers and targeting specific business departments. So, what's to be done? Let's start by sizing-up the problem and looking at how organisations are responding to this threat.

Impersonators, imposters, and thieves sneak past email security checkpoints

If you have customers, partners, investors or suppliers, you still need to use email.

Love it or loath it, there's no escaping email in today's digitally connected world. Your organisation may be using enterprise social networks and chat-based platforms to reduce internal email (and some companies are even starting to shift their customer communications to apps and chatbots), but none of these mediums has the same reach and range as email. In short, if you have customers, partners, investors or suppliers, you still need to use email.

Email protocols, standards, and architectures have evolved over several decades to address privacy, security, and authenticity issues. An ecosystem of ancillary products and services has also developed during this time to answer specific problems, challenges, and business requirements.

If you work in IT, and run email servers on-premise, you'll be aware of the many products and services that wrap around the corporate email system to provide in-bound and out-bound email hygiene and security. And if you've outsourced your corporate email, as many organisations have, then your service provider is likely to use an even greater mix of products and technologies to secure, protect, and maintain your inbox. We'll provide an insight into how widely these technologies are used a little later in this Inside Track, but we need to assess the threat that phishing poses to your business.

40 percent of survey respondents report at least daily phishing attacks.

The survey data (Figure 1) indicates the scale of the phishing problem, with around 40 percent of respondents reporting at least daily phishing attacks. Although there's a gradient that starts to ramp-up with company size, firms of all sizes can be targeted, and there's only slight variation across industries. The survey results also show that well-protected and well-prepared organisations also receive phishing reports from end users, so every business and institution is a potential target.

Copyright 2017, Freeform Dynamics Ltd

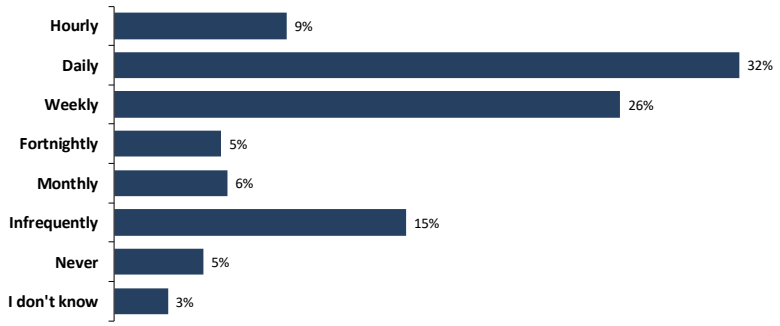


Figure 1

How frequently do you receive phishing reports from end-users?

Every phishing attack reported by an end user is evidence of at least two things. First, it proves that a well-crafted phishing attack can sneak past almost any security checkpoint or email filter. Secondly, it shows that some users are savvy enough to spot an attack and know how and where to report it.

Spear-phishing attacks targeting specific businesses and individuals are on the increase.

What this chart doesn't show us, however, is the number of attacks that go unnoticed/unread or hit their target. While scattergun phishing attacks are declining according to security industry reports, spear-phishing attacks targeting specific businesses and individuals are on the increase. So, who's being targeted and why?

Fraudsters target those who handle the money and administer company controls

Organised crime groups have targeted large and small companies and organisations in every U.S. state and more than 100 countries around the world.

The FBI started tracking business email compromise (BEC) attacks in 2013. In its 2016 Internet Crime Report (published June 2017), it stated that organised crime groups had targeted large and small companies and organisations in every U.S. state and more than 100 countries around the world, with losses now in the billions of dollars. In the UK, the 2016 Cyber Security Breaches Survey found that 32% of breaches/attacks involved impersonation of the organisation.

BEC can take a variety of forms, with fraudsters often targeting employees that have access to company finances, tricking them into making financial transfers to bank accounts controlled by the criminals. But spear-phishing attacks don't only target those who have access to the money, they also target those who manage business processes and IT controls (Figure 2). This opens organisations up to a range of vulnerabilities, including ransomware attacks and good old-fashioned extortion.

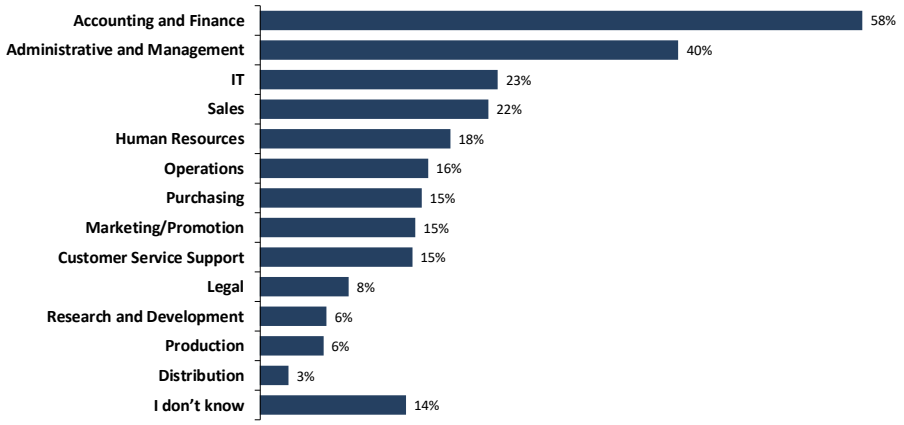


Figure 2

Which departments, are mostly targeted by phishing attacks in your organisation?

Lawyers, linguists, hackers, and social engineers are often used to craft a spear phishing attack.

Let's be clear, BEC perpetrators aren't amateur mischief makers, they're sophisticated groups with access to significant resources. The FBI reports that lawyers, linguists, hackers, and social engineers are often used to craft a spear-phishing attack, so it's easy to see how someone might fall victim to this form of deception.

But how do they do it exactly, and what can your organisation do to guard itself against this kind of concerted attack?

Is that email really from your Managing Director or a Master of Disguise?

With their eyes on the big prize, perpetrators are willing to go to considerable lengths, so they will study your organisation's processes and systems.

Scammers and fraudsters know there are plenty of "phish" in the sea, and these are now being used to help land "the big one". A so-called "whaling" attack will target your organisation by impersonating a senior manager or executive. With their eyes on the big prize, perpetrators are willing to go to considerable lengths, so they will study your organisation's processes and systems, collect email samples, and even monitor company events for an upcoming business trip that might present an opportunity to perpetrate their crime.

Here's how a spear-phishing attack might play-out: When the time is right, a maliciously crafted email will be sent to the victim by the fraudster. They'll spoof a familiar trustworthy account, such as an executive, senior manager, or supplier. The recipient, such as a finance officer or accounts clerk, will be directed to carry out some familiar financial transaction, only this time it will be a fraudulent request or instruction.

Over half of the respondents in our survey confirm that senior managers in their organisations have been impersonated in spear-phishing attacks (Figure 3). A targeted employee will usually believe that they are sending money (or commercially sensitive information) to a familiar account, but the details used will of course deposit the funds (or the information) in the scammer's account.

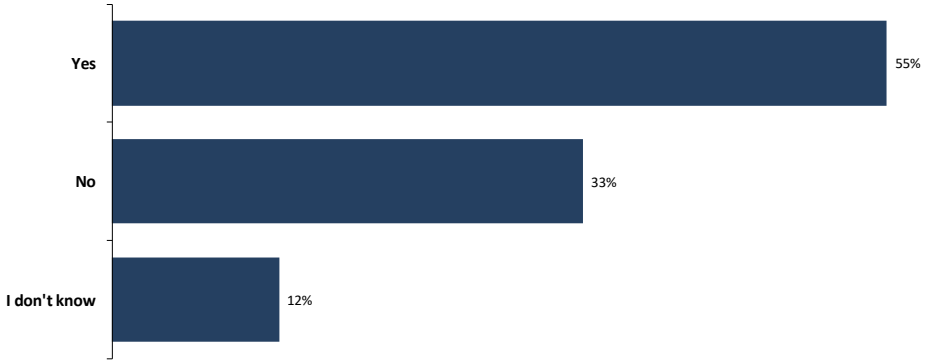


Figure 3

Have senior managers in your organisation been impersonated in phishing attacks directed at your business?

Professional fraudsters know what they're doing, and use money laundering techniques to transfer funds and cover their tracks.

Professional fraudsters know what they're doing, and use money laundering techniques to transfer funds and cover their tracks. It will usually be too late to recover the money if the transaction goes through or isn't discovered in time via other means. If it's commercially sensitive information that's been sent, this too will be in the hands of the perpetrator. This might be used for immediate commercial gain or some future purpose, such as tricking another individual within the organisation or supply chain.

Copyright 2017, Freeform Dynamics Ltd

With phishers and whalers becoming more adept, what can your organisation do to protect itself?

All of this might sound like a plotline for a Hollywood heist movie, but it's fast becoming a very common, and not-at-all glamorous, business story.

With phishers and whalers becoming more adept, what can your organisation do to protect itself?

Forewarned is forearmed: prior knowledge of possible phishing threats is key to survival

Defending against phishing and spear-phishing attacks requires a multi-level approach, and as with all things IT, technology on its own isn't enough. Polices and processes are just as important, with regular testing and refinement to ensure good business fit.

Even the most diligent of employees is fallible, so it makes good business sense to implement anti-phishing solutions.

Even the most diligent of employees is fallible, so it makes good business sense to implement anti-phishing solutions alongside other security products to help protect corporate email systems. End-point protection solutions add a layer of protection at the email client, especially on desktop and laptop PCs.

Over 60 percent of the respondents to our survey said they have already implemented anti-phishing protections or are "well advanced" when it comes to dealing with email-based phishing attacks, but this still leaves a sizeable proportion exposed (Figure 4). And given the survey audience has an interest in security and data protection topics, these figures are likely to be somewhat optimistic for organisations in general.

Figure 4

How prepared is your organisation when it comes to dealing with email-based phishing attacks?

Having IT security products, policies, and process in place is only part of the solution. There's no escaping the fact that we humans are the weakest link when it comes to security, so decision makers need to consider the business value of staff training, especially for those employees working in accounting and finance departments, administration and management, and of course IT (remember what we saw in Figure 2). A one-off training course is little more than a box-ticking exercise, so security officers and department managers will want to consider how employees can be kept on their toes, with simulation testing being one obvious option.

There's no escaping the fact that we humans are the weakest link when it comes to security.

Copyright 2017, Freeform Dynamics Ltd

What happens when things do go wrong and your organisation falls foul of the fraudsters?

If you've done all the above, well done. But it doesn't end there. We've already agreed that humans are fallible and that no security system can ever be perfect, so what happens when things do go wrong and your organisation falls foul of the fraudsters?

Protecting your business with a cybersecurity playbook

Being digitally connected brings significant business benefits and opportunities, but it also brings risks. There are hundreds of thousands of cyber-attacks on businesses like yours every day, attempting to steal your company's information and its money, or disrupting operations. Your organisation might be well prepared, but even the best defended company can never be totally safe. So, what happens when the inevitable happens and a spear-phishing or whaling attack hits its mark? Do you have a response plan?

Less than a quarter of those we surveyed said they had a specific playbook for dealing with sophisticated targeted email threats.

Less than a quarter of those we surveyed said they had a specific playbook for dealing with sophisticated targeted email threats and exploits (see Figure 5). And while 38% said they're "getting there", the remainder only have a very general approach at best for dealing with this kind of incident.

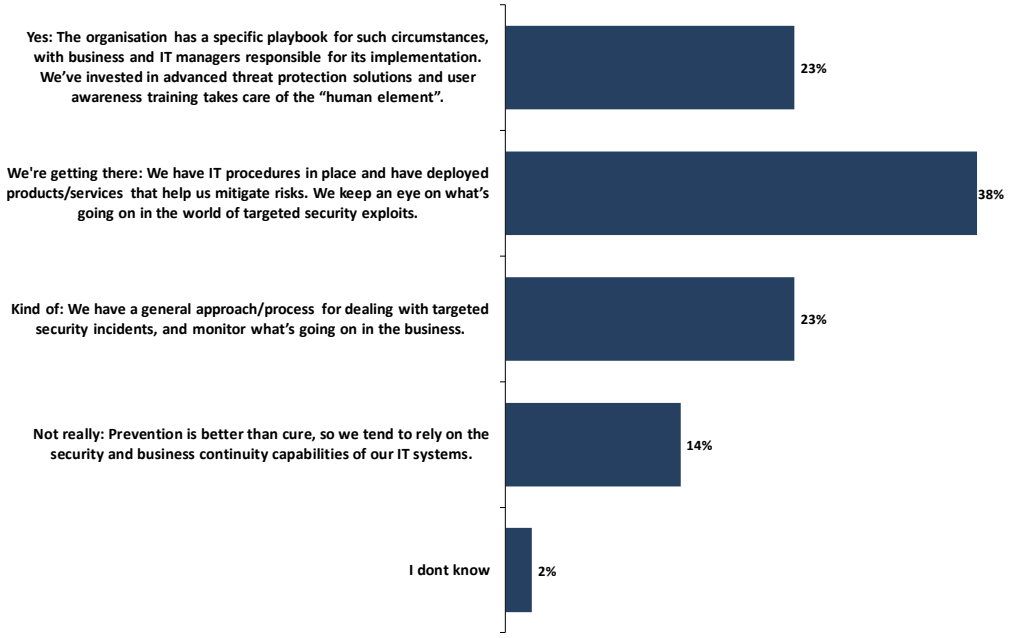


Figure 5

Does your organisation have a response plan or policy for dealing with sophisticated, targeted/sustained email threats and exploits?

If you don't yet have a response plan, it might be a good idea to get executive backing to design, develop, and test one as part of their fiduciary responsibility. There are plenty of sources of good practice, as well as specialist consultants who can advise if your budgets can be made to stretch. Think too about who you could turn to for support if your organisation becomes a victim of a financial phishing attack. Your audit firm or banking provider might be able to help here. If you suffer an IT service attack or disruption, think about what your recovery procedures will be and how you could keep your core business operations running.

Think about who you could turn to for support if your organisation becomes a victim of a financial phishing attack.

Let's now look at what organisations can do to mitigate the risks associated with phishing attacks.

Copyright 2017, Freeform Dynamics Ltd

What can organisations do to reduce the severity or seriousness of a phishing attack?

The adoption rate of anti-virus and anti-spam solutions is nearly 100%, but protection measures drop off significantly thereafter.

The adoption rate of anti-virus and anti-spam solutions is nearly 100%, but protection measures drop off significantly thereafter, with much smaller numbers saying they had anti-phishing measures, spoofing detection, URL protection, and data loss prevention (DLP) in place (Figure 6).

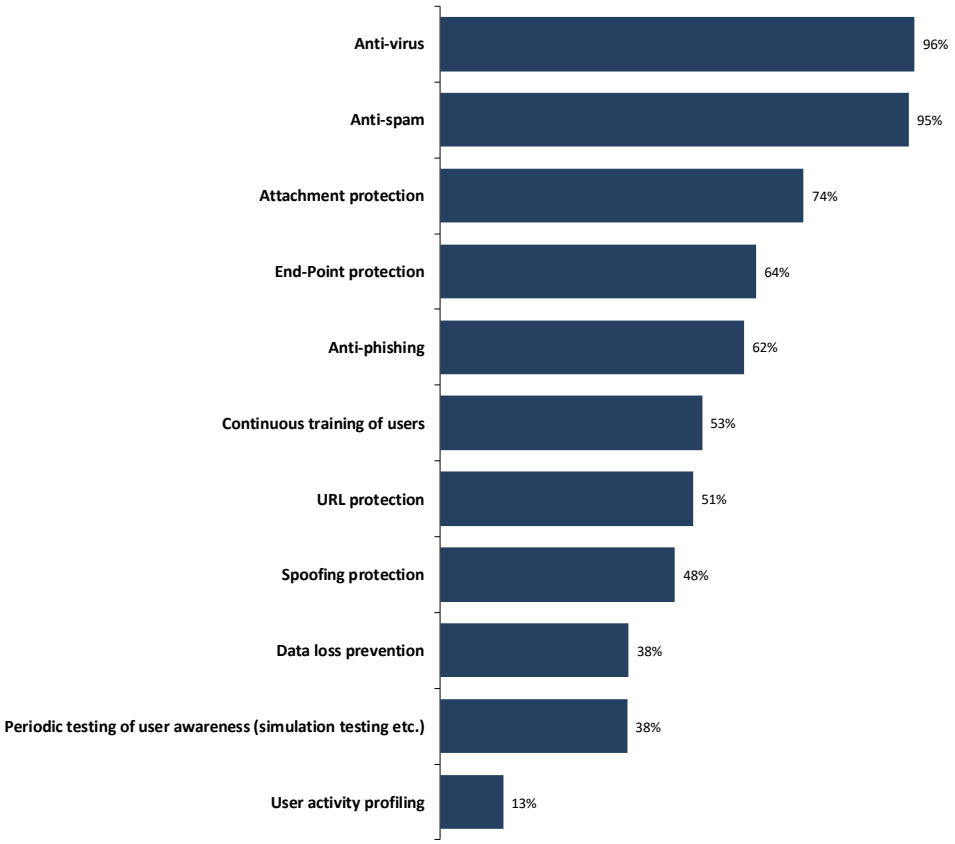


Figure 6

Which of the following measures do you have in place to mitigate against phishing attacks and other email security exploits?

We can assume that our survey group of IT professionals has good insight into security and risk mitigation measures, so it's somewhat disconcerting that anti-phishing, URL protection, and spoofing protection aren't more widely used. Some organisations may think they're better protected than they are (especially in the SMB space where email is generally outsourced), but budgets – or lack thereof – are also likely to be an issue.

Microsoft Office 365 and Google's G Suite have been the target of phishing scams.

Popular cloud-based communication and collaboration platforms, such as Microsoft Office 365 and Google's G Suite, can help organisations shoulder the burden of corporate email, but they've both been the focus of targeted phishing scams. Third-party anti-phishing solutions are available from vendors, but this still leaves the most vulnerable element – the end user – left to their own devices (quite literally in many cases). If you were to receive an out-of-hours email on your device from your boss marked "URGENT", albeit to your personal email account, would you open it?

Copyright 2017, Freeform Dynamics Ltd

Effective security measures are layered, multifaceted, and adaptive

Training staff to spot phishing attacks, and testing them periodically, is likely to have a positive effect on business security.

Training staff to spot phishing attacks, and testing them periodically, is likely to have a positive effect on business security, but it will never make for a totally safe working environment. Likewise, it's impossible to mitigate every risk using technology, no matter how much money and expertise is thrown at it. A combined approach is required: one that is layered, multifaceted, and adaptive.

We're just starting to see machine learning and artificial intelligence being employed to counter phishing attacks, but it will take a while for these technologies to enter the mainstream. In the meantime, organisations can reduce risk and enhance security by following best practice:

Good security habits take time to establish, so simulation and periodic testing should be part of your regime.

- Commit to educating, training, and testing employees. Good security habits take time to establish, so simulation and periodic testing should be part of your regime. IT security firms, industry bodies, and government agencies can offer tips and best practice.
- Advise employees to be wary of emails appearing to originate from C-suite executives, especially if the message compels urgency and requests immediate payment, funds transfer, or the sending of commercially sensitive information. Make sure payment policies and procedures are followed.
- Consider the use of digital signatures for executives using email, and the use of two-factor authentication protocols and procedures (such as a phone call or text message) when immediacy is required. Staff need to know that when something smells a bit "phishy", they should pick up the phone and speak directly with the person requesting the transaction or information.

When something smells a bit "phishy", pick up the phone and speak directly with the person requesting the transaction or information.

- Evaluate modern email protection services, such as anti-phishing, URL protection/detonation, spoofing protection, and user activity profiles for unusual or out-of-policy activities.
- Produce a playbook that details what to do when a spear-phishing attack penetrates your organisation, and if you suspect that you've been targeted by a phishing email, report the incident immediately to the relevant authorities.

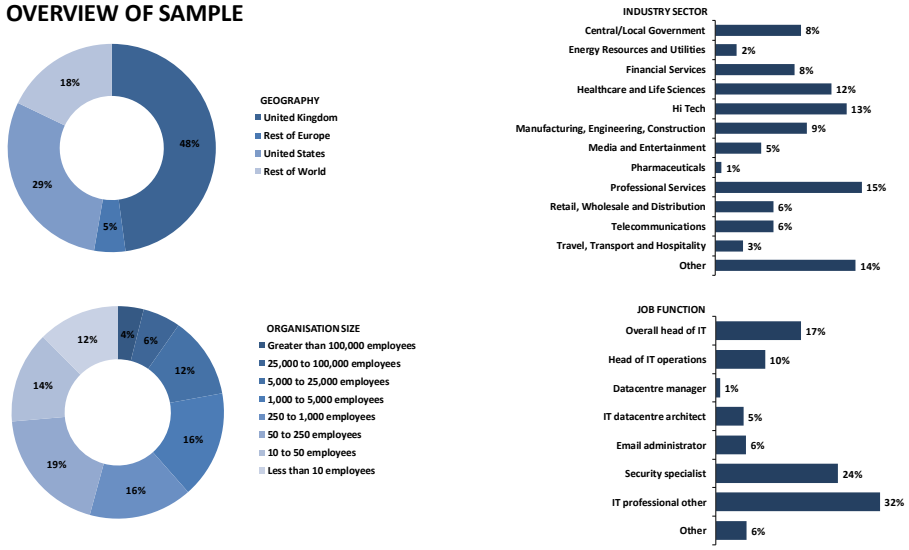
Copyright 2017, Freeform Dynamics Ltd

About the Research

The research upon which this Inside Track is based was designed and executed by Freeform Dynamics in collaboration with a mainstream IT news site. Data was collected from 330 IT professionals via an online survey completed in August 2017.

Figure 7

Online survey conducted in collaboration with a mainstream news and analysis website



Please note that the online methodology used in this study is subject to self-selection bias, so data may be skewed towards those with a greater interest in information security and data protection.

External links

1. FBI Public Service Announcement: THE 5 BILLION DOLLAR SCAM
   www.ic3.gov/media/2017/170504.aspx

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better-informed investment decisions.

For more information, and access to our library of free research, please visit www.freeformdynamics.com.

About Sophos

Sophos provides enterprise-grade security solutions that are simple to deploy, manage and use. The company offers security solutions covering endpoint, mobile, server, encryption, web, email, Wi-Fi, and UTM/next-generation firewall, all backed by SophosLabs -- a global threat analysis centre which provides real-time cloud-enabled security intelligence. Sophos is headquartered in Oxford, UK.

Learn more at www.sophos.com.

Terms of Use

This document is Copyright 2017 Freeform Dynamics Ltd. It may be freely duplicated and distributed in its entirety on an individual one to one basis, either electronically or in hard copy form. It may not, however, be disassembled or modified in any way as part of the duplication process. Hosting of the entire report for download and/or mass distribution by any means is prohibited unless express permission is obtained from Freeform Dynamics Ltd or Sophos. The contents contained herein are provided for your general information and use only. Neither Freeform Dynamics Ltd nor any third party provide any warranty or guarantee as to the suitability of this document for any particular purpose.