PHISHING RESPONSE TRENDS UK

Stop the Chaos

COFENSE

OVERVIEW

Organisations today take strong measures to guard against phishing attacks. With the number of phishing attacks at 1,220,523, a 65% increase over the previous year,[1] it's no wonder we find ourselves in an arms race against phishing attackers.

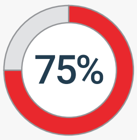
UK Data Breaches: Only Getting Worse

According to the Ponemon Institute, data breaches are costing UK organisations an average of £2.48 million.[2] They're also affecting customers by the thousands.

For example, Cex, the second-hand games, DVDs and hardware retailer, had personal information stolen from approximately two million customers.[3] And 727,000 UK children had their information compromised after a cyberattack on VTech, manufacturer of electronic learning toys.[4]

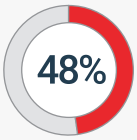
So, are we winning the war or just holding ground?

The findings of this report suggest the latter. The following data on phishing and responses show that businesses are flooded with suspicious emails targeting employees but are ill-prepared to process and respond to those threats. In fact, most organisations feel they have little, if any, expertise in anti-phishing and many feel their incident response processes are weak. Notable findings include:



Over 75% of surveyed IT executives have dealt with a security incident originating with a deceptive email.

Nearly 1/2 say their biggest challenge is multiple security solutions that haven't been integrated.



48% say their phishing response ranges from "not ineffective" to only "somewhat effective."

The #1 security worry is email-related threats.

In other words, despite all their investments in technology, three out of four UK organisations surveyed have experienced a phishing-related incident and almost all still worry about email-related threats. With little more than half of the organisations believing they have sufficient controls in place, it's obvious there's much work to be done in implementing solutions. And that work includes automation to analyse phishing emails and to help incident responders distinguish noise from real threats.

Read on to learn about the implications of our phishing response data and what organisations can do to improve their anti-phishing security.

SURVEY METHODOLOGY: Phishing Response Data

Senior Decision-Makers

In August 2017, Censuswide surveyed select UK IT professionals on phishing response strategies. One hundred professionals participated, largely senior decision-makers.

Numerous Industries

The surveyed companies represented firms in a wide variety of industries: business services, high tech, manufacturing, healthcare, financial, retail trade, wholesale trade, transportation, consumer services, telecom and general. One hundred percent of respondents participated voluntarily; none were engaged using telemarketing.

Nearly 1/4 of respondents see more than 500 suspicious emails weekly.

Among all those suspicious emails companies receive each week, something is often missed by filtering technologies. The result? Potentially, a costly security breach.

With the average office worker receiving 122 emails each day,[5] it's no wonder phishing is the top attack vector in data breaches.[6] Now imagine being a small team of incident responders receiving every forwarded employee email, some truly suspicious, some just spam. Given limited staff and time, how do you sort through hundreds to thousands of emails to find the real threats? ***The answer:*** better solutions that (a) leverage broader teams to identify phishing and (b) automate and orchestrate response. By reducing noise in the reporting inbox (if they have one), companies can free responders to focus on real threats.

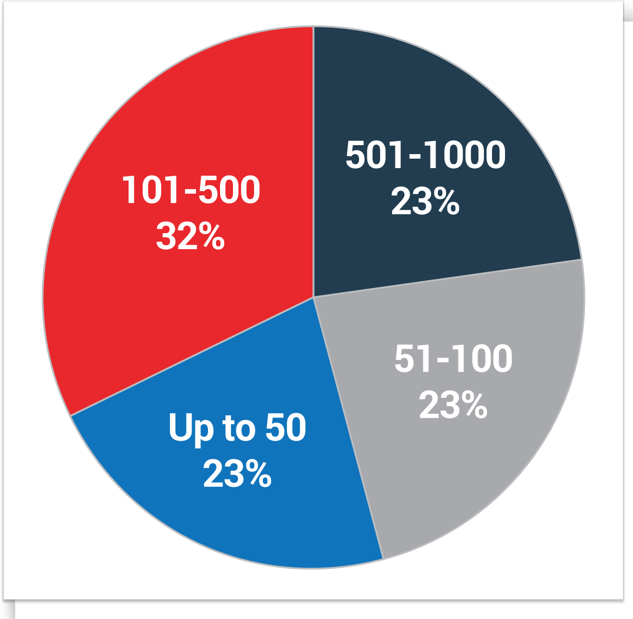


Figure 1: How many suspicious emails are reported in your organisation each week?

Manual reporting and analysis delay detection and response.

Whether it's managing emails from 100 employees or 10,000, security and helpdesk teams can be overwhelmed with suspicious email reports. Sifting through emails – spam and potential attacks alike – is a boring and thankless task for IT professionals that would rather hunt for spear phishing and ransomware.

On top of that, helpdesk teams are often spread thin and lack the right phishing detection training and skills. Thus, many may fail to identify and escalate threats or establish protective measures such as blocking access to known malicious sites at the perimeter. It's a "lose-lose" when reported threats go unnoticed that can lead to disastrous breaches. The global median time from compromise to discovery is 99 days[7] – giving phishers ample time to wreak their havoc.

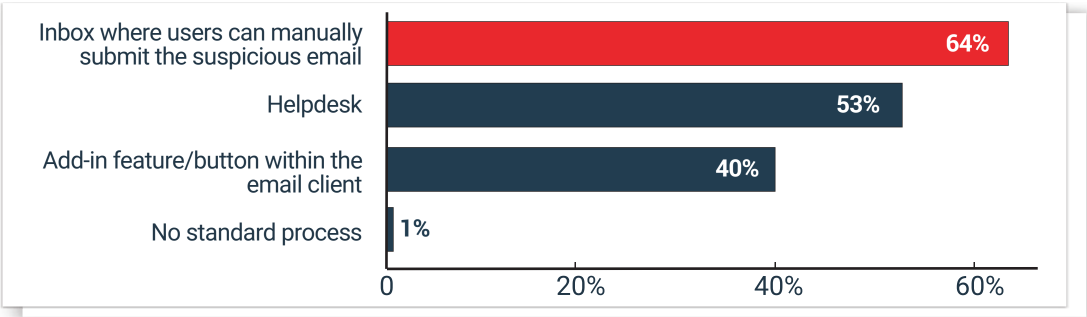


Figure 2: How do users report suspicious emails in your organisation?

100% of respondents have layers of security in place.

The combinations may differ but virtually all surveyed organisations have at least one and many have more than four security solutions in place to help them combat email and phishing threats. Many companies rely on technology alone, with nearly 80% utilising anti-malware solutions and 65% using email gateway filtering.

The Answer: better solutions that (a) leverage broader teams to identify phishing and (b) automate and orchestrate response. By reducing noise in the reporting inbox (if they have one), companies can free responders to focus on real threats.

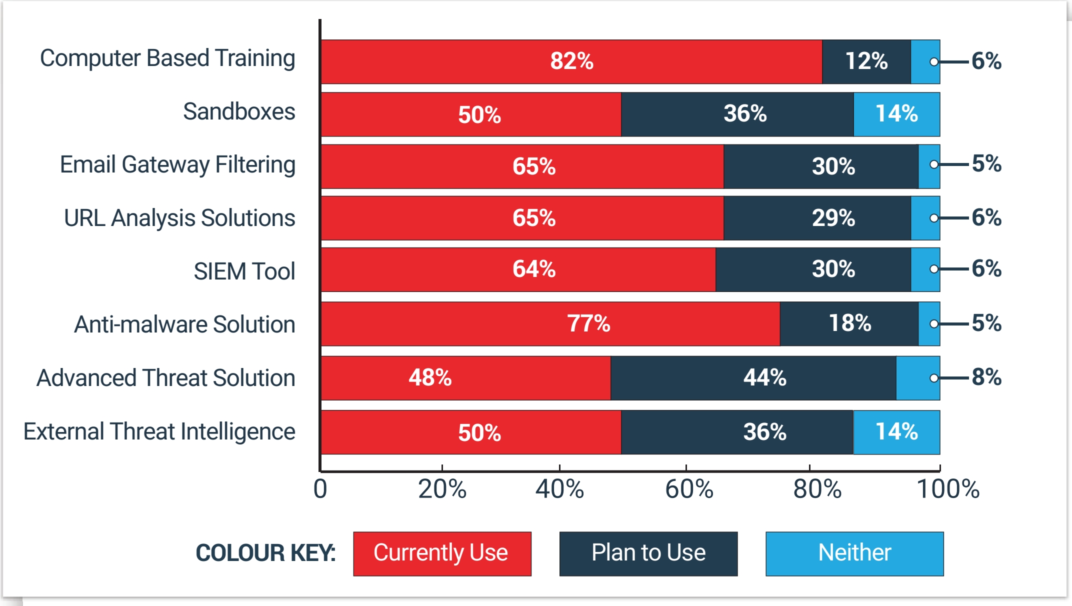


Figure 3: What type(s) of security solutions does your organisation use or plan to use?

2/3 of surveyed IT executives have dealt with a security incident originating with a deceptive email.

Even with global spending for information security products at an estimated $81.6 billion in 2016[8] and the UK's 1.9 billion-pound investment plans to counter cyberattacks,[9] it's clear that no matter how good your perimeter defences are, malicious emails will get through. Our phishing response survey shows that 66% of companies have faced an email-related security incident with 60% facing them more than once.

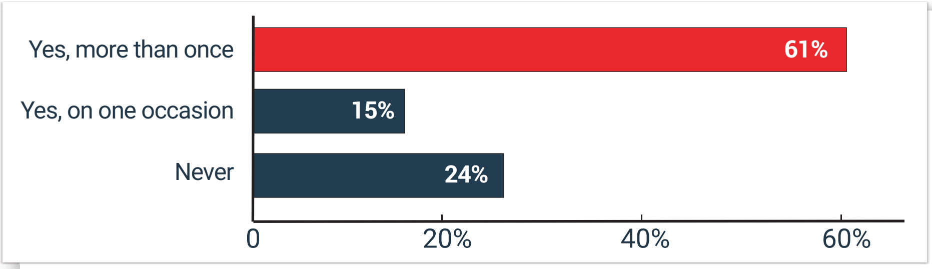


Figure 4: Has your organisation ever experienced a security incident that originated with a deceptive email?

Email-related threats are the biggest security worries.

Despite significant and strategic investments in security, most organisations are still concerned about phishing emails getting through. Malware Bytes reports that 54% of UK companies have been hit by ransomware—and 58% of targets pay up.[10] With even the most tech-savvy companies – think Google and Facebook—being swindled out of millions by phishing scams, concern over email-related threats is valid.

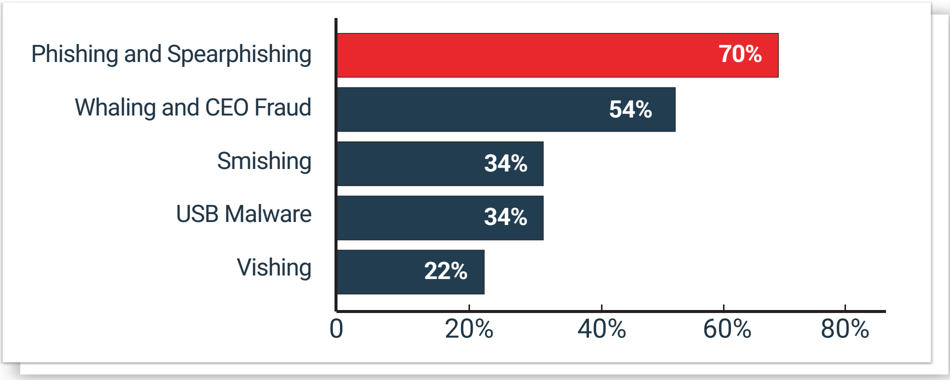


Figure 5: Which of the following security threats concerns you most?

Technology alone won't solve the problem.

Nearly 50% of respondents name lack of integration among security solutions as their biggest anti-phishing challenge. Those solutions mostly rely on tech, not human assets, underscoring that technology by itself isn't the answer to phishing. A human-focused approach—conditioning employees to recognise and report possible phishing—fills in gaps between layers of tech defence.

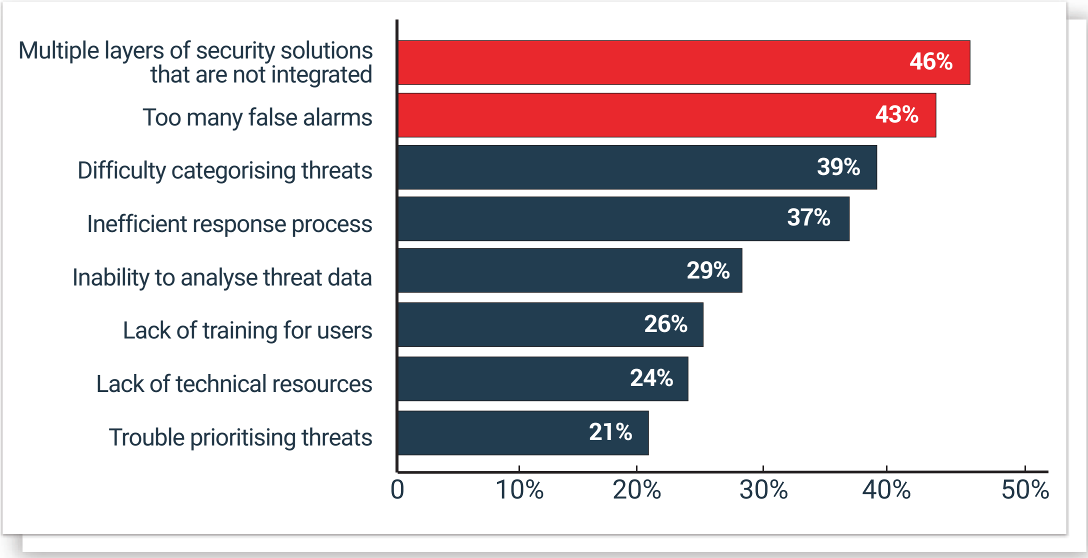


Figure 6: What challenges do you have related to managing phishing attempts?

48% say their phishing response ranges from “ineffective” to mediocre.

In other words, according to our phishing response data, nearly half of companies aren’t feeling too secure. With scattered technology, processes and limited resources, it’s really no surprise. Phishing response can be tough. It’s not like the attacks are aimed at network resources – they target the receptionist, the CEO, the admins, etc. Too often, technology fails at the top of the phishing-detection funnel, so response is inconsistent, depending on the situation.

But with the right systems, software and education, they can sleep better. At Cofense, we’ve seen organisational susceptibility to phishing emails drop 20% in just a few weeks after just one failed simulated attack and better engagement among all employees to help fight phishing.

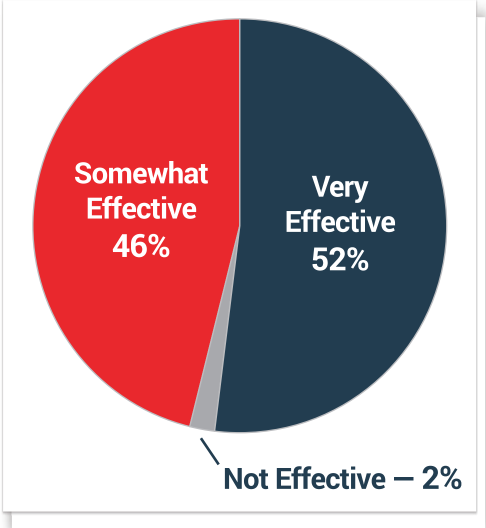


Figure 7: How effective do you think your current phishing response process is?

96% plan to upgrade their phishing prevention and response over the next year.

In Q4 2016 alone there were over 1.2 million[11] phishing attacks and nearly a quarter of UK companies have lost confidential data due to email-based impersonation attacks.[12] As phishing emails become more sophisticated and dangerous, businesses know they need to keep defences up-to-date. Most aren’t waiting, with plans to make upgrades within 12 months.

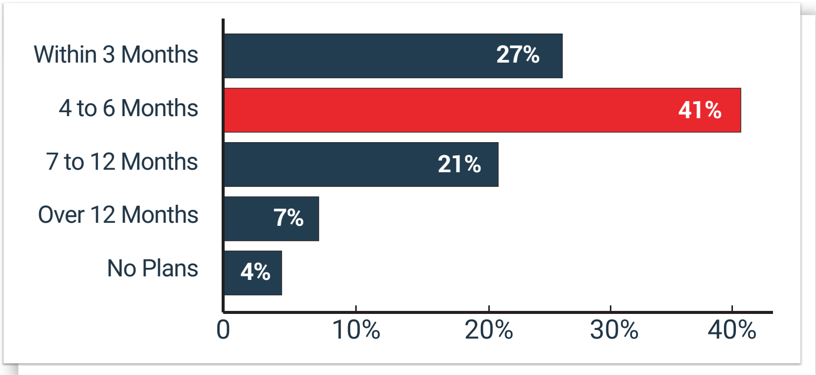


Figure 8: When do you expect to update or augment your phishing prevention and response processes?

Automated analysis: #1 on the wish list of anti-phishing solutions.

Manually analysing phishing emails and possible malware is difficult and time-intensive. And although many have various analysis tools, they usually don't work in concert, complicating the responder's job—while malware may be spreading throughout the organisation. Automation could be the answer to eliminating the manual tasks spread across already thin resources.

Are all employees going to "get it" every time? Probably not. But they don't have to if the rest of the organisation is ready to recognise and report suspicious emails. It only takes one to report it, so the incident response team can substantially reduce the impact of phishing attacks.

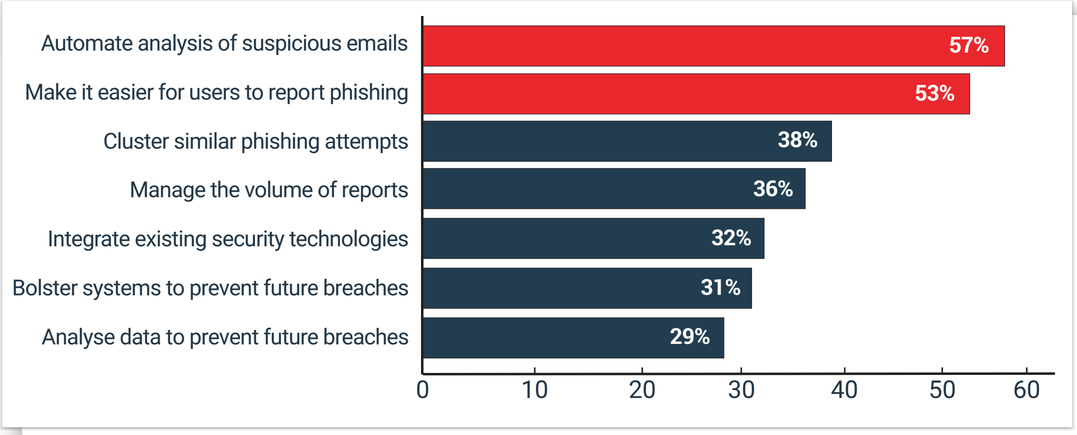


Figure 9: What do you wish you could do better regarding phishing attempts?

The Missing Link

Investments in anti-phishing technology alone aren't doing the job. Phishing threats of all types continually reach employees, so companies need to view them as their last line of defence.

Popular technologies, like email gateway filtering and anti-malware solutions, work – but only up to a point. But trained, vigilant employees are often better at detecting attacks such as Business Email Compromise (BEC). Human-reported intelligence can be invaluable to incident responders, who, in turn, can use automation to analyse and react.

Are all employees going to "get it" every time? Probably not. But they don't have to if the rest of the organisation is ready to recognise and report suspicious emails. It only takes one to report it, so the incident response team can substantially reduce the impact of phishing attacks.

CASE STUDY: Large EMEA Manufacturer Fight Phishing with Cofense

Recognising their employees were vulnerable to phishing attacks, a multinational manufacturer of imaging and optical products with more than 18,000 employees in the EMEA region concluded it was only a matter of time before a phishing attack would cause serious damage.

The client's ability to catch phishing emails has vastly improved since implementing Cofense Simulator and Cofense Reporter. According to the client, Cofense's technical support has remained accessible and responsive throughout the adoption process. "They give results in a couple of hours and they're very nice people – all of them." The client notes that compared with other vendors getting support from Cofense is definitely easier. Based on that success, and the technology's tangible results. The Information Security Manager says he'd have no qualms about recommending Cofense to his peers. When anyone asks him how to deal with phishing, his answer is simple: "Buy Cofense."[13]

| Read More >>

ABOUT Cofense

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyberattacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.

CITATIONS

1. Anti-Phishing Working Group, "Phishing Activity Trends Report 4th Quarter 2016," 2016.
2. The Ponemon Institute, "Cost of Data Breach Study," 2017.
3. Wired UK, "Millions of Customer Records and Card Details Stolen from Cex," 2017.
4. Ibid.
5. The Radicati Group, Inc., "Email Statistics Report, 2015-2019."
6. Verison, "2017 Data Breach Investigations Report 10th edition," 2017.
7. Mandiant, "M-Trends 2017: A View from the Front Lines," 2017.
8. Information Week, "Global IT Security Spending Will Top $81 Billion in 2016," 2016.
9. Cabinet Office, HM Treasury, The Rt Hon Ben Gummer, and The Rt Hon Philip Hammond MP, "Britain's cyber security bolstered by world-class strategy," 2016.
10. Malware Bytes, "State of Ransomware," 2017.
11. Cisco Continuum News, 2017.
12. Computer Weekly, "UK Impersonation Fraud up 39% in Last Quarter of 2016," 2017.
13. Cofense, "Cofense Reduces Global Phishing Exposure," 2017.