AUSTRALIA PHISHING RESPONSE TRENDS

Losing the War

PHISHME
Human Phishing Defence

OVERVIEW

Organisations in Australia and around the world are moving aggressively to fight phishing attacks. With the number of global 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 attackers.

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 Australian 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.

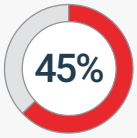
Australia Data Breaches: Only Getting Worse

According to the Ponemon Institute, malicious or criminal attacks account for 48% of data breaches in Australia, with the average number of breached records at over 18,000[2]. IBM reports that the cost of data breaches to Australian companies is $2.51 million.[3]

The Australian government now mandates that organisations report data breaches. If a business spots data activity that a reasonable person feels would cause "serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm," they are obliged to report it to Australia's Privacy Commissioner within 30 days[4]. **Notable findings include:**

89% of surveyed IT executives have dealt with a security incident originating with a deceptive email.

Over 50% say their biggest challenge is poorly integrated security solutions.



45% 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, almost nine out of 10 Australian organisations surveyed have experienced a phishing-related incident and almost all still worry about email-related threats. With nearly half of the organisations believing they have insufficient controls in place, it's obvious there's much work to be done in implementing solutions. 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 Q1 2017, research consultant Censuswide surveyed select Australian IT executives on phishing response strategies. One 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 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.

89% have dealt with a security incident originating with a deceptive email, with nearly 2/3 experiencing an incident more than once.

Even with global spending for information security products at an estimated $81.6 billion in 2016[5], it's clear that no matter how good your perimeter defences are malicious emails will get through. Our phishing response survey shows that over 60% of companies have faced an email-related security incident more than once, with a quarter having handled single incidents.

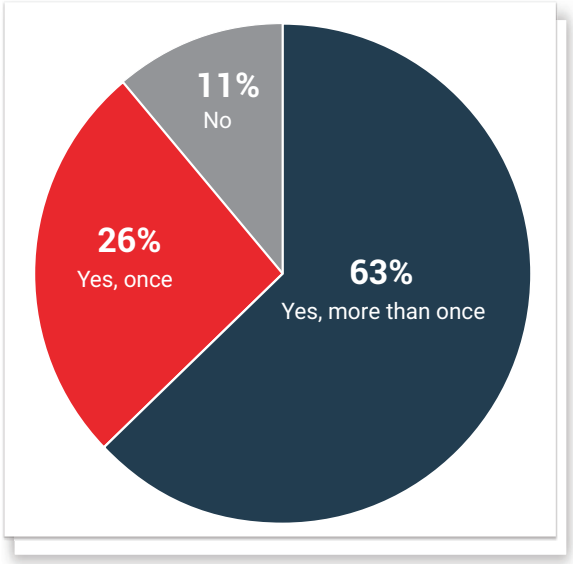


Figure 1: Has your organisation ever experienced a security incident that originated with a deceptive email?

One-third 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,[6] it makes sense that phishing is the top attack vector in data breaches.[7] 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.

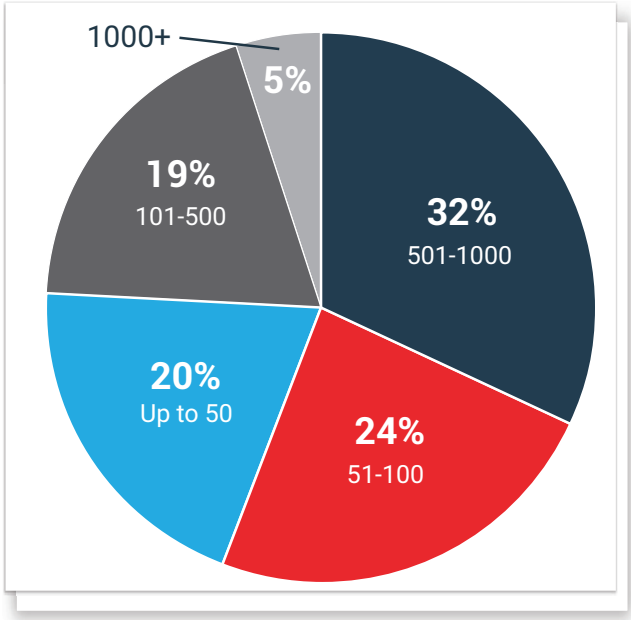


Figure 2: How many suspicious emails are reported in your organisation each week?

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[8] – giving phishers ample time to wreak their havoc.

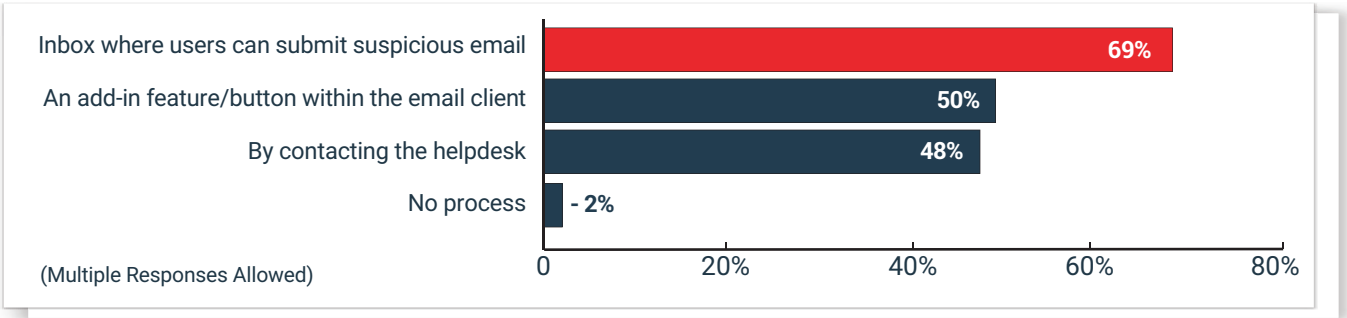


Figure 3: How do users report suspicious emails in your organisation?

Nearly all 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 two-thirds utilising anti-malware solutions and roughly the same percentage 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.

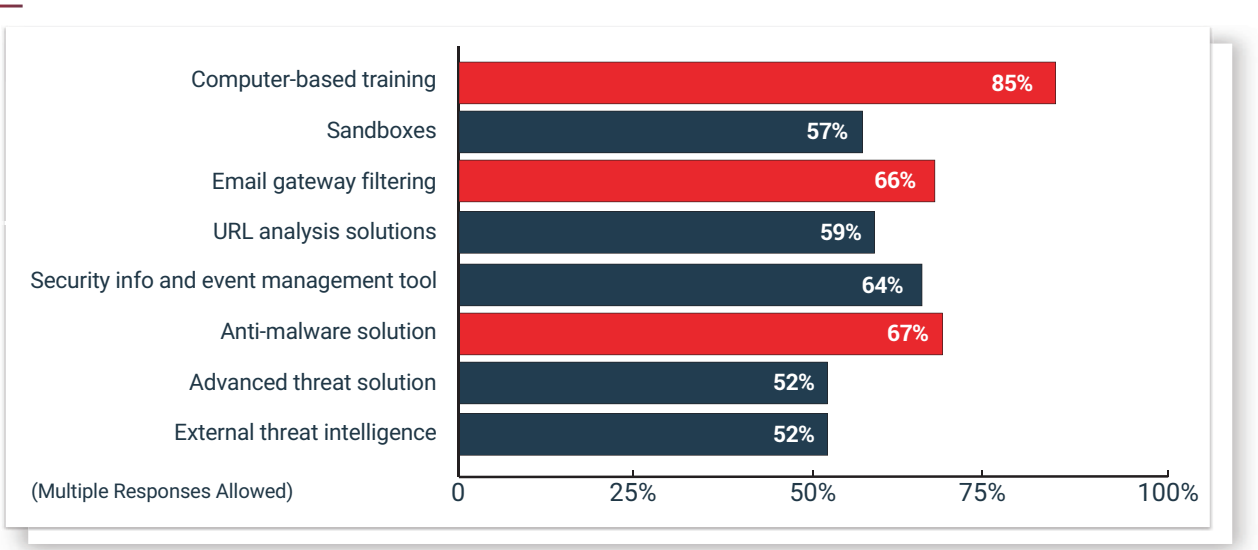


Figure 4: What type(s) of security solutions does your organisation use or plan to use?

Email-related threats are the biggest security worries.

When the Australian Red Cross Blood Service suffered the largest data breach in the nation's history—about 1.3 million records relating to over half a million blood donors—cyber attackers moved in fast.

Scammers used compromised personal information to target donors, sending them text messages containing phishing links. The texts told victims they had an anomaly in their blood donation and directed them to click to learn more.[9]

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.

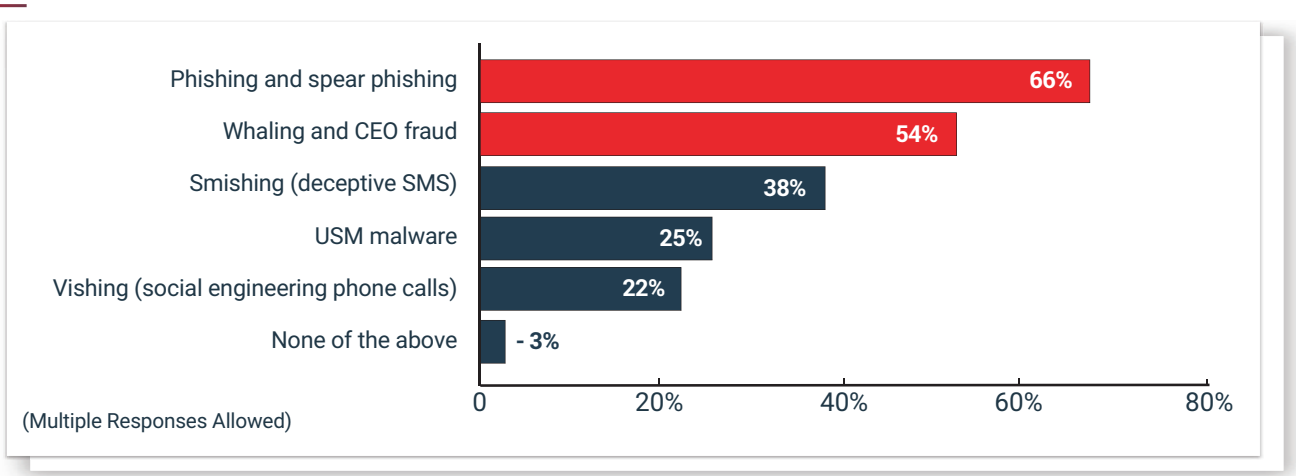


Figure 5: Which of the following security threats concern you most?

Technology alone won't solve the problem.

More than half of respondents cite systems integration as their top anti-phishing challenge. 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.

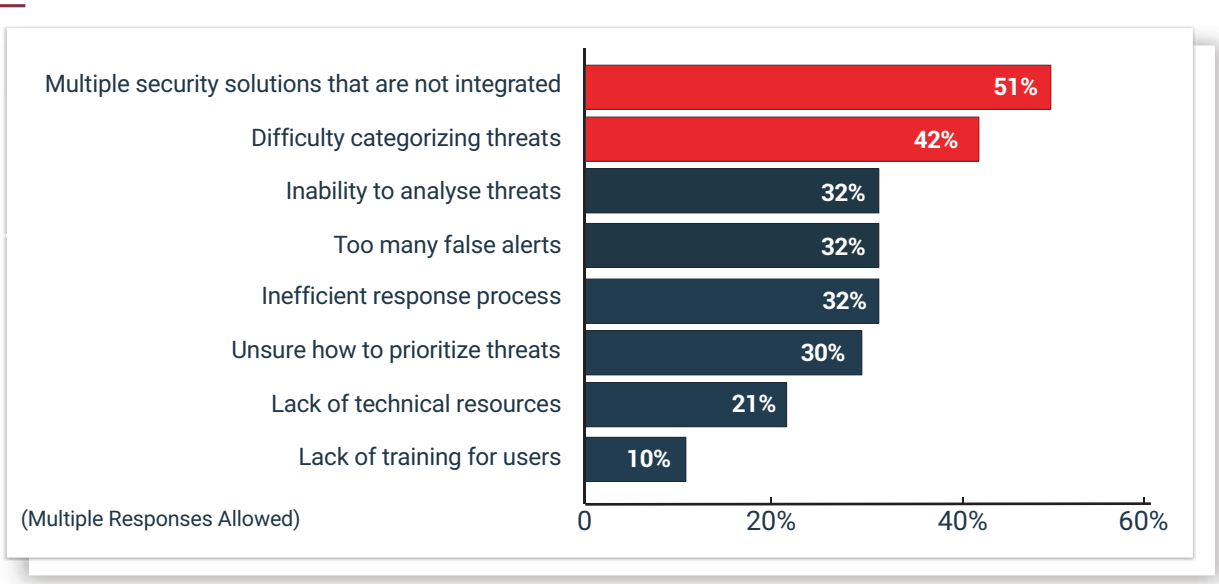


Figure 6: What challenges do you have related to managing phishing attempts?

45% say their phishing response ranges from ineffective to mediocre.

In other words, according to our phishing response data, close to one 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, organisations can sleep better. At PhishMe, we've seen organisational susceptibility to phishing emails drop 20% in just a few weeks, after only one failed simulated attack, and better engagement among all employees to help fight phishing.

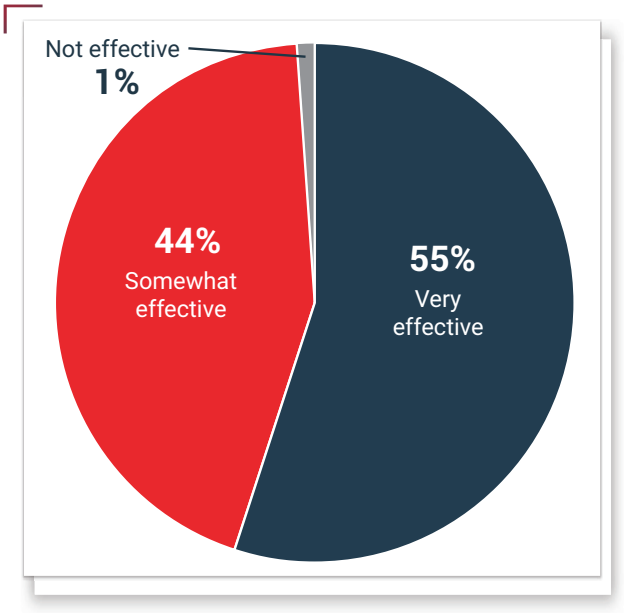
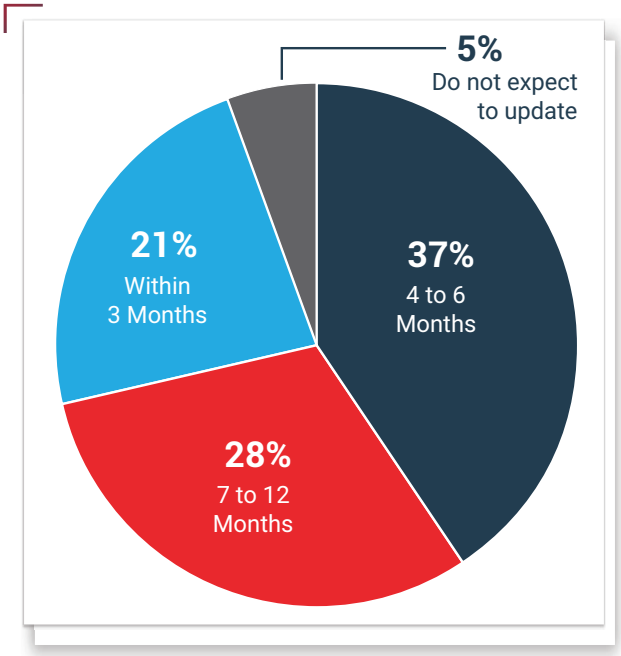


Figure 7: How effective do you think your current phishing response process is?

95% plan to upgrade their phishing prevention and response over the next year.

In Q4 2016 alone there were over 1.2 million phishing attacks[10] around the world. 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. More than half of respondents see automation as the best way to eliminate the manual tasks spread across already thin resources.

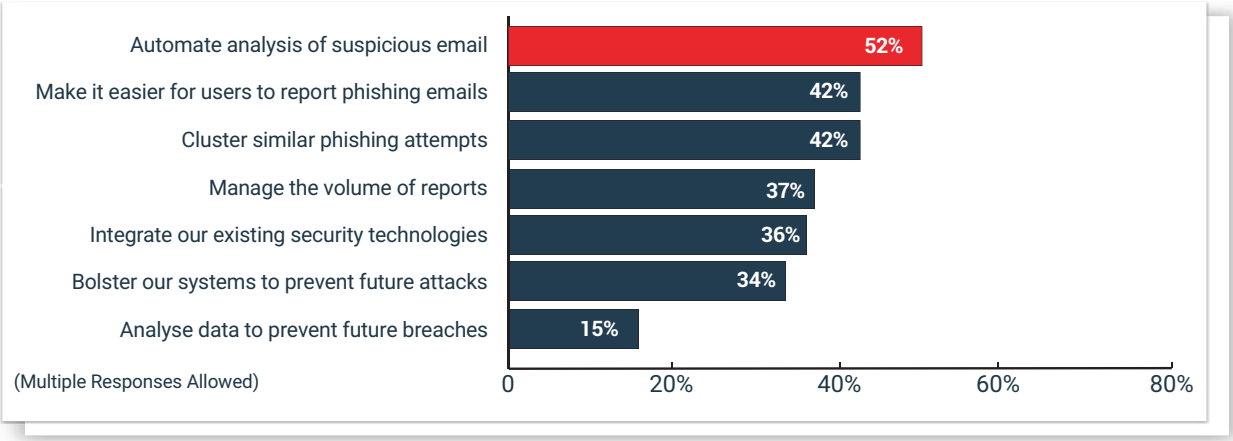


Figure 9: What do you wish you could do better regarding phishing attempts?

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 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 takes only one person to report an attack, so the incident response team can substantially reduce the impact of phishing.

CASE STUDY: Multinational Manufacturer Fights Phishing with PhishMe

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

The company's ability to catch phishing emails has vastly improved since implementing PhishMe Simulator and PhishMe Reporter. According to the client, PhishMe'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 PhishMe is easier. Based on that success, and the technology's tangible results, the Information Security Manager says he'd have no qualms about recommending PhishMe to his peers. When anyone asks him how to deal with phishing, his answer is simple: "Buy PhishMe.[11]

| Read More >>

How Australia's Phishing Response Compares to the US's and UK's

PhishMe has recently produced reports on phishing response trends in the US and UK. Here's how key results in Australia stack up:

Roughly the same number of Australian companies say they're unprepared for phishing.

Australia: 45% US: 43% UK: 48%

Yet more in Australia **have dealt with security incidents sparked by deceptive emails.**

Australia: 89% US: 66% UK: 76%

Like US and UK counterparts, most Australia **companies delay response with manual phishing reporting or no reporting at all.**

Australia: 69% US: 75% UK: 60%

Most Australia**companies plan to upgrade their phishing defence within the next year.**

Australia: 95% US: 80% UK: 96%

In Australia**, automated email analysis is the most wished-for anti-phishing solution.**

Australia: 52% US: 33% UK: 57%

ABOUT PHISHME

PhishMe is the leading provider of human-focused phishing defense solutions for organisations concerned about their susceptibility to today's top attack vector — spear phishing. PhishMe's intelligence-driven platform turns employees into an active line of defence by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organisation's security decision making process. PhishMe's customers include the defence industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behaviour will improve security, aid incident response, and reduce the risk of compromise. Learn more about PhishMe solutions at phishme.com

---

CITATIONS

1. Anti-Phishing Working Group (APWG), "Phishing Activities Trends Report," 2017.
2. The Ponemon Institute, "Cost of Data Breach Study," 2017.
3. IBM, "2017 Cost of Data Breach Study: Australia," 2017.
4. The Register, "Australia finally passes mandatory data breach reporting legislation," 2017.
5. Information Week, "Global IT Security Spending Will Top $81 Billion in 2016," 2016.
6. The Radicati Group, Inc., "Email Statistics Report, 2015-2019," 2015.
7. Verizon, "2017 Data Breach Investigations Report 10th edition," 2017.
8. Mandiant, "M-Trends 2017: A View from the Front Lines," 2017.
9. IT News, "Phishers Go after Red Cross Data Breach Victims,"2016.
10. Cisco Continuum News, 2017.
11. PhishMe, "Multinational Imaging and Optical Manufacturer Reduces Global Phishing Exposure with PhishMe," 2017.