PHISHING RESPONSE TRENDS

Europe

COFENSE

OVERVIEW

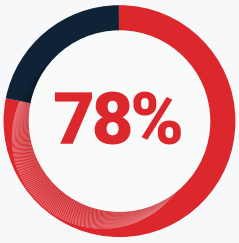
Companies in Europe and around the world are ramping up to fight phishing. No wonder. Last year, there were over 1.2 million phishing attacks globally, a 65% annual increase.[1] So, is Europe winning the war against email-related threats?

The findings of this report strongly suggest not. Most businesses in the countries we surveyed—the UK, Germany, France, the Netherlands and Belgium—are barely holding ground or flat out losing.

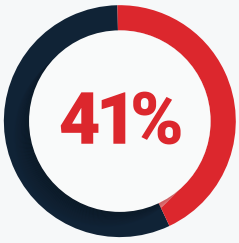
They're flooded with suspicious emails targeting employees, but are ill-prepared to manage and respond to those threats. In fact, most companies think they have insufficient anti-phishing expertise and rate their incident response process as weak.

Headlines throughout Europe echo these alarms. According to a major study, UK companies are the world's most frequent business targets of phishing[2]. Also, hackers targeted senior engineers at Irish energy networks and, while networks weren't disrupted, the attackers may have stolen passwords and other sensitive information.[3] Through a similar spear phishing attack, hackers infiltrated the network of a German steel mill and inflicted "massive" physical damage.[4] Outside the business arena, Russia-linked hackers attempted, with mixed success, to compromise the systems of pro-EU French presidential candidate Jean Macron.[5]

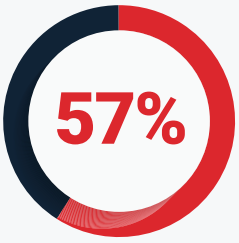
Notable Findings of This Report



Surveyed IT executives have dealt with a **security incident originating with a deceptive email**



Say their biggest anti-phishing challenge **is poorly integrated security systems**



Say their phishing response ranges from **"not effective" to only "somewhat effective"**

Security concern is **phishing and related threats**

In other words, despite all their investments in technology, almost 80% of European companies surveyed for this study have experienced a phishing-related incident. With nearly 6 in 10 companies believing they have insufficient defences, there's a gap between "We're worried" and "We're well prepared."

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

Research consultant Censuswide surveyed select European IT executives on phishing response strategies. Five hundred executives participated, largely senior decision-makers who work across security operations centres (SOCs) and incident response or threat analysis teams.

Numerous Industries

The surveyed companies represent 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.

78% have dealt with a security incident originating with a deceptive email, with nearly half experiencing an incident more than once.

Global spending for information security products was an estimated $81.6 billion in 2016[6]. But no matter how good your perimeter defences are, malicious emails will get through. Our survey shows that 45% of companies have faced an email-related security incident more than once, with almost 1/3 having handled single incidents.

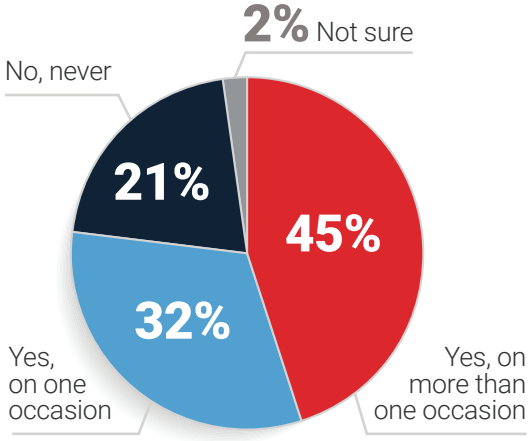


Figure 1: Has your organisation ever experienced a security incident that originated with a deceptive email?

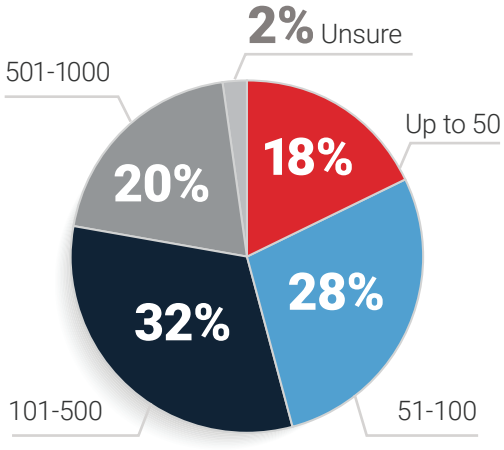


Figure 2: How many suspicious emails are reported in your organisation each week?

1 in 5 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,[7] it's no surprise that phishing is the top attack vector in data breaches.[8] Now imagine being on 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 or even thousands of emails to find the real threats? Automated phishing response platforms are your best bet. They identify and rank threats by severity, allowing responders to do their jobs more efficiently.

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 who'd rather hunt spear phishing and ransomware.

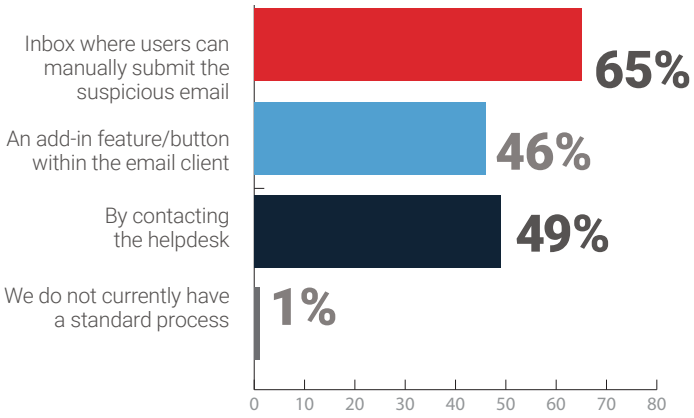
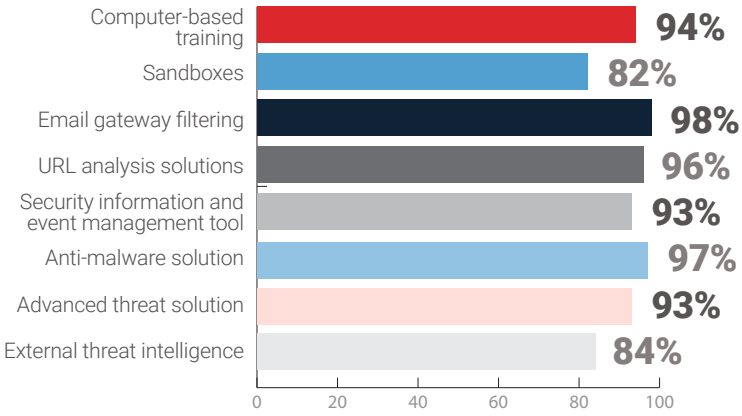


Figure 3: How do users report suspicious emails in your organisation?

On top of that, helpdesk teams are often spread thin and lack the right phishing detection training and skills. 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 and invite disastrous breaches. The global median time from compromise to discovery is 99 days[9]—giving phishers ample time to wreak havoc.



***** Multiple responses allowed.

Figure 4: What type(s) of security solutions does your organisation use or plan to use?

Nearly all respondents have layers of security in place.

In fact, while the combinations may differ, many companies have more than four security solutions in place to combat email and phishing threats. They often rely on technology alone, with two-thirds utilising anti-malware solutions and roughly the same percentage using email gateway filtering.

Ultimately, the answer is 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.

Email-related threats are the biggest security worries.

70 million euros. That's how much Belgian bank Crelan lost in a phishing-induced breach. The tactic was CEO fraud, a kind of business email compromise (BEC) that targets C-level executives.

After compromising the email account of a top executive (or convincingly impersonating his/her emails) the attackers sent a message to Finance ordering disbursement of funds. Such orders usually come with reasons why they must be carried out right away and kept under wraps. Though law enforcement agencies have warned businesses about BEC scams, untrained employees still fall for them.[10]

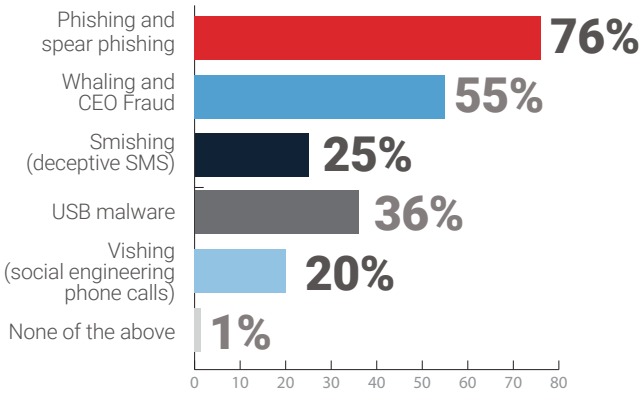
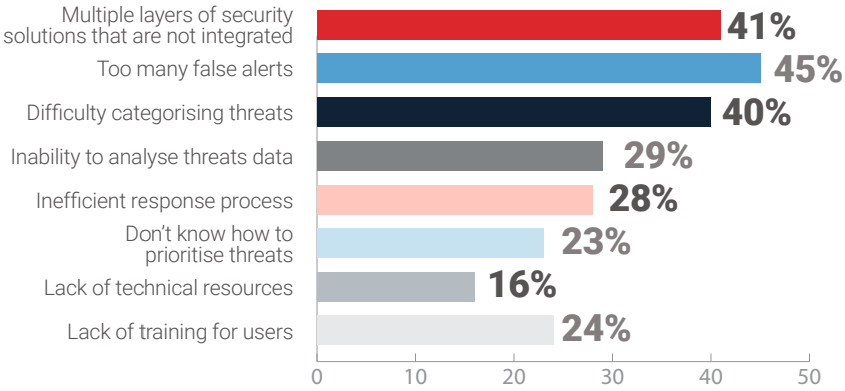


Figure 5: Which of the following security threats concerns you most?

With even the most tech-savvy companies—think Google and Facebook—losing millions in phishing scams, everyone should be keeping a close eye on their inboxes.



***** Multiple responses allowed.

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

Technology alone won't solve the problem.

More than 40% of respondents cite systems integration as their top anti-phishing challenge, a close second to numerous false alerts. This underscores that technology alone 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. Employees feed valuable intelligence to machines for rapid analysis, which in turn helps incident responders spot real threats faster.

57% say their phishing response ranges from ineffective to mediocre.

In other words, over half of organisations aren't feeling too secure. With scattered technology, processes and limited resources, it's not a shock.

Phishing response can be tough. It's not like the attacks are aimed at network resources—they target the receptionist, the CEO, the admins, you name it. Too often, technology fails at the top of the phishing-detection funnel, so response is inconsistent, depending on the situation.

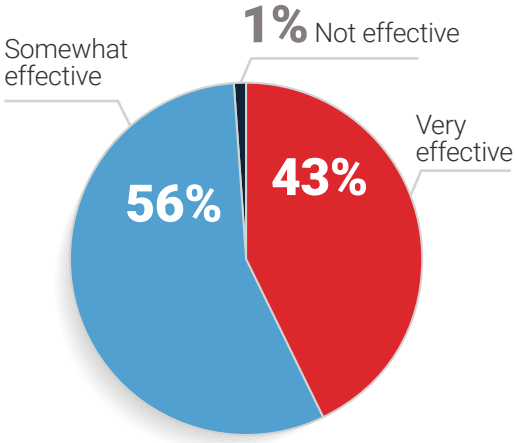


Figure 7: How effective do you think your current phishing response process is?

But with the right systems, software and education, companies can breathe easier. At Cofense, we've seen organisational susceptibility to phishing emails drop 20% in just a few weeks, after only one failed simulated attack, along with better overall employee engagement.

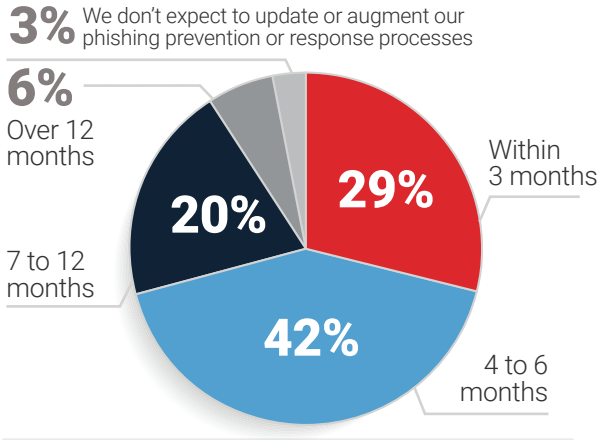


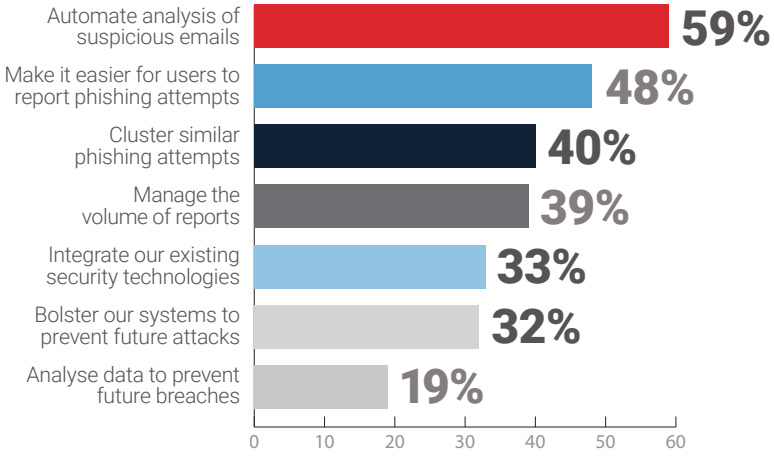
Figure 8: When do you expect to update or augment your phishing prevention and response processes?

91% plan to upgrade their phishing prevention and response over the next year.

In Q4 2016 alone, the world saw over 1.2 million phishing attacks[11]. 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.

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

Manually analysing emails is difficult and time-intensive. Although companies have a choice of various analysis tools, they usually don't work in concert, complicating the responder's job—while malware may be spreading throughout the organisation. More than half of respondents see automation as the best way to eliminate manual tasks and maximise finite resources



* Multiple responses allowed.

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. Trained, vigilant employees are often better at detecting threats like BEC attacks. Human-reported intelligence is 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 that's not necessary if the rest of the organisation is trained to recognise and report phishing.

Large Multinational Manufacturer Fights Phishing with Cofense

Recognising its employees were vulnerable to phishing attacks, a multinational manufacturer of imaging and optical products decided to act. The company implemented Cofense PhishMe™ and Cofense Reporter™, so employees could identify and report suspicious emails. Since then, the company's ability to reduce phishing has improved vastly.

Moreover, this business has found the Cofense technical support team to be accessible and responsive. "They give results in a couple of hours and they're very nice people—all of them."

The manufacturer's 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."[12]

Read the Full Story

HOW EUROPE'S PHISHING RESPONSE COMPARES TO THE US

Cofense has also produced a report on phishing response trends in the US. Here's how key results in Europe stack up:

		
More European companies say they're unprepared for phishing.	**57%**	**43%**
Yet more in Europe have dealt with security incidents sparked by deceptive emails.	**78%**	**66%**
Like US counterparts, most European companies delay response with manual phishing reporting or no reporting at all.	**65%**	**75%**
Most European companies plan to upgrade their phishing defence within the next year.	**91%**	**80%**
In Europe, automated email analysis is the most wished-for anti-phishing solution.	**59%**	**33%**

ABOUT Cofense

Phishing emails will continue to evade your layers of defence and reach your end users. Turning employees into your last line of defence is the best way to fortify your entire organisation. The key: conditioning employees to recognise and report malicious emails so incident response teams can research and respond faster. Cofense focuses on engaging the human–your last line of defence after a phish bypasses other technology—and enabling incident response teams to quickly analyse and respond to targeted phishing attacks.

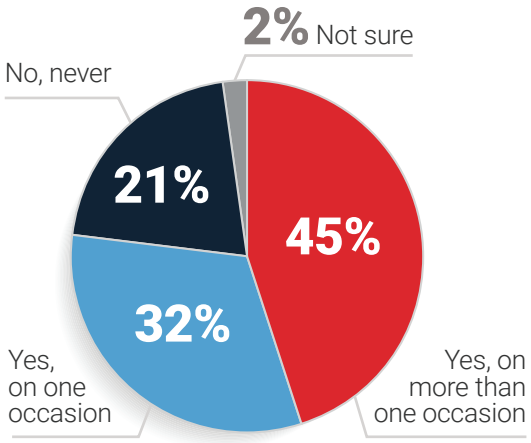
Learn more about Cofense solutions at www.cofense.com

CITATIONS

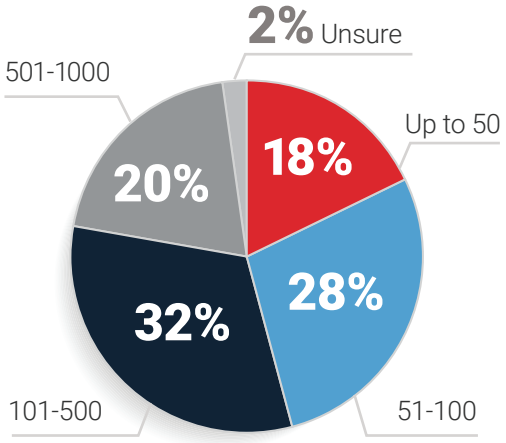
1. Anti-Phishing Working Group (APWG), "Phishing Activities Trends Report," 2017.
2. IT Pro, "UK Businesses under Attack from Phishing Scams," 2016.
3. The Independent, "Hackers Target Irish Energy Networks Amid Fears of Further Cyber-Attacks on UK's Crucial Infrastructure," 2017.
4. Wired, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," 2015.
5. CNBC, "French Presidential Frontrunner's Campaign Hit by Phishing Attempts from Russia-Linked Hackers," 2016.
6. Information Week, "Global IT Security Spending Will Top $81 Billion in 2016," 2016.
7. The Radicati Group, Inc., "Email Statistics Report, 2015-2019," 2015.
8. Verizon, "2017 Data Breach Investigations Report 10th edition," 2017.
9. Mandiant, "M-Trends 2017: A View from the Front Lines," 2017.
10. HelpNet Security, "Belgian Bank Crelan Loses €70 Million to BEC Scammers," 2016.
11. Cisco Continuum News, 2017.
12. Cofense, "Multinational Imaging and Optical Manufacturer Reduces Global Phishing Exposure with Cofense," 2017.

APPENDIX I : United Kingdom

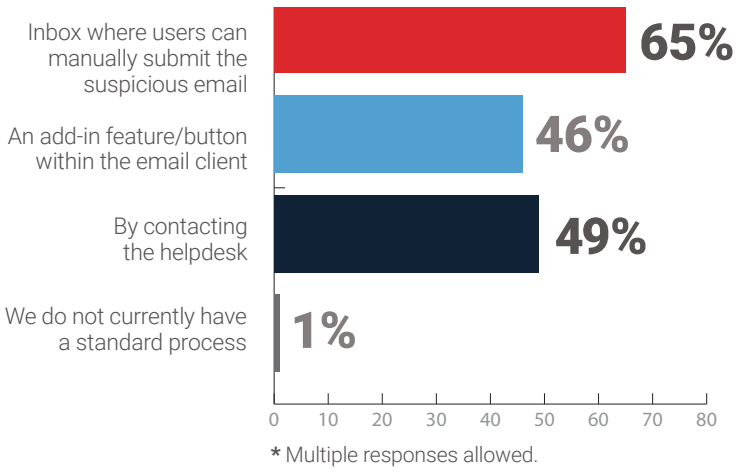
Has your organisation ever experienced a security incident that originated with a deceptive email?



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



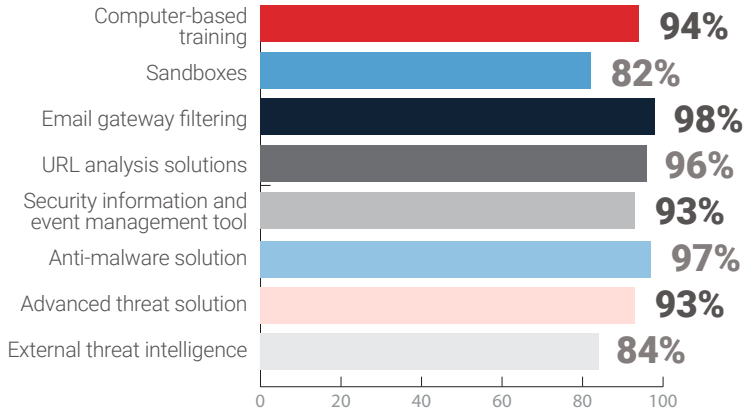
How do users report suspicious emails in your organisation?



* Multiple responses allowed.

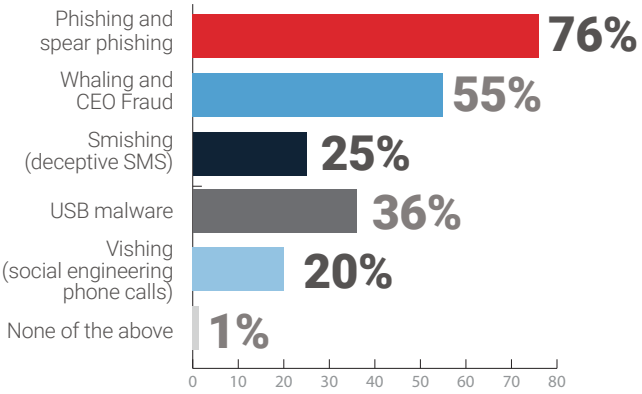
APPENDIX I : United Kingdom

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



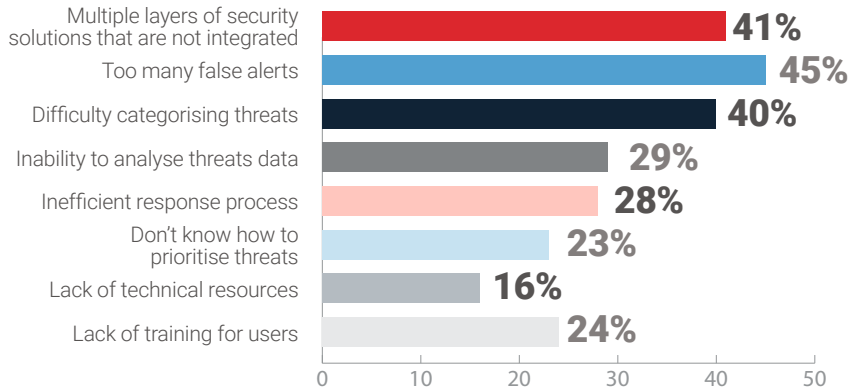
* Multiple responses allowed.

Which of the following security threats concerns you most?



* Multiple responses allowed.

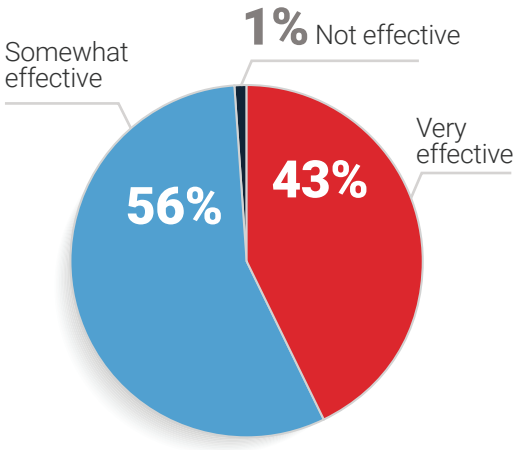
What challenges do you have related to managing phishing attempts?



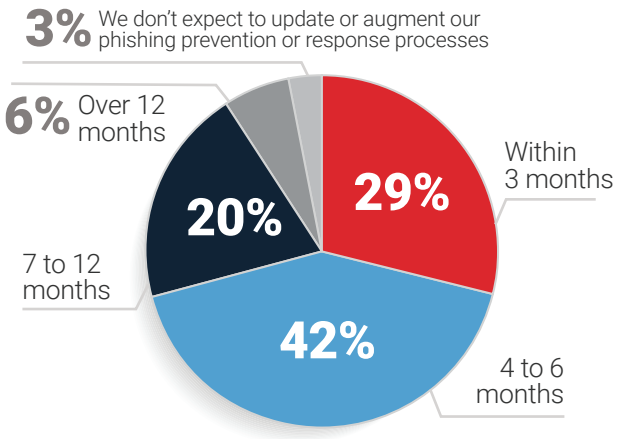
* Multiple responses allowed.

APPENDIX I : United Kingdom

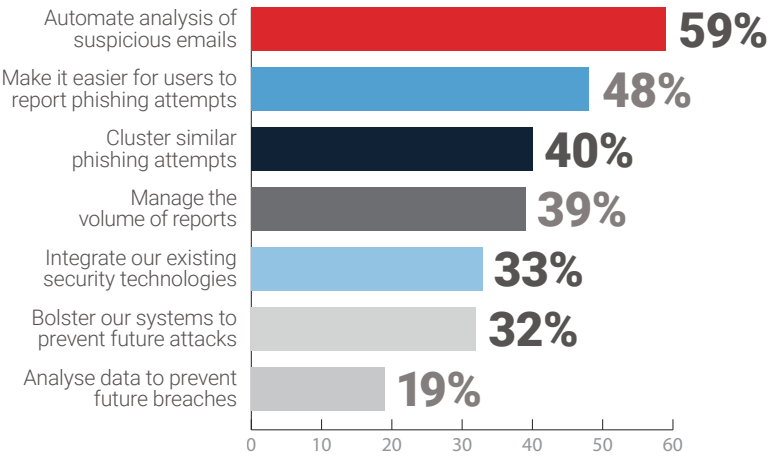
How effective do you think your current phishing response process is?



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

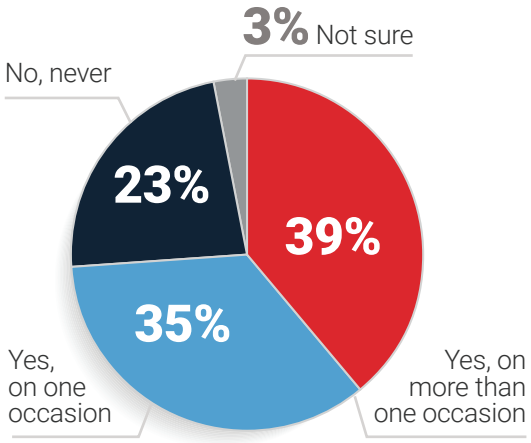


What do you wish you could do better regarding phishing attempts?

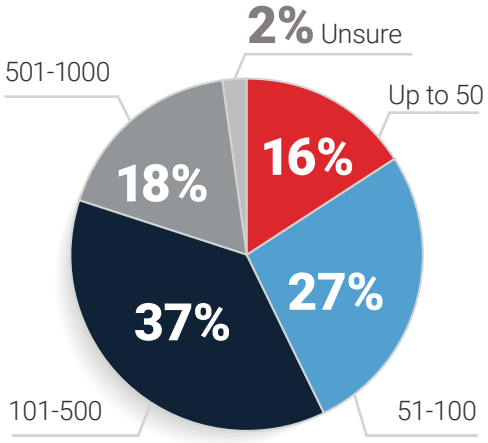


APPENDIX II : Germany

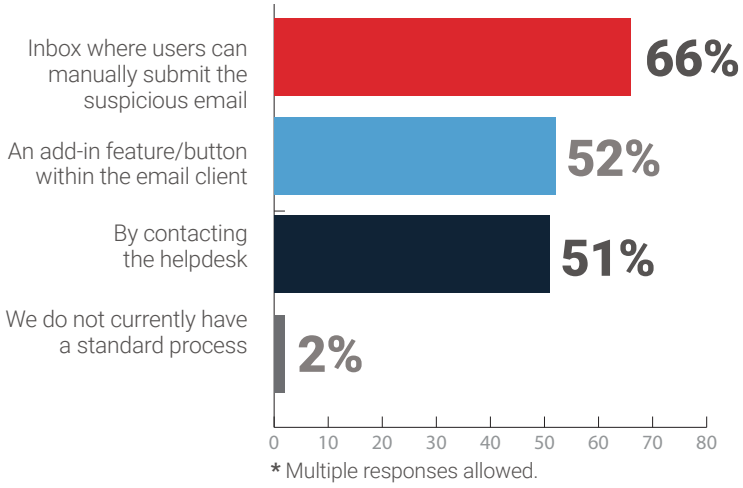
Has your organisation ever experienced a security incident that originated with a deceptive email?



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



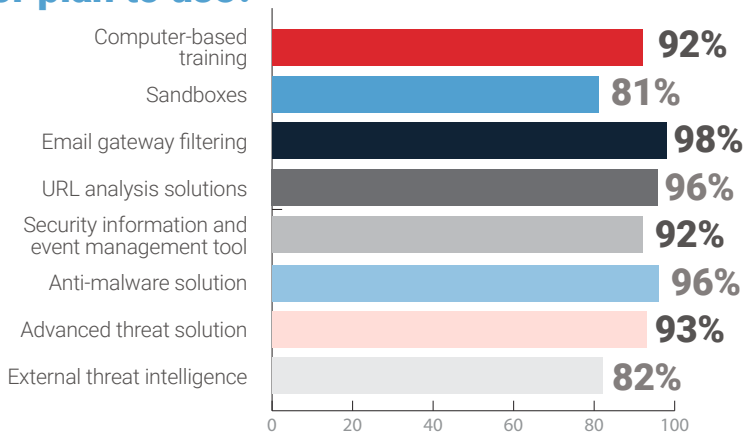
How do users report suspicious emails in your organisation?



* Multiple responses allowed.

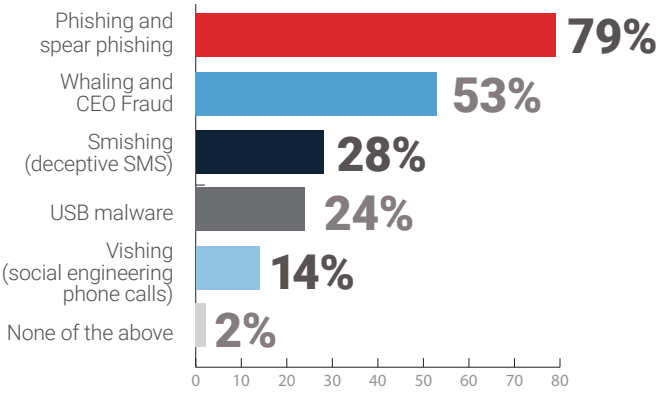
APPENDIX II : Germany

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



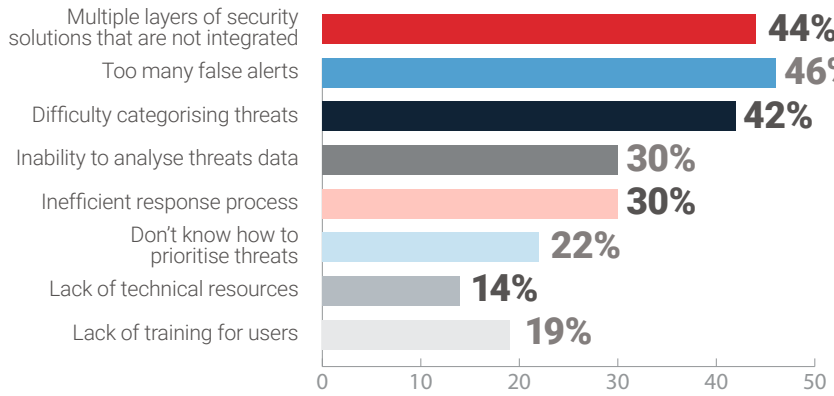
* Multiple responses allowed.

Which of the following security threats concerns you most?



* Multiple responses allowed.

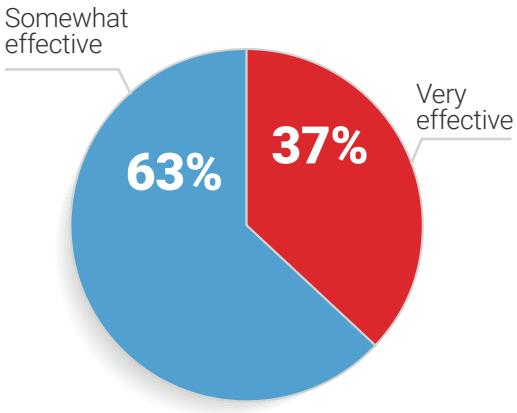
What challenges do you have related to managing phishing attempts?



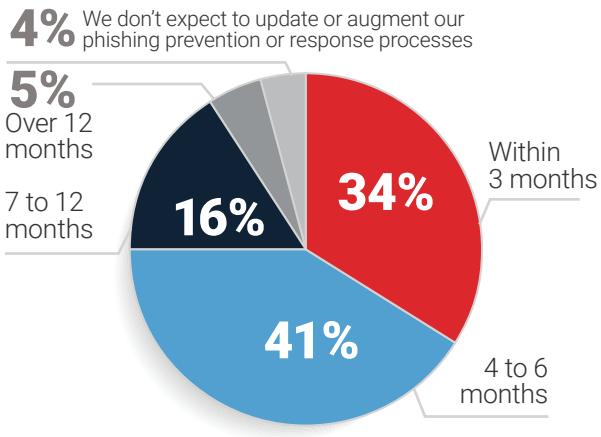
* Multiple responses allowed.

APPENDIX II : Germany

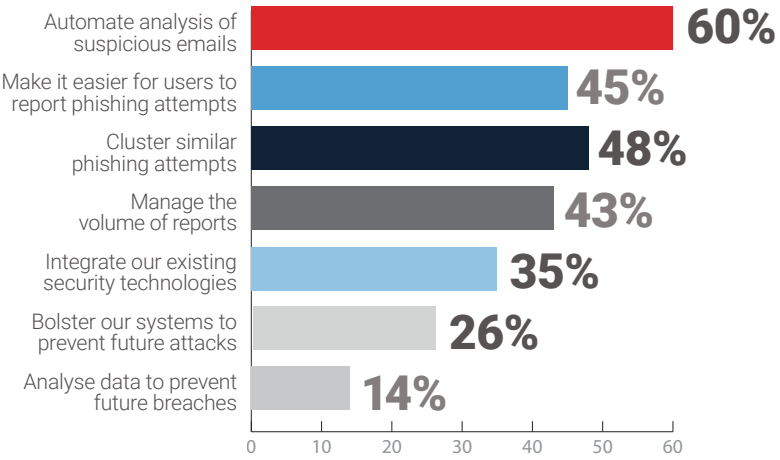
How effective do you think your current phishing response process is?



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



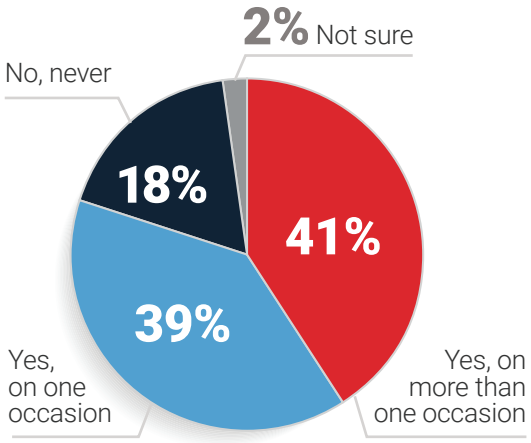
What do you wish you could do better regarding phishing attempts?



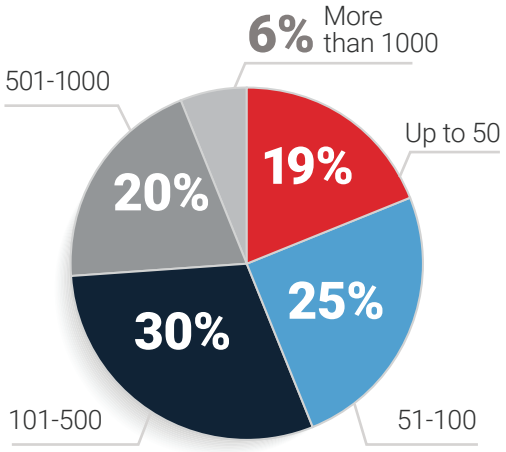
* Multiple responses allowed.

APPENDIX III : France

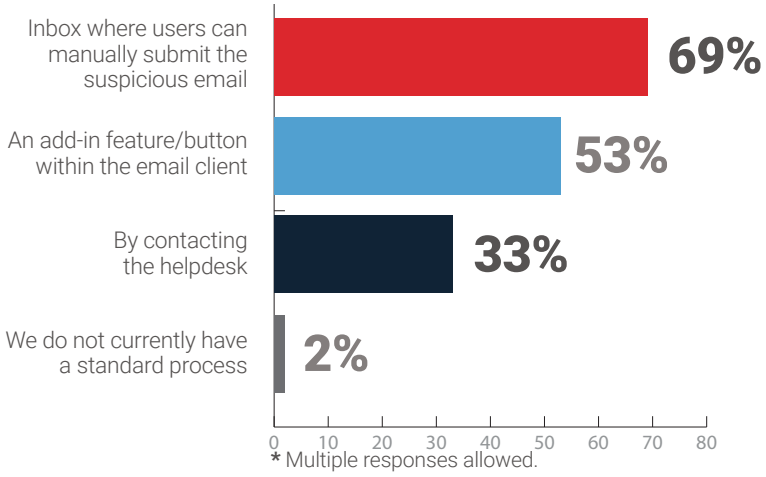
Has your organisation ever experienced a security incident that originated with a deceptive email?



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

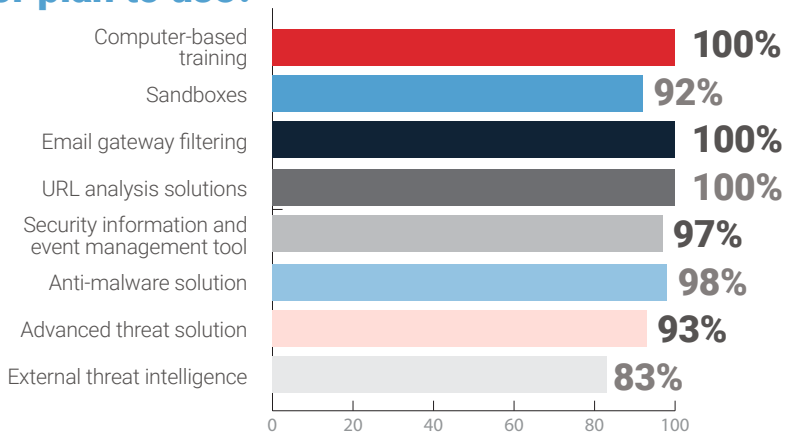


How do users report suspicious emails in your organisation?



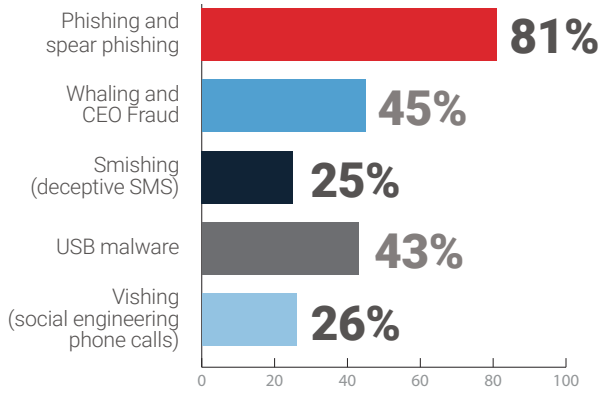
APPENDIX III : France

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



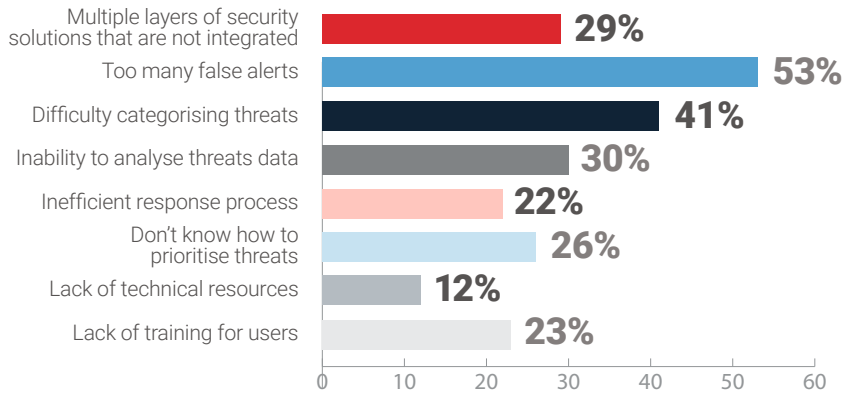
* Multiple responses allowed.

Which of the following security threats concerns you most?



* Multiple responses allowed.

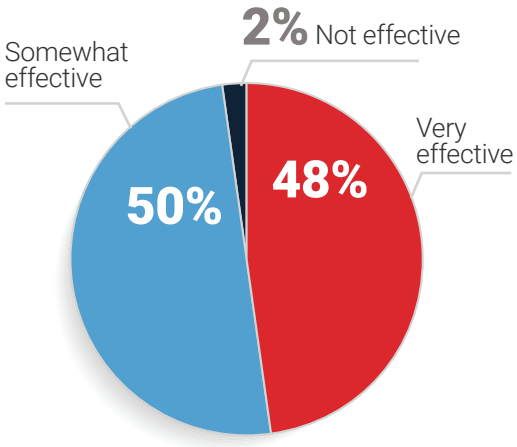
What challenges do you have related to managing phishing attempts?



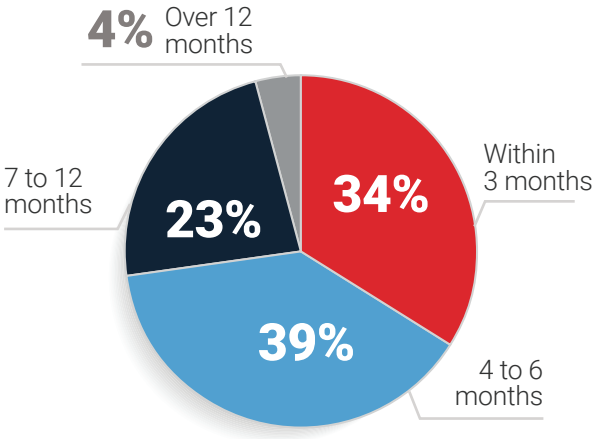
* Multiple responses allowed.

APPENDIX III : France

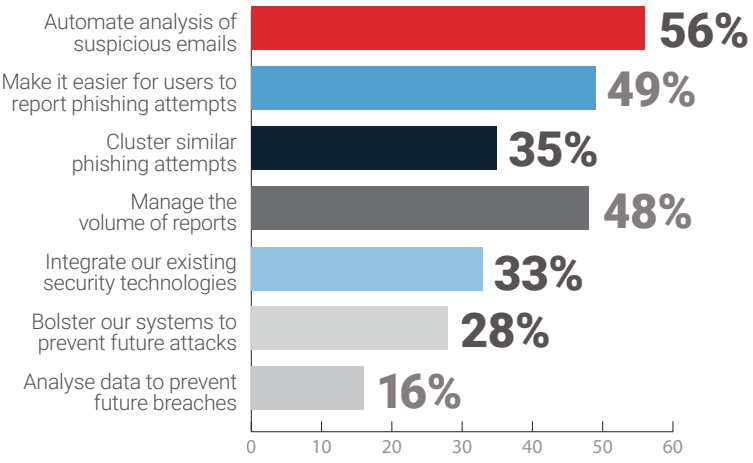
How effective do you think your current phishing response process is?



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



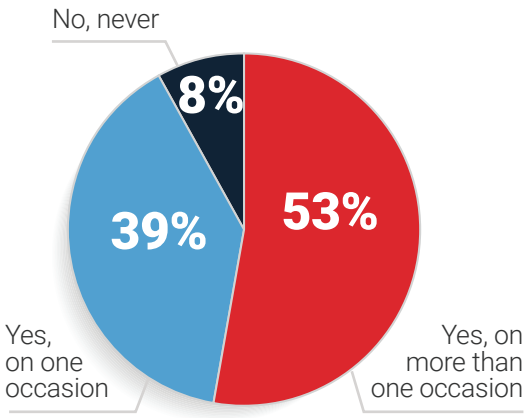
What do you wish you could do better regarding phishing attempts?



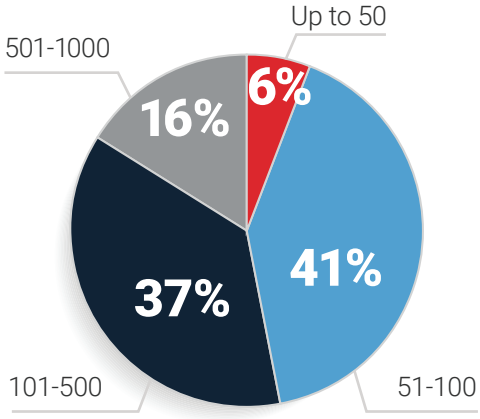
* Multiple responses allowed.

APPENDIX IV : Belgium

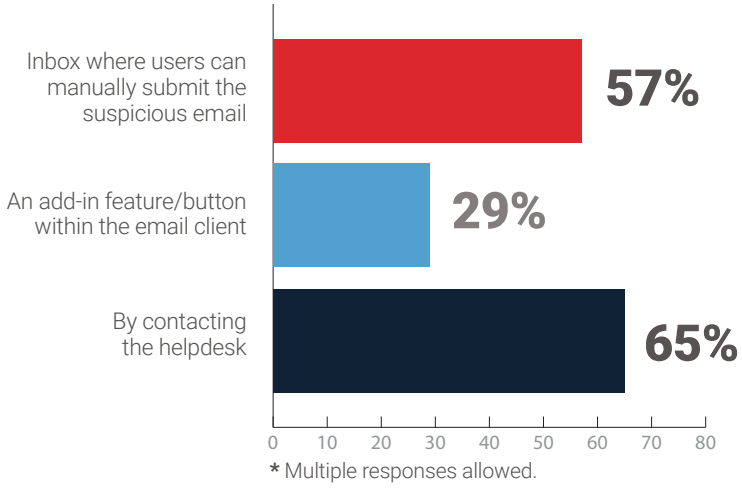
Has your organisation ever experienced a security incident that originated with a deceptive email?



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



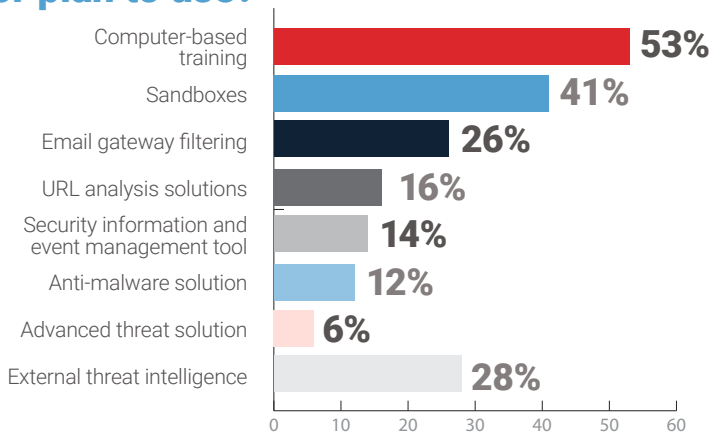
How do users report suspicious emails in your organisation?



* Multiple responses allowed.

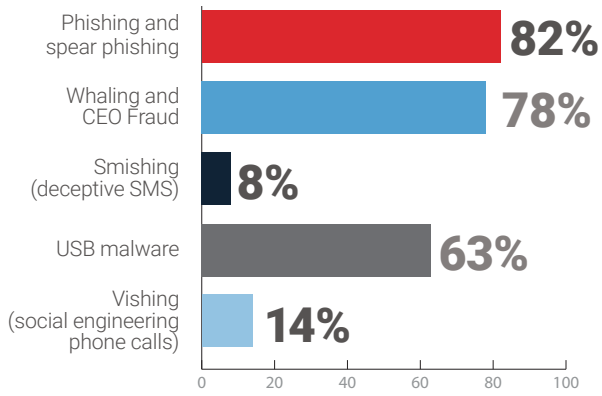
APPENDIX IV : Belgium

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



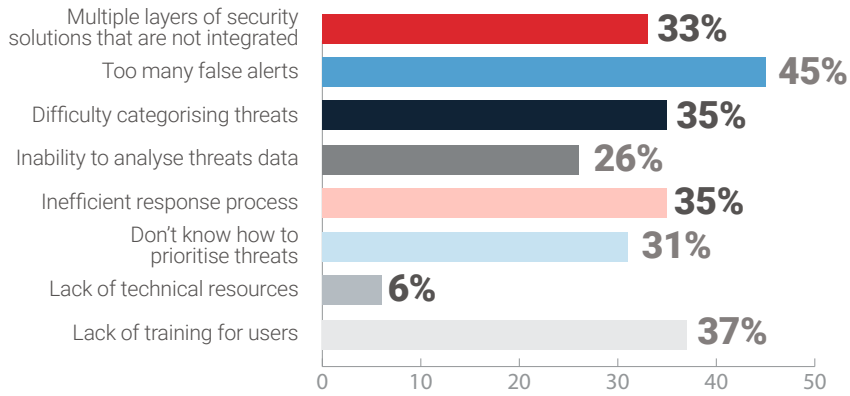
* Multiple responses allowed.

Which of the following security threats concerns you most?



* Multiple responses allowed.

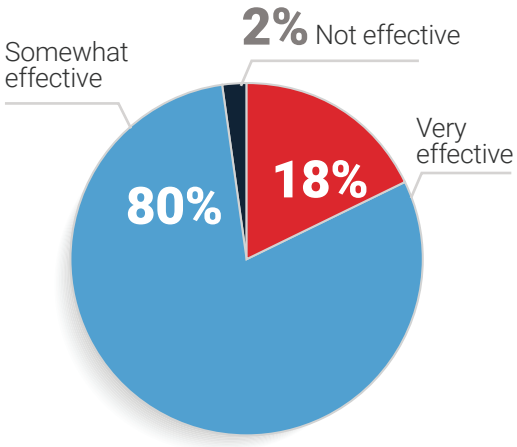
What challenges do you have related to managing phishing attempts?



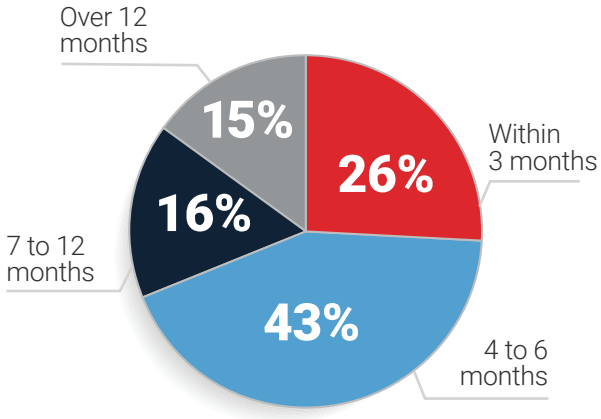
* Multiple responses allowed.

APPENDIX IV : Belgium

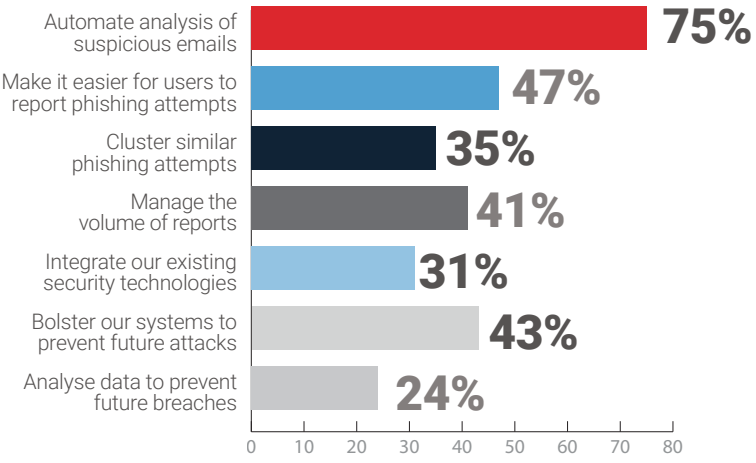
How effective do you think your current phishing response process is?



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



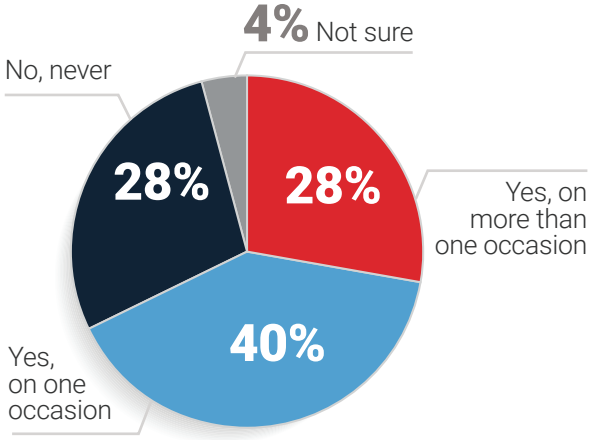
What do you wish you could do better regarding phishing attempts?



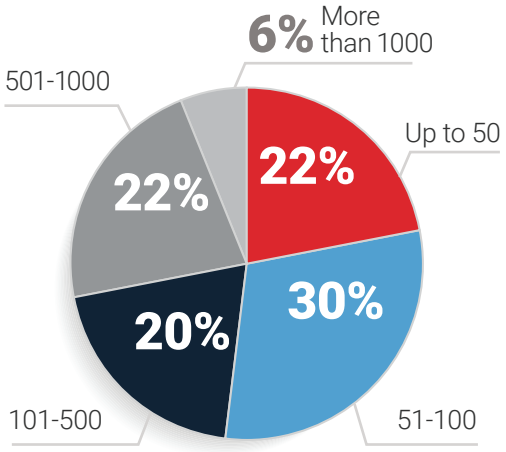
* Multiple responses allowed.

APPENDIX V : The Netherlands

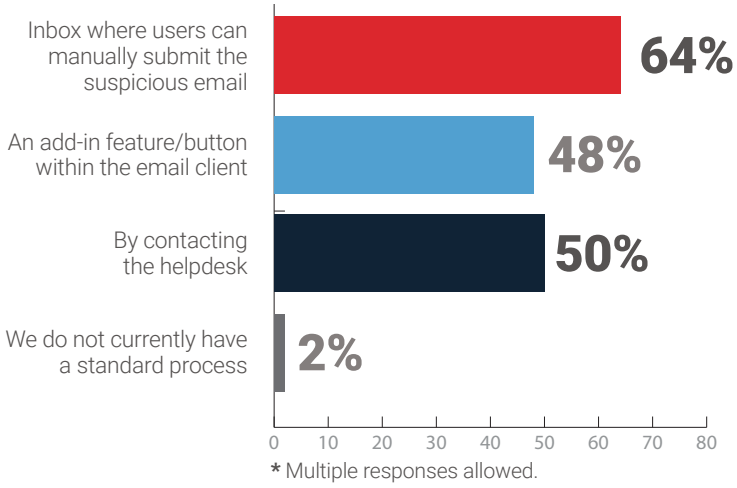
Has your organisation ever experienced a security incident that originated with a deceptive email?



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



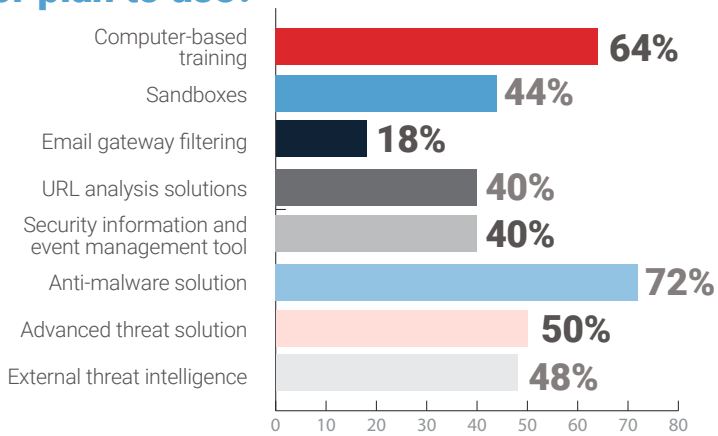
How do users report suspicious emails in your organisation?



* Multiple responses allowed.

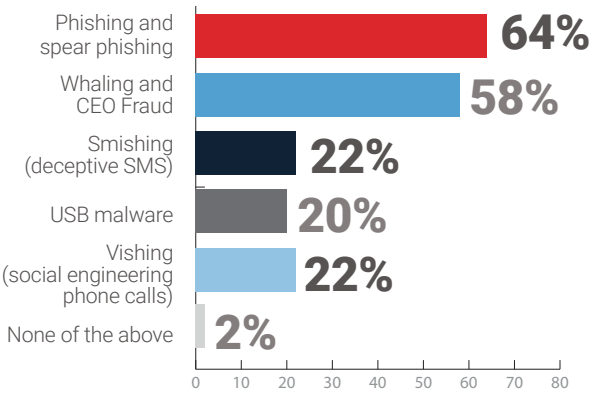
APPENDIX V : The Netherlands

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



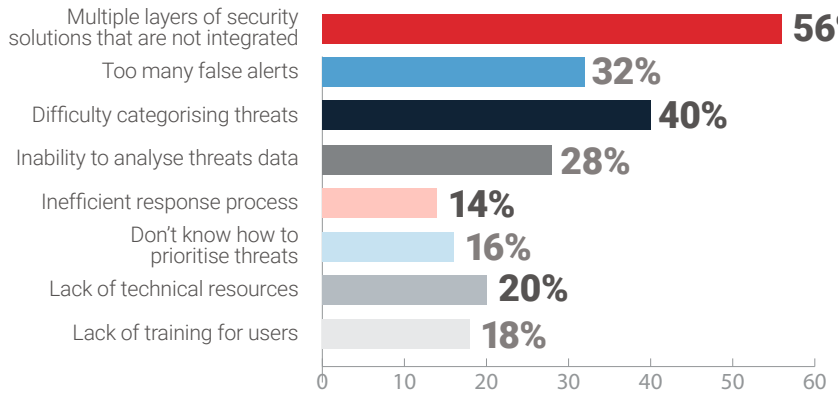
* Multiple responses allowed.

Which of the following security threats concerns you most?



* Multiple responses allowed.

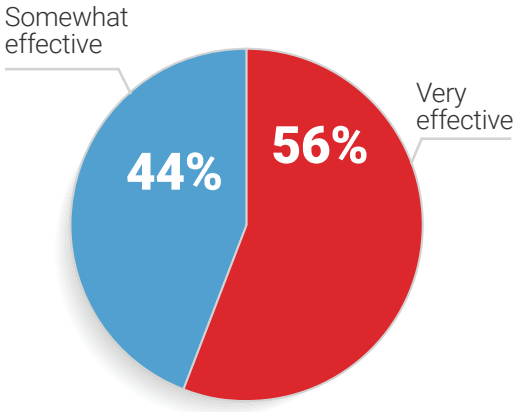
What challenges do you have related to managing phishing attempts?



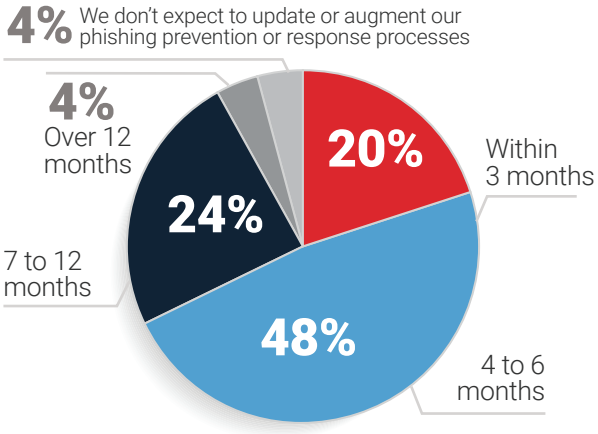
* Multiple responses allowed.

APPENDIX V : The Netherlands

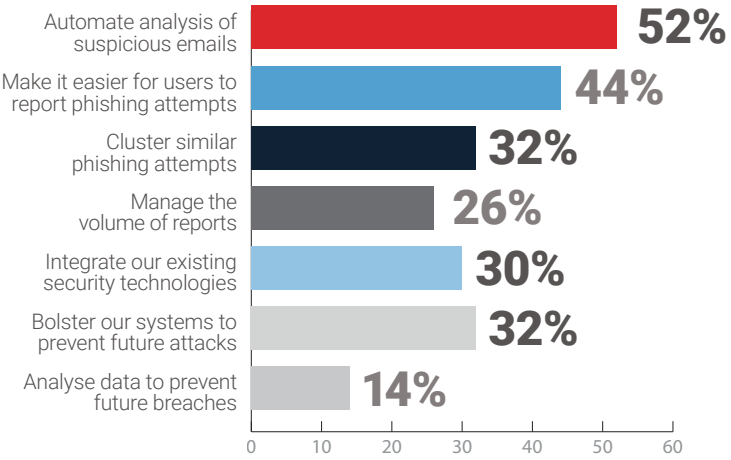
How effective do you think your current phishing response process is?



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



What do you wish you could do better regarding phishing attempts?



* Multiple responses allowed.