Market Pulse

Survey Shows Phishing Attacks Are Up and Few Are Spared

COMPANIES REPORTED AN AVERAGE OF 28 ATTACKS EACH IN PAST 12 MONTHS, DESPITE VALIANT EFFORTS AT EDUCATION AND PROTECTION.

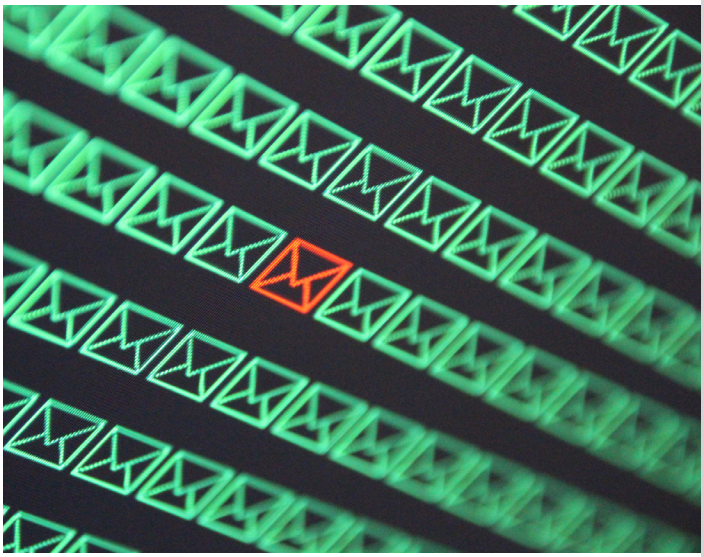
Concern about phishing attacks is high among IT and cybersecurity decision-makers, especially those at larger companies, and cuts across global geographies. It is also warranted, as phishing attacks are on a dramatic rise since the onset of the COVID-19 pandemic.

These are just some of the highlights from a recent IDG Research survey of 300 IT executives, equally divided among North America, Europe, and Asia-Pacific (Japan and Australia). In the survey, 93% of the responding executives reported being concerned about phishing, 61% highly so.

It's little wonder, given that 76% of the respondents said that phishing attacks are up since the pandemic began. On average, respondents estimate they've been targeted 28 times in the past year, and more than half have been hit with a COVID-related phishing attempt.

Those numbers are reflected in the "2021 Webroot BrightCloud Threat Report," which found that phishing attacks increased by 510% from January to February of 2020, in the early months of the pandemic, and then leveled off in the summer. The report found a more modest 34% increase from September to October of 2020.

Similarly, the most frequent security incident suffered by respondents to the "2020 IDG Security Priorities Study," cited by 36%, was "non-malicious user error," which includes users' falling victim to phishing attacks. The same category was the top cause of security incidents across numerous vertical industries — including manufacturing, education, government, and healthcare — and a close second in financial services and retail.



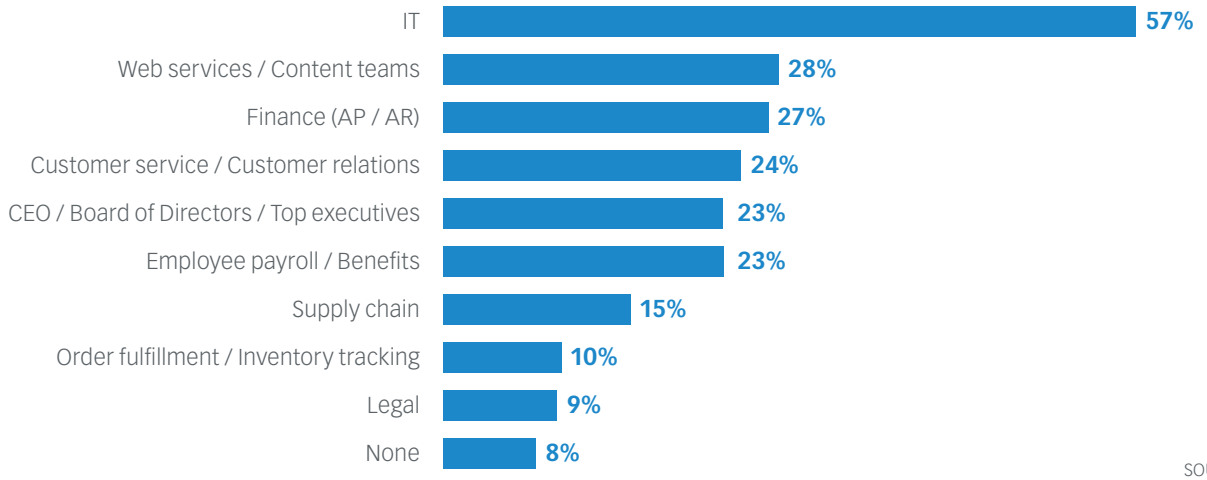
MULTIPLE TYPES OF ATTACKS

Phishing attacks can take numerous forms. The most common form is a standard untargeted mass phishing attack. Nearly four out of five of the respondents to the IDG survey said they either were definitely targeted by such an attack (37%) or suspect they were (42%).

Next most common is a malware attack, where the user gets an email with an attachment — usually a Microsoft Office document — that launches malware if clicked on. Among the respondents, 44% confirmed they were the victim of such an attack and 23% suspect so.

CARBONITE + WEBROOT
— opentext companies —
IDG
SPONSORED CONTENT

FIGURE 1 **Areas of Business Targeted by Phishing Attacks – Past 12 Months**



SOURCE: IDG

Malware attacks joined search engine phishing and clone phishing as the most difficult types of attacks to recognize and avoid, all cited by around one-third of the respondents. Search engine phishing involves fake websites that show up in search engine results, including in paid ads. Often posing as some type of financial institution, the sites then entice users to enter personal information, including banking credentials.

Clone phishing involves a legitimate email conversation you have with someone. That person's account gets hacked, and the attacker attempts to continue the conversation, perhaps sending a malicious attachment or drawing out personal data.

"You feel you trust the person, so you don't worry about normal phishing suspicions," said Tyler Moffitt, senior security analyst with Carbonite + Webroot, which sponsored the IDG study. "That one is definitely very dangerous, because it often works."

The responses about which types of attacks were most difficult to avoid varied by region. For North America, the top response was malware (48%), whereas for Europe it was pharming, also known as domain-name-system (DNS) poisoning, at 35%, and in Asia-Pacific it was man-in-the-middle (32%), in which an eavesdropper monitors a conversation to steal sensitive information. In each case, the top selection was at least 11 points higher than the second most difficult for that region.

WHO'S GETTING ATTACKED

As for what sorts of people phishing attacks target, IT personnel are tops, with 57% of the respondents saying their IT group was targeted in the previous year, more than double any other group *(see Figure 1)*.

That does not surprise Moffitt, because attackers covet domain-level credentials that give them widespread access — and lots of IT personnel have such credentials. "Even if malware targets someone with lower-level access, the attacker will move laterally to eventually find an IT administrator," he says. The attacker may then linger for a week or more to find valuable data to steal or a balance sheet that gives an indication of how much ransom they can charge.

In short, attackers go where the opportunity is, which explains why top executives and finance groups are also common targets. Public-facing customer service employees also offer easy access.

CONSEQUENCES OF PHISHING

No matter the attack vector, phishing attacks have serious consequences, with three-quarters of the respondents reporting that their organization has suffered negative impacts.

More than a third (37%) cited exposure of sensitive data, and 32% said they've suffered lost productivity. One in five had suffered a loss of revenue from phishing, and nearly as many (19%) had had to pay legal or regulatory fines.

You feel you trust the person, so you don't worry about normal phishing suspicions. That one is definitely very dangerous, because it often works.

— Tyler Moffitt, senior security analyst with Carbonite + Webroot

Perhaps worse, more than one-third (37%) reported that their organization had suffered downtime lasting longer than a day as a result of phishing attacks. Larger organizations (500 to 999 employees) were far more likely to report such downtime, at 44%, versus 14% for small companies (25 to 100 employees).

Larger organizations are also more likely to report negative consequences from phishing, especially exposure of sensitive data: nearly half (49%) of all the respondents from large companies, versus 35% for medium (100 to 499 employees) and 16% for small companies.

PROTECTING AGAINST PHISHING

Protecting against phishing attacks is a tall task. Chief among the challenges is "gaps in skills/expertise," cited by 45% of the survey respondents.

That should not be surprising, given the well-documented shortage of cybersecurity professionals we've been experiencing for years. A recent *Washington Post* story, citing data gathered under a U.S. Commerce Department grant, put the number of unfilled cybersecurity jobs at 465,000 in the U.S. alone.

Another issue could be in play. A blogger at *Government Technology* writing about cybersecurity positions posits: "The pandemic may have made things even worse as organizations curtail hiring due to budget constraints or other business difficulties."

Other challenges with respect to battling phishing attacks include inadequate training, cited by 42% of the respondents, along with more frequent personal device use on the part of employees and increased use of insecure Wi-Fi, both cited by 40%.

TRAINING TAKES CENTER STAGE

Although it's clear that fighting phishing is a challenge, the survey also makes clear that respondents don't consider it an insurmountable one.

Endpoint security is a popular phishing defense mechanism, with 61% already using it and 32% planning to. Similar numbers of respondents are either already backing up email and collaboration data so it's recoverable after an attack (65%) or plan to (26%).

But the most popular defense against phishing is mandated security awareness training, adopted by a solid majority of the responding organizations (87%), with another 6% planning to.

The survey delved deep into the issue of security awareness training. It found that investments in training have increased over the past year at 60% of the responding companies and remained the same at about a third (32%). Budget increases were far more likely at larger (70%) and midsize companies (61%) than at smaller ones (33%).

42% of the respondents cited **inadequate training** as a key challenge.

The frequency of security awareness training varies, with 29% mandating annual training, 34% quarterly, and 24% monthly. The vast majority offer training on how to recognize phishing attempts (91%), and nearly three-quarters (74%) offer opportunities to practice recognizing phishing.

Fully one-quarter, however, do not offer phishing simulations that give employees practice. That's an opportunity for improvement, Moffitt says, because simulations are key to the effectiveness of SAT, as evidenced by his company's Threat Report, which shows that companies that do zero simulations per year will see a click rate of around 30%. But running one simulation per year will result in 11% to 12% of users clicking, whereas once a month will get it down to 3%.

"Not many organizations do phishing simulations every

month," he notes, often because they consider it too annoying for employees. A hybrid approach is to conduct simulations every three to six months. Those who pass are good for the quarter or another six months. But those who fail get retested perhaps every month until they prove they can recognize phishing attempts. It's also important to keep simulated attempts current, playing off events such as the pandemic — just as attackers do.

It's also important to measure the effectiveness of your security training, as three-quarters of the respondents do — either annually (23%), quarterly (45%), or monthly (27%). Many respondents aren't kidding themselves about how effective their training is, however. An even split, at 49% each, say their training is "somewhat effective" or "very effective."

A MULTILAYERED APPROACH TO CYBERSECURITY

That kind of skepticism is healthy, because, as Moffitt notes, "You'll never get 100% of employees not clicking."

A multilayered security approach can be effective to protect against what happens when users do fall for a phishing attack, giving you peace of mind that all is not lost due to a single user lapse. Although no layer is 100% effective on its own, taking several layers together gets you very close. If you can get the phishing success rate down to 3%, for example, you've eliminated 97% of attacks right off the bat.

Next you can implement DNS protection to protect against users' clicking on a phishing web page. It works by evaluating each DNS request and, using machine learning, filtering out those that appear malicious. It then blocks the phishing web page and shows the user why it was blocked.

DNS protection is around 90% effective, Moffitt says. On top of phishing simulations, now you've eliminated all but 0.3% of total attacks.

Next up, consider endpoint protection to cover multiple attack vectors. One effective approach is to use a tool that employs machine learning to examine each file as it is written to disc but before it executes, to determine whether it's malicious or not. "That kind of approach is around 99.7% effective and has to work only on the 0.3% of attacks that make it through the other two layers," he notes.

Another layer is traditional antivirus software, which kicks in when files try to execute and stops the process whenever it detects viruses or malware.

A reliable backup solution is another piece of the protection puzzle, with cloud backup being most common. That enables companies to restore any data that may be lost in a successful attack.

It's important to consider file versioning with cloud backup solutions, Moffitt says. Some providers will limit backups to 25 versions of a file or fewer and start throwing out older versions as those limits are reached.

Some ransomware takes that into account. "They encrypt all the files and sync to the cloud over and over to eat up the historical snapshots," he said. A backup solution with no historical limits, then, will provide better protection.

"Whatever files you choose to back up, you'll have unlimited numbers of copies on the back end," he said. "That's important."

CARBONITE + WEBROOT: A POWERFUL COMBO

These days it's not a matter of if you'll be targeted in a phishing attack but when. The pandemic has changed the security dynamic, with more employees working from home, expanding the attack surface for threat actors. Indeed, nearly three-quarters of the respondents to the recent "CSO Pandemic Impact Survey" said the impact of the pandemic will alter the way their business evaluates risk for at least the next five years.

It's clear that steps such as educating users to recognize phishing attacks and conducting periodic simulations are important pieces of the security puzzle. But it's also possible to be prepared for when attacks succeed despite your best training efforts.

A "defense in depth" security posture utilizing DNS and endpoint detection, antivirus software, and a sound backup strategy can give you confidence that you're prepared to withstand even successful phishing attacks.

Together, Carbonite and Webroot provide the full range of cyber resilience solutions you need in order to keep data secure and protected. They also make cyber resilience simple, to ensure uptime for your organization.

To learn more, visit:
www.webroot.com/cyber-resilience
www.carbonite.com/cyber-resilience