# PHISHING CONFESSIONS FROM SECURITY PROFESSIONALS

COFENSE.COM

# WE ASKED 102 SECURITY PROFESSIONALS 11 QUESTIONS ABOUT PHISHING.

The topics covered the gamut: personal experience with phishing, developments making the problem worse, challenges in tackling it, approaches to phishing defence, and more. Some data on survey respondents:

## ORGANISATION SIZE

- 200 employees or fewer – 22%
- 200-1,000 employees – 24%
- 1,000-5,000 employees – 17%
- More than 5,000 employees – 37%

## PROFESSIONAL ROLES

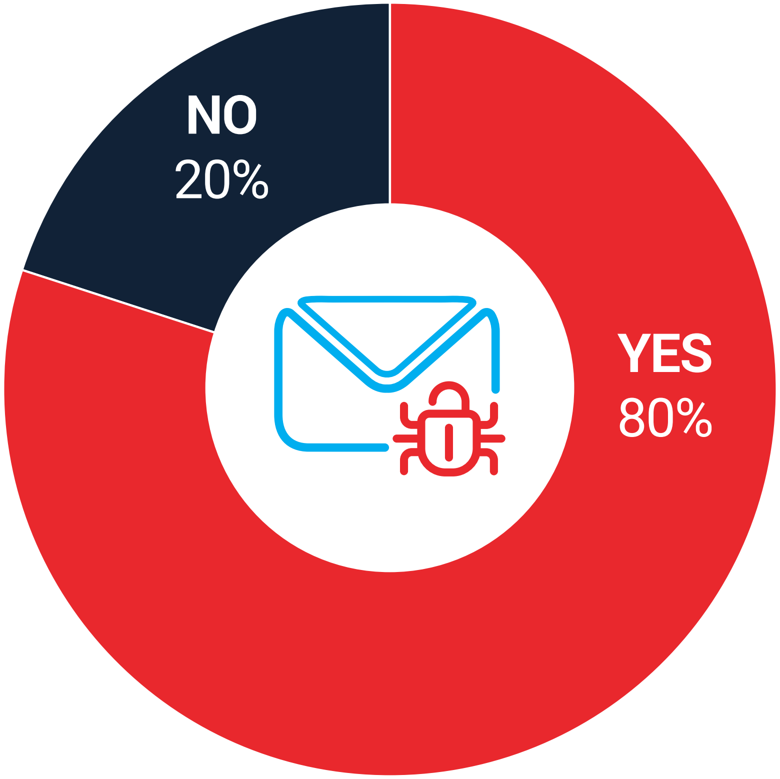
Multiple Responses Allowed

- 52% were in IT Security
- 41% were in Security Operations
- 18% were in Incident Response

Here’s what security professionals told Cofense about phishing and how they combat the threat.

# 80% KNOW SOMEONE **VICTIMISED BY PHISHING.**

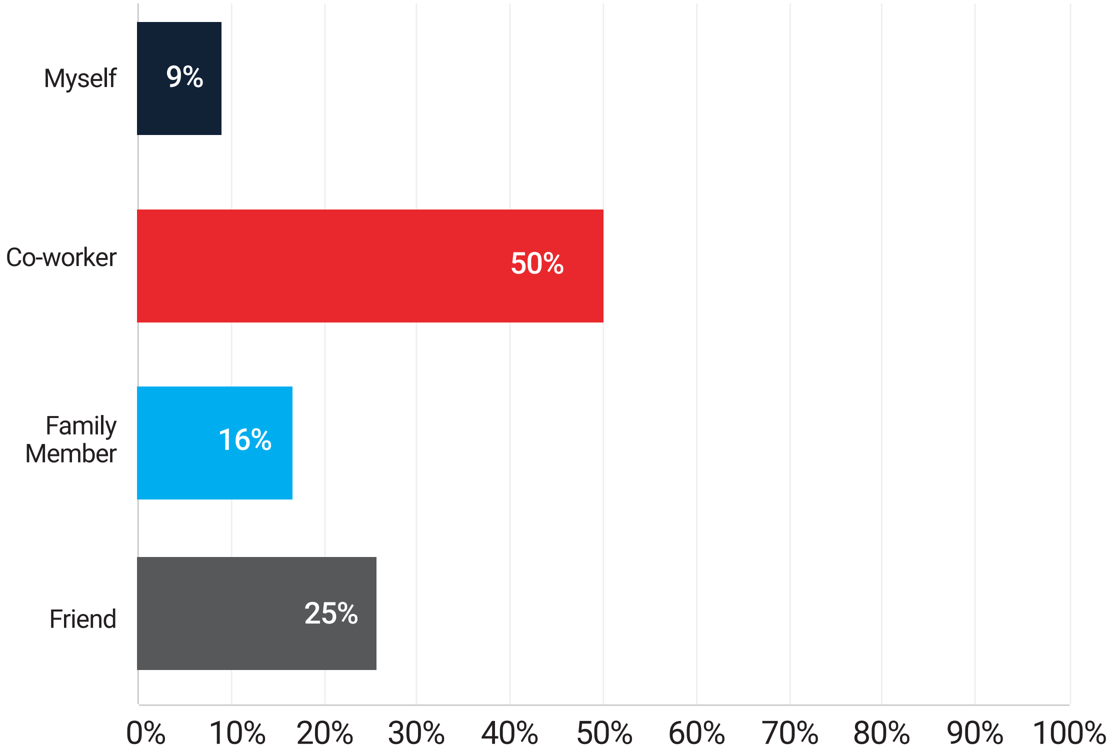
This tracks with findings from other sources. The Anti-Phishing Working Group (APWG) reports that phishing attacks are growing by 65% annually.[1] The average phishing attack costs a mid-sized company $1.6 million[2] and, according to the FBI, Business Email Compromise (BEC) cost global businesses over $5 billion from 2013 to 2016.[3] If you know someone tricked by a phishing email, you've got lots of company. If you don't, you're in the minority. At least for now...



**Do you know anyone that has fallen victim to a phishing attack?**

# 50% WHO KNOW A PHISHING VICTIM SAY THEY'RE **CO-WORKERS**

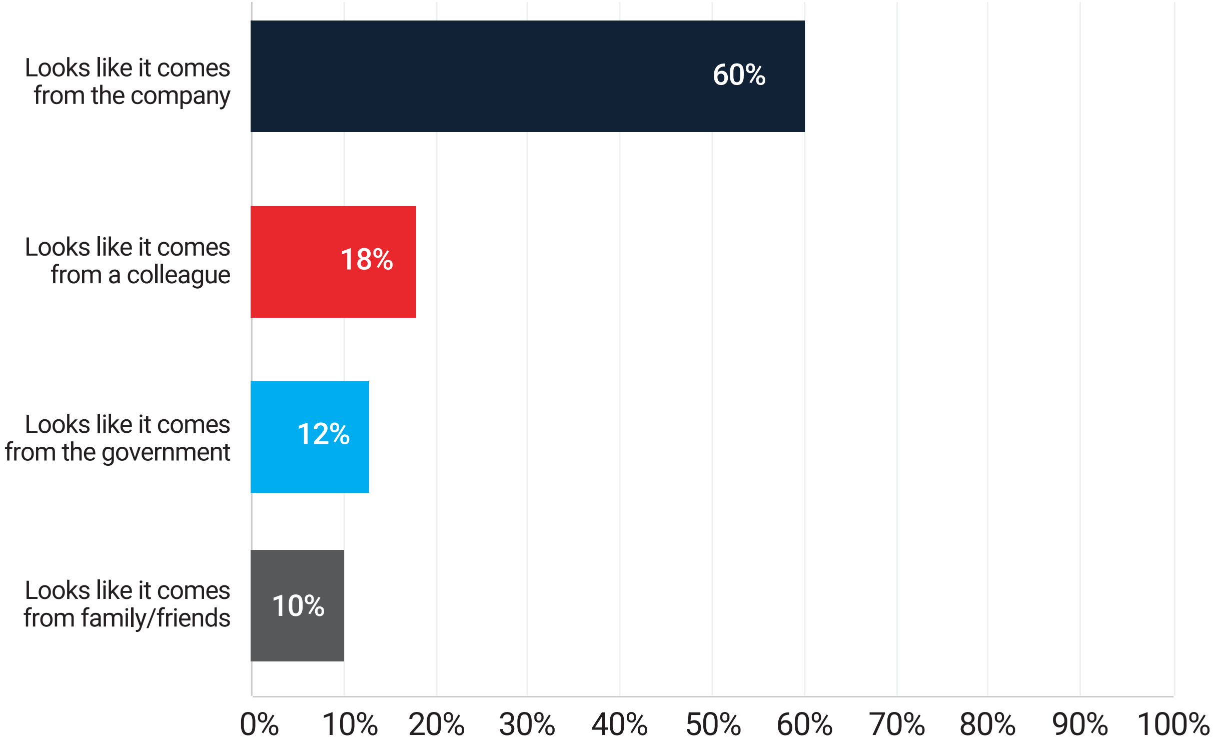
To phishing attackers, employees are irresistible targets. It's easy to trick busy, distracted human beings into activating malware or wiring corporate funds. Yet when phishing emails slip by tech defences like email gateways—and it happens all the time, even with "next-gen email security platforms"—users are your last layer of defence. That's why thousands of organisations train with phishing simulations. Everyone's a target. Not all become a victim.



**Who do you know that has fallen victim to a phishing attack?**

# 60% WORRY THE MOST ABOUT EMAILS **SPOOFING** COMPANY MESSAGES.

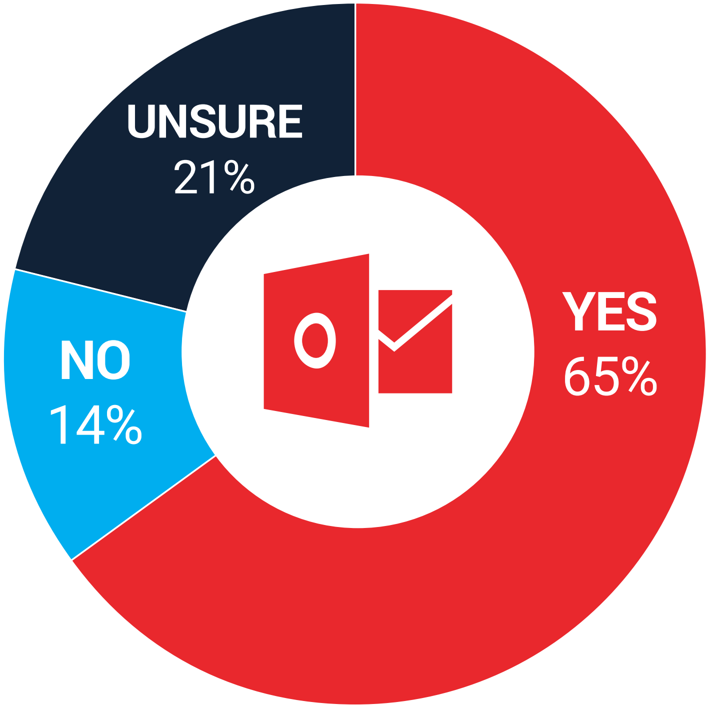
This tracks with other Cofense research. Our most recent Phishing Resiliency and Defence Report shows that bogus office communications make for potent phishes. Examples of subject lines from seemingly official emails: "Salary Adjustment" and "Package Delivery." Fun-looking emails work their own kind of scams: "Holiday Party Pics" or "Free Coffee." FYI, when hackers use already compromised email accounts, it's harder for perimeter tech to stop them.



**Which type of phishing attempts are you most concerned will trick employees?**

# 65% THINK **MICROSOFT OFFICE** LEAVES USERS OPEN TO ATTACKS.

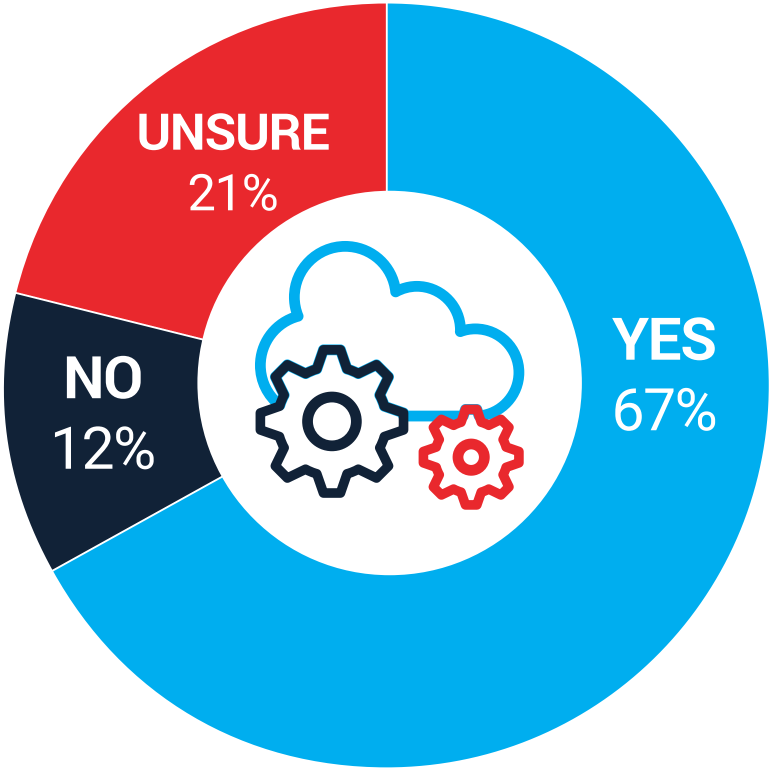
Microsoft Office is ubiquitous, which makes it ripe for phishing. Attackers are exploiting both popular Office features and core Windows functionality, the latter designed to improve interoperability but also, wouldn't you know, expanding the attack vector. Because so many people rely upon and trust Office attachments, attackers use those attachments, mostly Word and Excel, to deliver malware. Last year, Cofense analysed nearly 600 Office Macro campaigns alone, plus almost 100 abusing Office Object Linking and Embedding (OLE). To learn MORE, see the Cofense Malware Review 2018.



**Do you believe Microsoft Office leaves office workers vulnerable to phishing attacks?**

# AND EVEN MORE, 67%, BELIEVE **CLOUD SERVICES** DO THE SAME.

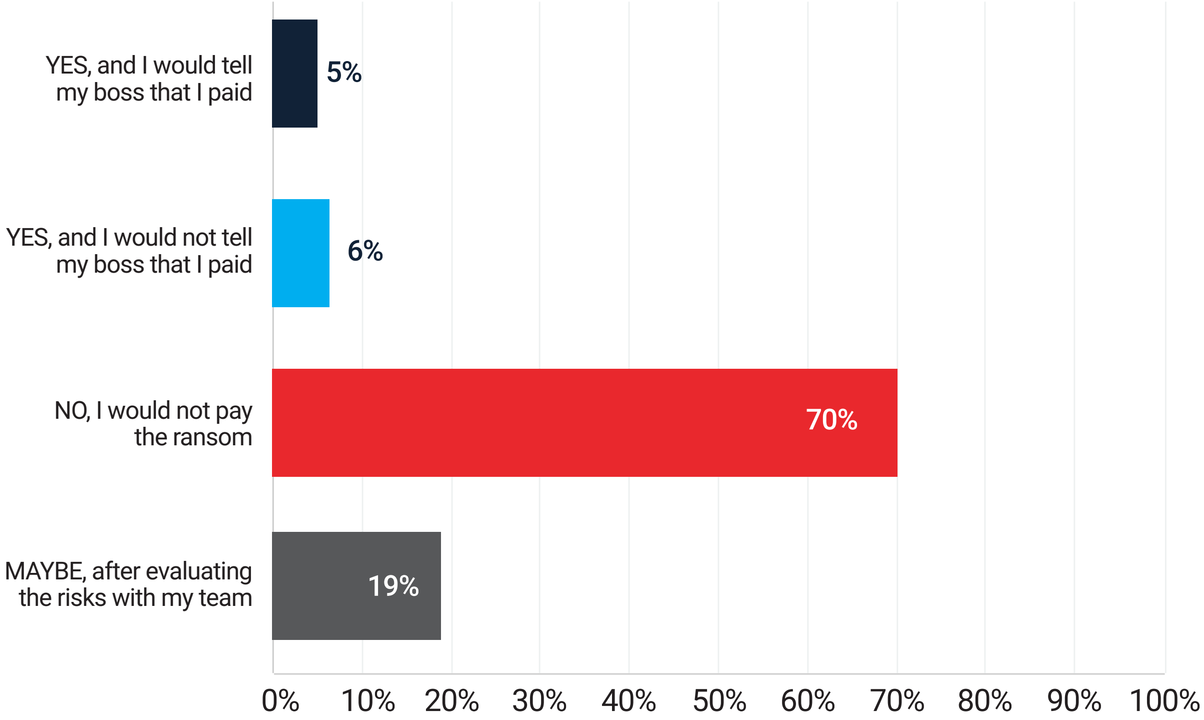
Sixty-seven percent think the Cloud is fueling phishing. With nearly everyone using the Cloud to store and provide critical data, attackers are phishing for Cloud credentials via document-sharing services or single sign-on suites. Some attacks deliver malicious plugins and Cloud applications to connect to legitimate Cloud accounts, similar to 2017's Google Docs™ worm. While tactics will always vary, look for this trend to continue.



**Do you believe Cloud services leave office workers vulnerable to phishing attacks?**

# WHILE MOST WOULD REFUSE, OVER 30% WOULD **MAKE RANSOMWARE PAYMENTS** OR AT LEAST CONSIDER IT.

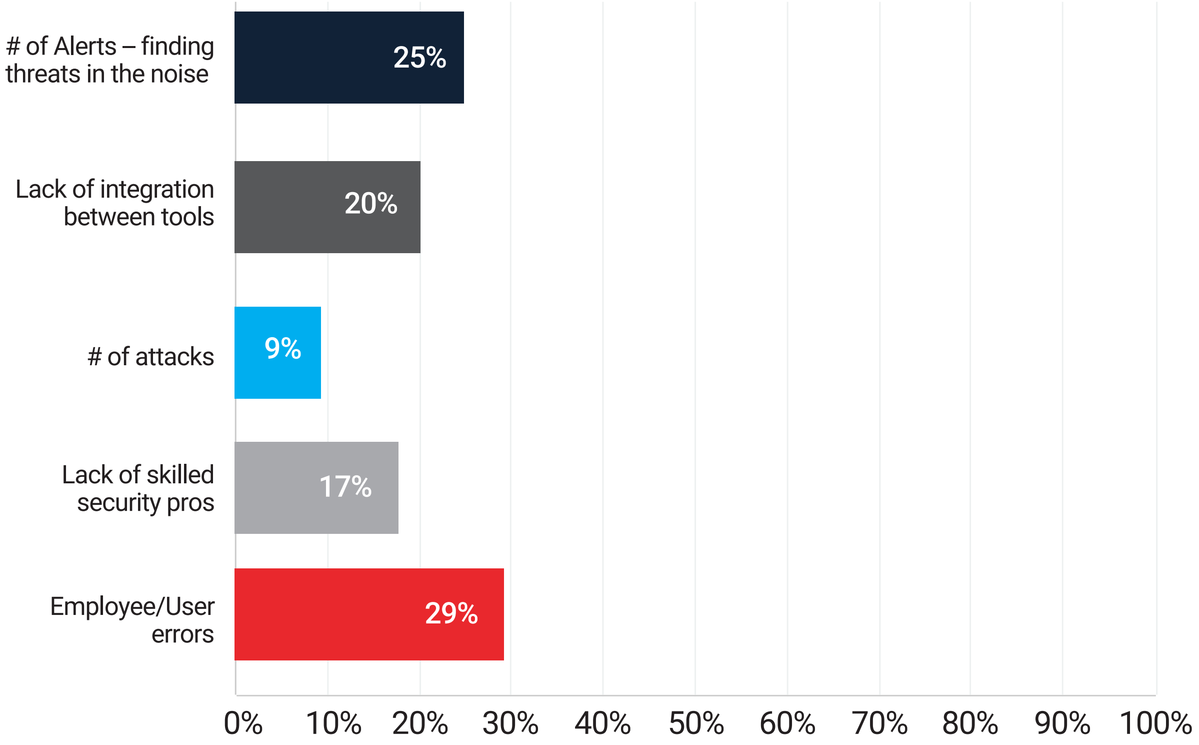
An effective phishing defence lowers the odds of facing the choice: pay criminals to unlock your systems or lose money as business grinds to a halt. Or, if you're a hospital, watch lives hang in the balance as the clock ticks. Presumably, some of the 70% who say they wouldn't play ball back up their data. Learn more about ransomware trends in the Cofense Malware Review 2018.



**Would you pay the ransom if your company was hit by a ransomware attack?**

# 45% HAVE TROUBLE **FINDING REAL THREATS** AND SYNCING RESPONSE.

Employee/user errors is the single biggest barrier to defending against threats. But a combined 45% point to the sheer number of alerts, which make it hard to tell threats from noise, and a lack of integration between security and IT tools. An effective phishing response platform tackles these challenges by automating the analysis of reported emails; clustering emails by phishing campaigns; filtering spam and other noise before it hits the SOC; and helping orchestrate response by identifying all users that received a malicious email.



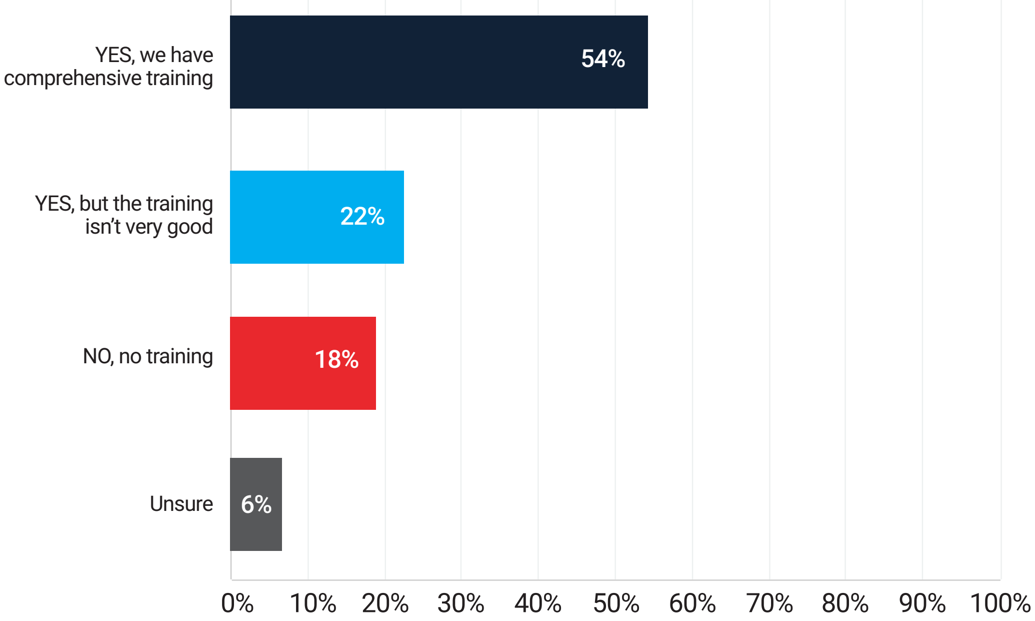
**What is your biggest challenge in identifying and responding to cybersecurity threats?**

# NEARLY 50% DON'T HAVE **EFFECTIVE** PHISHING AWARENESS TRAINING.

Either (a) their companies offer this training to employees and it's woeful or (b) there is no training. When you think about it, phishing awareness training is an important way to deal with some of problems cited earlier:

- The number of co-workers victimised by phishing
- Malicious emails spoofing company messages
- Vulnerabilities left by Microsoft Office and Cloud services
- The decision on whether or not to make a ransomware payment

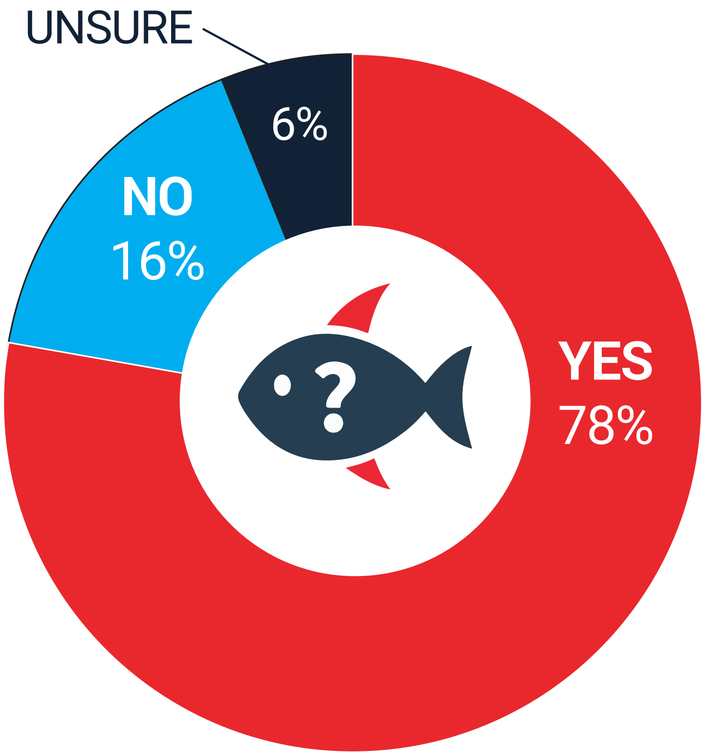
Proper training is that ounce of prevention worth a pound of cure. It's an investment that helps prevent losses potentially in the millions.



**Does your company train employees how to spot a phishing attempt?**

# 78% GIVE USERS A WAY TO **REPORT** SUSPICIOUS EMAILS.

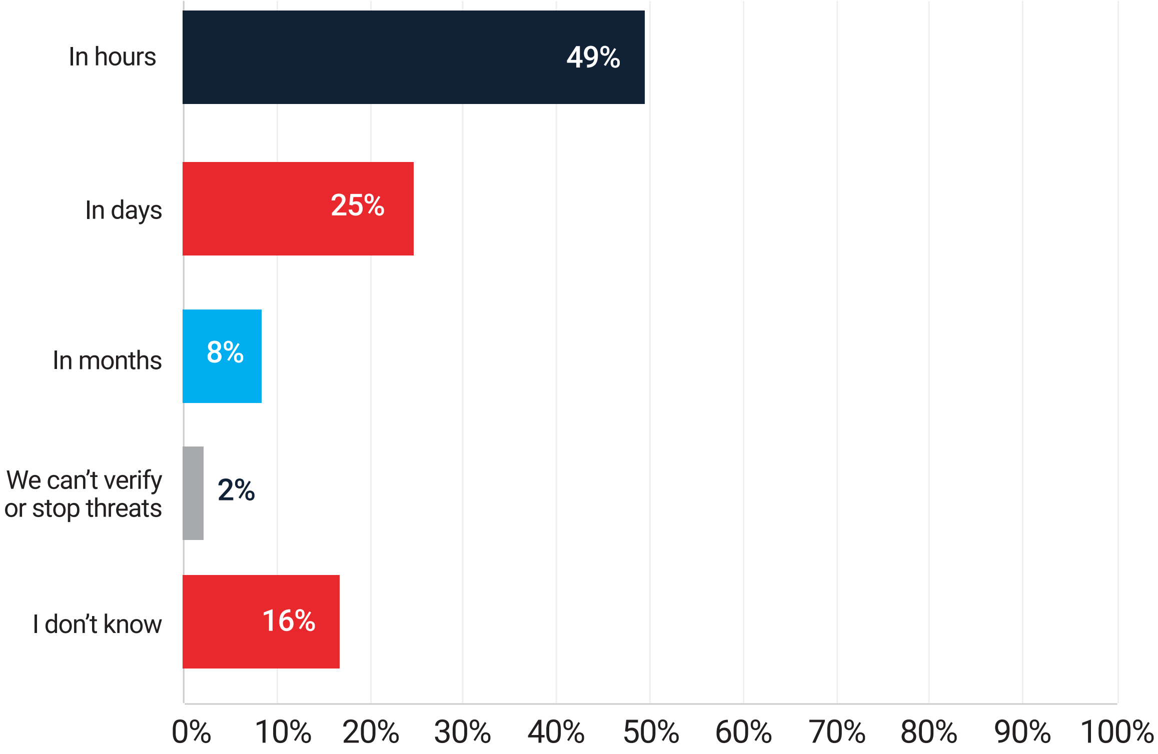
When coupled with effective phishing awareness training, a reporting mechanism—ideally, a button in email toolbars– is a simple but powerful tool. It allows users to apply their training in real situations, transforming them into layers of defence in depth and helping incident responders find and mitigate threats. **Note:** automation to sort through all those reported emails helps your SOC team identify genuine threats amidst all the noise.



**Does your company have a way for employees to report suspicious emails?**

# OVER 50% TAKE **DAYS OR MONTHS** TO RESPOND TO VERIFIED THREATS.

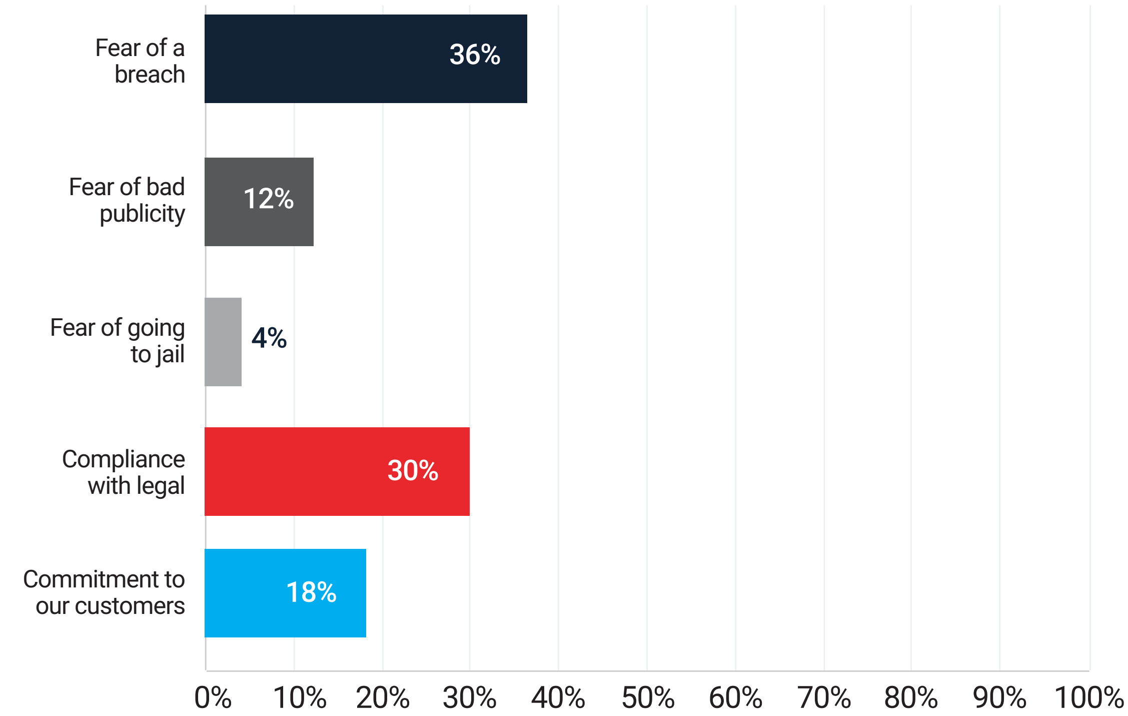
To verify a threat, you must first identify it. If a phishing email makes it past your perimeter technology, and isn't recognised and reported by well-trained humans, then your SOC team, which like most is probably understaffed and over-stressed, is somehow supposed to catch the threat in their spare time. Again, the right phishing response platform, fueled by automation and human intel, cuts through noise to verify threats, so security teams can act faster.



**How quickly can your incident response teams stop verified threats?**

# 52% SAY **FEAR** DRIVES IT SECURITY SPENDING.

Fear of breaches, bad publicity, and even jail time drive investments, along with compliance requirements and customer commitment. According to FireEye®, the average dwell time, the period from compromise to internal detection, is 101 days, the kind of lag that sends chills throughout the SOC. A lot can go wrong in 3 or 4 months, from stolen customer records to loss of intellectual property, seeding class action suits and migraine-inducing headlines.



**What drives IT security spending at your organisation?**

# LET'S SUMMARISE.

Nearly **8 in 10** security professionals know someone hit by phishing, often a co-worker. Professionals are particularly concerned about emails that spoof company messages. Yet roughly half their companies don't offer adequate phishing awareness training and about the same percentage take days or months, not minutes, to detect and respond to threats. When making security investments, many companies are driven by fear. Little wonder.

# ABOUT COFENSE.

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defence solutions world-wide. Cofense delivers a collaborative approach to cybersecurity by enabling organisation-wide engagement to active email threats. Our collective defence suite combines timely attack intelligence sourced from employees with best-in-class incident response technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organisations in defence, energy, financial services, healthcare and manufacturing sectors that understand how changing user behaviour will improve security, aid incident response and reduce the risk of compromise.

# COFENSE SOLUTIONS.

## MOBILISE

- **Cofense PhishMe™** is the leading phishing simulation and awareness service. Over 27 million employees in 160 countries, including users at half the Fortune 500, rely on Cofense training and education to recognise phishing.
- **Cofense Reporter™** makes it easy for employees to report suspicious emails. By clicking the Reporter button on their email toolbar, users can send emails for inspection and possible mitigation.

## MITIGATE

- **Cofense Triage™** analyses and prioritises reported emails, identifying real threats among high volumes of false alarms. Incident response teams depend on Triage to accelerate threat detection, mitigation, and resolution.
- **Cofense Intelligence™** analyses millions of messages daily to identify new and emerging phishing and malware threats. The information comes in context—not simply revealing that something is bad but explaining how and why.

# CITATIONS.

1. The Anti-Phishing Work Group, "Phishing Activity Trends Report," 2016.
2. Cloudmark, "Spear Phishing: The Secret Weapon Behind the Worst Cyber Attacks," 2016.
3. FBI, "Business E-Mail Compromise/E-Mail Account Compromise the 5 Billion Dollar Scam," 2017.
4. Bitglass, "Cloud Adoption Report," 2016.
5. FireEye, M-Trends Report, 2018.