Phishing Insights 2021

While phishing has been around for a quarter of a century, it remains an effective cyberattack technique primarily because it continues to evolve. Adversaries are quick to identify new phishing opportunities – of which the pandemic provided many – and develop new tactics and techniques.

For organizations, phishing is often the first step in a complex, multi-stage attack. Adversaries frequently use phishing to trick users into installing malware or sharing credentials that provide access to their victim's network. A seemingly innocuous email can ultimately lead to ransomware, cryptojacking, or data theft.

This report provides the latest insights into phishing based on an independent survey of 5,400 IT professionals at the IT frontline around the globe, along with a case study of a real-world phishing attack that led to a multi-million-dollar ransomware incident.

According to the Verizon 2021 Data Breach Investigation Report, 36% of confirmed data breaches involve phishing (up from 25% in 2019). Use these survey findings to evaluate your own phishing security posture and identify opportunities to extend your defenses.

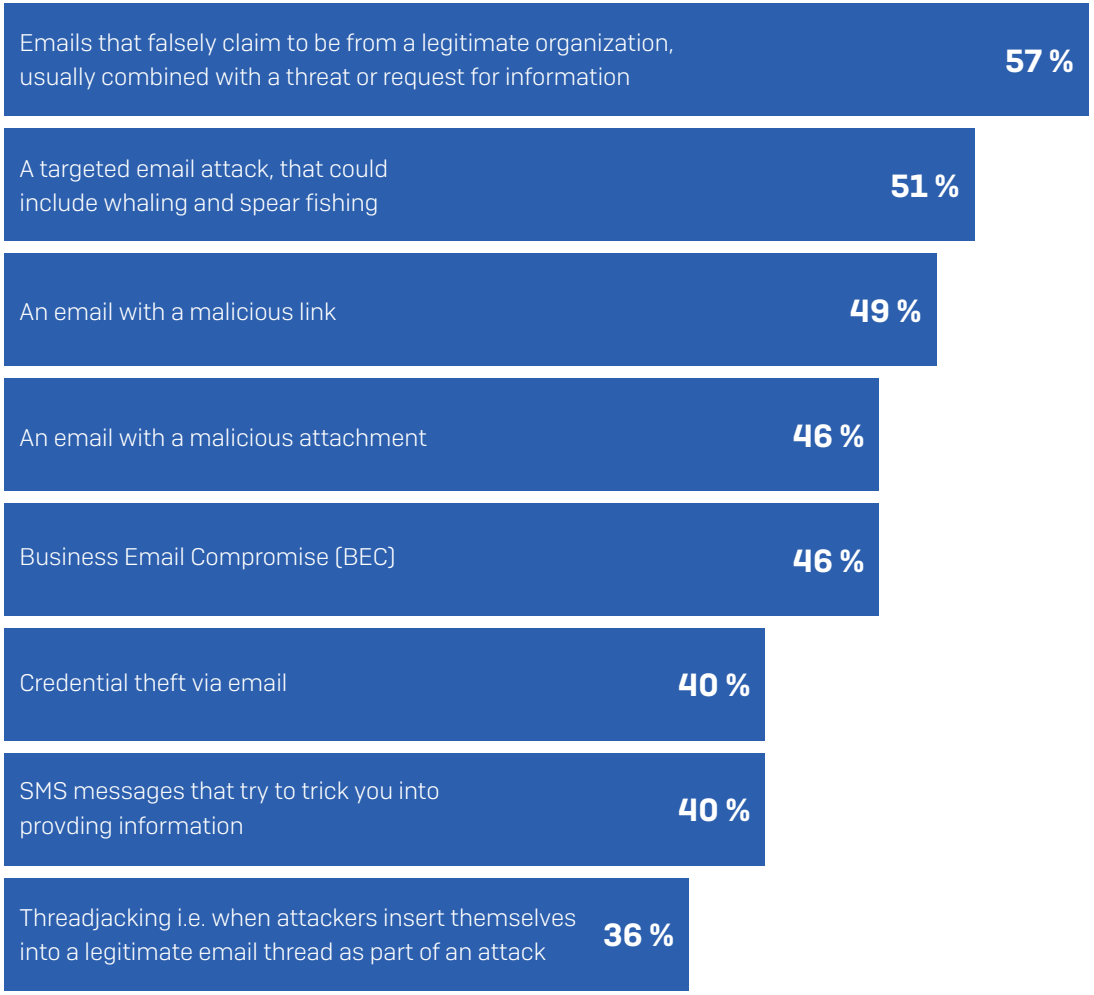
SOPHOS

1. Phishing means different things to different people

What is phishing? Our survey reveals that even among IT professionals there is wide variation in what people consider to be a phishing attack. The most common understanding is *emails that falsely claim to be from a legitimate organization, usually combined with a threat or request for information*. While this was the most popular answer, fewer than six in 10 (57%) respondents selected this option, illustrating the breadth of meanings understood by phishing.

46% of respondents consider Business Email Compromise (BEC) attacks to be phishing, while over a third (36%) understand phishing to include threadjacking i.e. when attackers insert themselves into a legitimate email thread as part of an attack.

Which of the below options do you consider to be a phishing attack?



Which of these options do you consider to be a phishing attack? [5,400] Excluding some answer options

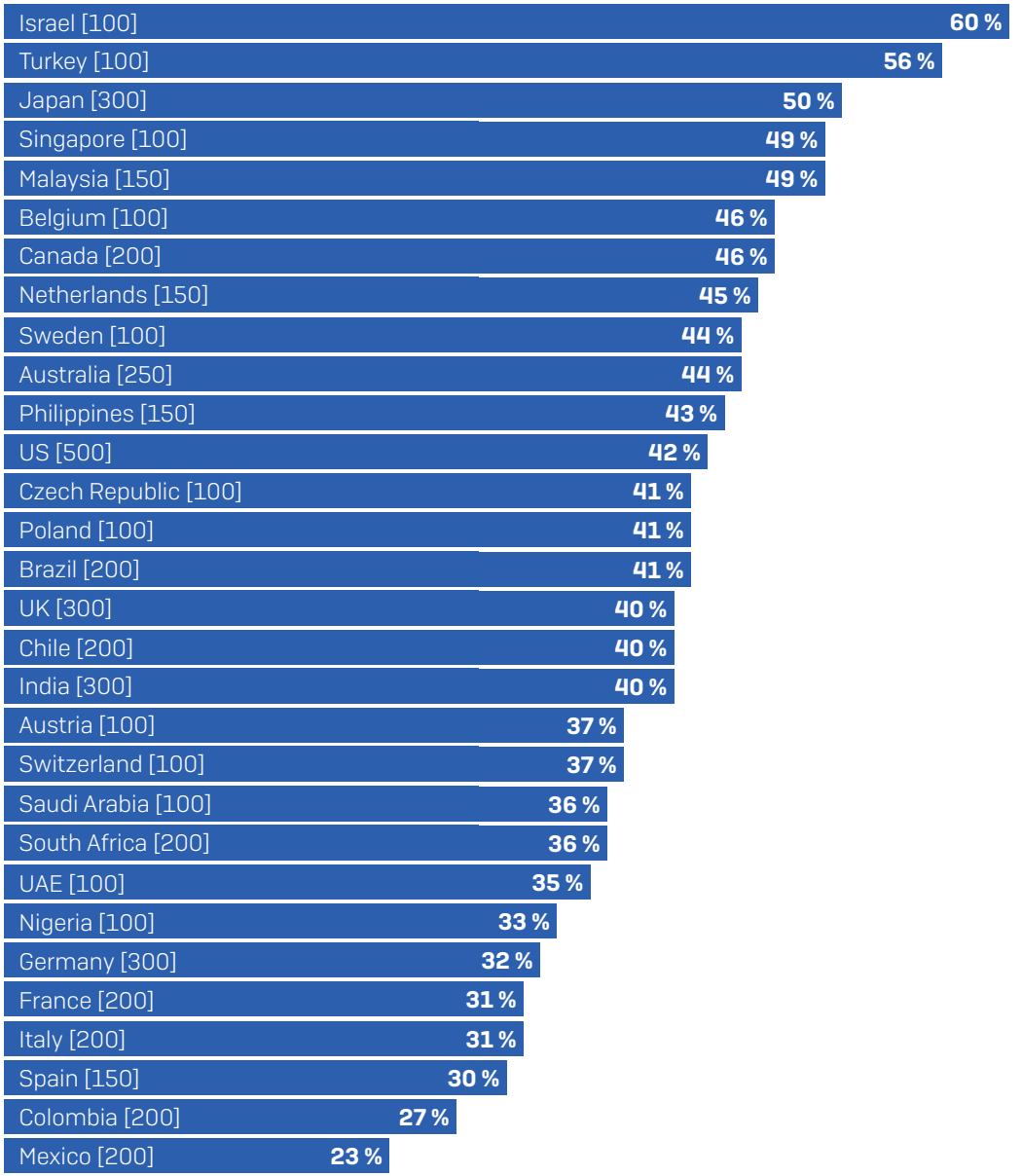
Cultural factors have a major impact on people's understanding of phishing. For example, the proportion of respondents in Israel that considers SMS messages that try to trick you into providing information to be phishing is more than double the percentage in Mexico (60% vs. 23%). While many IT pros call this smishing rather than phishing, false messages claiming to be from brands we trust have the same effect regardless of transmission method.

Considering this extensive variation among IT professionals in how they understand or define phishing attacks, it's reasonable to expect a similar or greater range of interpretations among non-IT employees.

Understanding that phishing means different things to different people is a significant insight for anyone creating or running phishing awareness and education programs. For phishing training to be effective, it is important to ensure a shared baseline definition of phishing so what we learn can be understood in the correct context.

TAKEAWAY: BE MINDFUL THAT PHISHING MEANS DIFFERENT THINGS TO DIFFERENT PEOPLE WHEN PROVIDING EDUCATIONAL RESOURCES AND USER AWARENESS TRAINING. WITHOUT THE CORRECT CONTEXT, THE TRAINING WILL BE LESS EFFECTIVE.

Respondents that consider SMS messages that try to trick you into providing information to be phishing



Which of these options do you consider to be a phishing attack? [base numbers in chart] SMS messages that try to trick you into providing information

2. Phishing has increased considerably since the start of the pandemic

70% of survey respondents reported an increase in phishing attacks on their organization since the start of the pandemic. All sectors were affected, with central government experiencing the highest increase (77%), closely followed by business and professional services (76%) and healthcare (73%).

The small variation between sectors – just 10 percentage points before rounding* – affirms that adversaries are often indiscriminate and will try to reach as many people as they can to increase their likelihood of success.

SophosLabs research showed that adversaries were quick to take advantage of opportunities presented by the pandemic and the resulting blurring of home/work boundaries, including:

- Rapid increase in working from home. It's likely that attackers hoped people would lower their guard while adjusting to working from home and operating in a non-business environment.
- Growth in home deliveries. Phishing messages purporting to be from a home delivery company became commonplace during the first months of the pandemic as people turned to online shopping in large numbers.
- Widespread concern about the pandemic. Adversaries exploited people's anxiety and need for information on COVID-19 with pandemic-themed scams. They anticipated that the high level of concern would make people less likely to check that a message was legitimate before clicking.

Sector	Respondents that experienced an increase in phishing attacks on their organization since the start of the pandemic
Central government and NDPB [117]	77%
Business and professional services [361]	76%
Healthcare [328]	73%
Media, leisure and entertainment [145]	72%
Energy, oil/gas and utilities [197]	72%
Retail [435]	71%
Education [499]	71%
Other [768]	71%
Local government [131]	69%
Distribution and transport [203]	68%
Financial services [550]	68%
Construction and property [232]	68%
IT, technology and telecoms [996]	68%
Manufacturing and production [438]	66%

Have you noticed a change in the number of phishing attacks on your organization since the start of the pandemic? [base numbers in chart] Yes, a large increase, Yes, a small increase

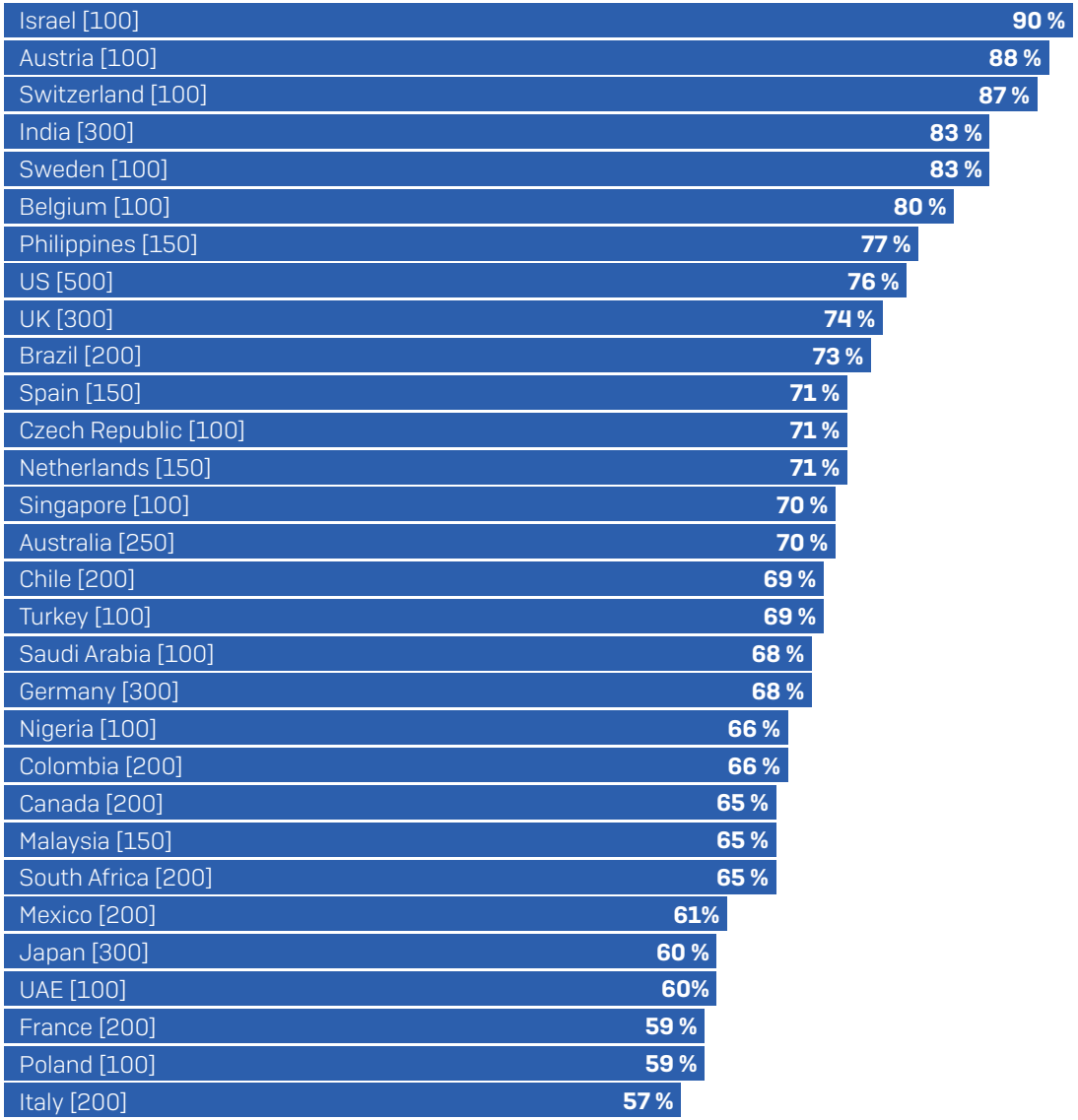
** Before rounding, 76.92% of respondents in central government reported an increase compared to 66.43% in manufacturing, giving actual variance of 10.48%*

While there was little overall variance by sector, the survey did reveal considerable difference in the increase in phishing attacks reported by country since the start of the pandemic. For example, 90% of respondents in Israel reported an increase in phishing compared to 57% in Italy. These results, although influenced by respondents' definition of phishing and their ability to track and measure attacks, offer valuable insight into the real-world experience of IT professionals at the frontline.

Just as there are many different types of phishing email, so there are many different cybercriminals behind them. Skilled adversary groups typically focus their targeted attacks on countries with higher GDP such as Austria, Switzerland, and Sweden to maximize their financial return, likely contributing to the widespread increases in phishing in those countries. At the same time, phishing is also used in mass market 'spray and pray' attacks where adversaries hope that if they try enough people, eventually someone will fall for the scam.

TAKEAWAY: DON'T LET UP IN YOUR ANTI-PHISHING EFFORTS. CYBER CRIMINALS ARE INCREASING THEIR USE OF THIS TECHNIQUE AND NO INDUSTRY OR COUNTRY IS SPARED.

Respondents that have experienced an increase in the number of phishing attacks on their organization since the start of the pandemic



Have you noticed a change in the number of phishing attacks on your organization since the start of the pandemic? [base numbers in chart] Yes, a large increase, Yes, a small increase

3. Most organizations run cybersecurity awareness programs to address phishing

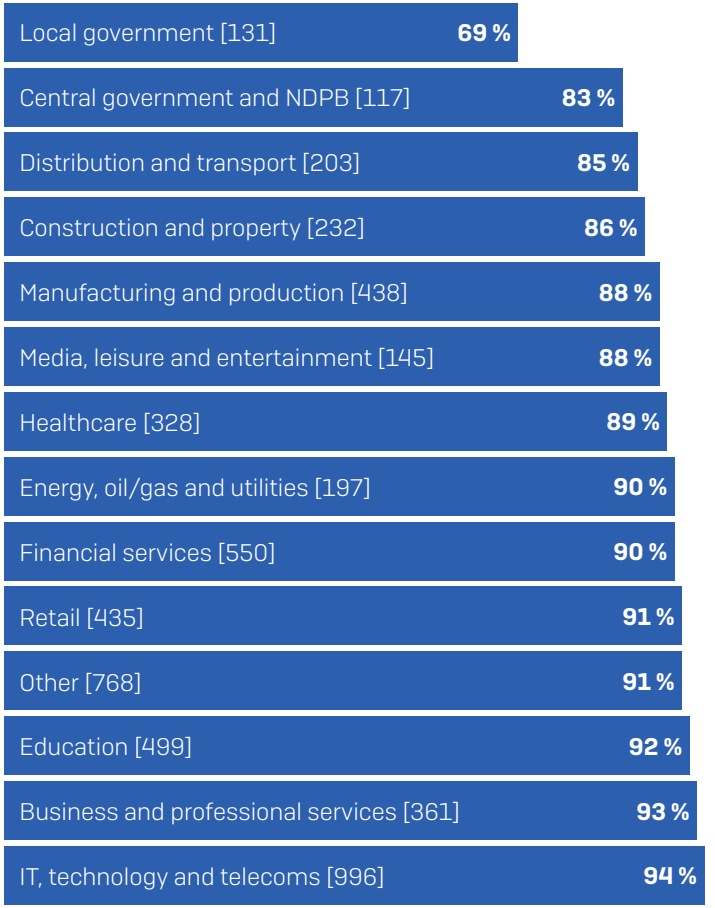
90% of organizations have implemented a cyber awareness program to address phishing, with an additional 6% planning to set one up.

The most popular approach is computer-based training, used by 58% of organizations. Over half (53%) use human-led training, and 43% run phishing simulations. 16% of organizations combine all three techniques – computer-based training, human-led training and phishing simulations – in their awareness programs.

The survey revealed that the government sector lags behind when it comes to running cybersecurity awareness programs to address phishing, with the two bottom spots taken by local government (69%) and central government (83%). This is concerning, as government organizations are frequent targets for high impact cyberattacks: central government is most likely to experience extortion-style ransomware attacks, while local government is most likely to have their data encrypted in a ransomware attack.

TAKEAWAY: IF YOU'RE IN THE 10% THAT DOESN'T YET HAVE A CYBERSECURITY AWARENESS PROGRAM TO ADDRESS PHISHING, PUT ONE IN PLACE WITHOUT DELAY.

Use of cybersecurity awareness programs to address phishing



Does your organization have a cybersecurity awareness program in place to address phishing? [5,400] Yes, we do computer-based training programs; Yes, we do human-led training programs; Yes, we run phishing simulations

90%

have implemented a cyber awareness program to address phishing

58%

run computer-based training programs

53%

run human-led-training programs

43%

run phishing simulations

Does your organization have a cybersecurity awareness program in place to address phishing? [5,400] Yes, we do computer-based training programs; Yes, we do human-led training programs; Yes, we run phishing simulations

4. Phishing awareness programs are well established

Almost two thirds (65%) of phishing awareness programs were implemented between one and three years ago, reflecting organizations' response to the shift in attacker technique in the middle of the last decade. Improvements in cyber defenses against web-based attacks in the mid-2010s forced adversaries to switch to new vectors such as email which, in turn, created a strong need for user education programs.

Given the widespread increase in phishing since the start of the pandemic, it's encouraging that 98% of organizations had their phishing awareness program in place before COVID-19 hit. Thanks to these programs employees will have been well placed to withstand the barrage of phishing emails over the last year.

When did your organization implement the cybersecurity awareness program to address phishing?	
Within the last year	2%
1-2 years ago	30%
2-3 years ago	35%
3-4 years ago	20%
4-5 years ago	12%
More than 5 years ago	0%
Don't know	1%

Respondents whose organization has an awareness program in place to address phishing [4,866]

TAKEAWAY: BE SURE TO REGULARLY REVIEW AND UPDATE YOUR PHISHING AWARENESS MATERIALS AND ACTIVITIES TO ENSURE THAT THEY ARE STILL RELEVANT AND ENGAGING FOR YOUR USERS.

5. Positive tracking measures dominate training effectiveness assessment

Almost all (98%) organizations running a user awareness program to address phishing assess the impact of their efforts. Measuring and tracking results enables organizations to optimize their programs to improve results.

The most common approaches are tracking the number of phishing emails reported to IT (68%) and/or the level of reporting of phishing by users (65%). It's encouraging that these positive measures that reflect good user awareness and behaviors are the most commonplace. Identifying and raising awareness of a phish enables IT teams to proactively prevent others from falling for it.

Half of organizations (50%) track the click rate on phishing emails. While a negative measure (it focuses on falling for the scam), click rate provides IT teams with data to help them target awareness programs where they are most needed, and tailor content to reflect the realities within their organization. The more data points, both positive and negative, that you can track, the better.

98%
assess the impact of their awareness program

68%
Track number of phishing-related tickets raised with IT

65%
Track level of reporting of phishing emails raised by users

50%
Track click rate on phishing emails

What do you track to assess the impact of your awareness program? [4,866 Respondents whose organization has an awareness program in place to address phishing] Number of phishing-related tickets raised with IT; Level of reporting of phishing emails by users; Click rate on phishing emails. We do not assess the impact of our phishing awareness programs. Excludes some answer options

TAKEAWAY: REGULARLY REVIEW YOUR USER EDUCATION PROGRAMS IN LIGHT OF THE RESULTS OF YOUR ASSESSMENTS AND FOCUS ON RECOGNIZING AND CELEBRATING POSITIVE BEHAVIORS.

Case study: How a phishing email led to a multi-million-dollar ransomware attack

The Sophos Rapid Response team was recently called in to assist a company experiencing a major ransomware attack. After the attack had been contained, the Rapid Response team investigated the incident to understand how it started. Here's what they discovered:

Three months before the attack, an employee received a phishing email. The email appeared to come from a colleague in another office – it's likely that the attackers had accessed the co-worker's email account to trick fellow employees into trusting the message.

The message was very short and written in poor English. It asked the employee to click on a link to check a document. The link was in fact a malicious weblink and when the employee clicked on it, they enabled the attackers to get the access credentials for the Domain Admin.

The Rapid Response team believes the phishing email was sent by an Initial Access Broker, a cybercriminal that focuses on securing access to organizations' environments and then selling the access on to other adversaries for use in a range of attacks including ransomware and data theft.

In this case, the victim's IT team stepped in and shut down the phishing attack. That seemed to be the end of it.

Eight weeks later, however, a malicious actor installed and ran two tools, Cobalt Strike and PowerSploit PowerView, on the victim's computer. These are commercial tools used legitimately by penetration testers, and also by cybercriminals for malicious purposes. The attackers probably used PowerView to perform network reconnaissance, while Cobalt Strike provided persistence, enabling them to remain in the network.

For about two weeks after the attackers' exploratory activity everything went quiet. The Rapid Response team believes this was because the Initial Access Broker was looking for a suitable buyer for the access credentials.

Once sold, the new "owners" were quick to take advantage of their purchase. They soon appeared on the network, installed Cobalt Strike on more machines, and began to collect and steal information.

Three months after the original phishing email, the attackers unleashed REvil ransomware at 4 am local time and demanded a ransom of $2.5 million.

Get AI-powered phishing protection with Sophos Email

Advanced machine learning **identifies phishing imposters and BEC attacks**

Real-time scanning for key phishing indicators **blocks social engineering** techniques

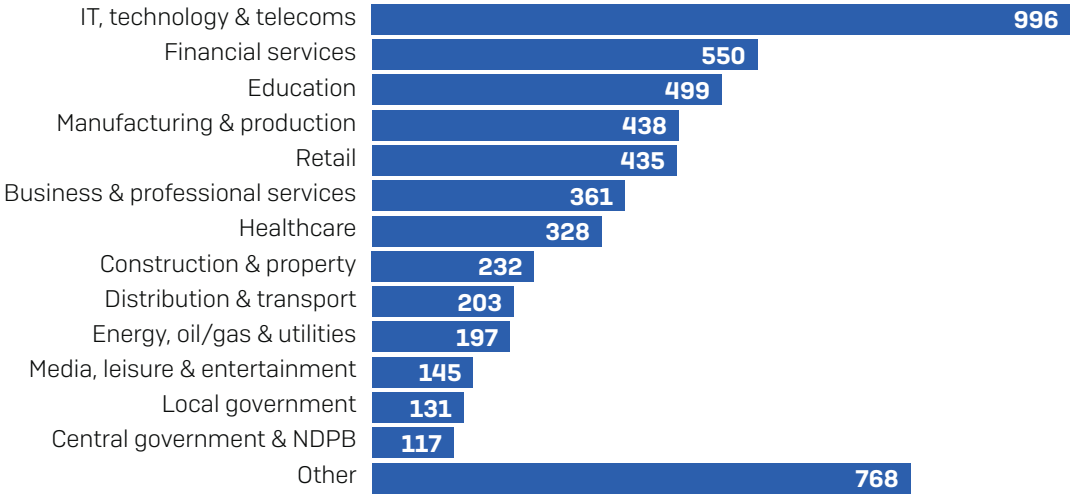
Pre and post delivery protection stops **malicious links and malware**

Learn more and try for free at sophos.com/email

About the survey

Sophos commissioned independent research house Vanson Bourne to survey 5,400 IT decision makers in mid-sized (100-5,000 employee) organizations across 30 countries. The survey was conducted in January and February 2021. Respondents also came from both private and government/public sectors.

Number of respondents per sector



Number of respondents per country

Country	# Respondents	Country	# Respondents	Country	# Respondents
Australia	250	India	300	Saudi Arabia	100
Austria	100	Israel	100	Singapore	150
Belgium	100	Italy	200	South Africa	200
Brazil	200	Japan	300	Spain	150
Canada	200	Malaysia	150	Sweden	100
Chile	200	Mexico	200	Switzerland	100
Colombia	200	Netherlands	150	Turkey	100
Czech Republic	100	Nigeria	100	UAE	100
France	200	Philippines	150	UK	300
Germany	300	Poland	100	US	500

2021-08-13 WPEN (NP)

SOPHOS