CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

COVID-19 CLICKS

How Phishing Capitalized on a Global Crisis

> *People aren't great at handling uncertainty. Even those of us who know we shouldn't click on emails from unknown senders may feel uncertain and click anyway. That's because we've likely all clicked these kinds of emails in the past and gotten a positive reward. The probability of long-term risk vs. short-term reward, coupled with uncertainty, is a recipe for poor decision-making, or, in this case, clicking what you shouldn't.*
>
> **Prashanth Rajivan, Ph.D.**

Introduction

As a cybercriminal tactic, phishing is not new. In fact, one of the very first records of the term appeared in an early internet "cracking" application in January of 1996. Despite its age, phishing continues to be one of the most pervasive cyber threats individuals and businesses face. When technology moves at today's astonishing rates, why is such an old method of internet trickery still so common? The answer is simple: because it's still wildly successful. Perhaps the more important question, then, is: why are people still clicking?

We surveyed 7,000 office workers in the United States, United Kingdom, Australia/New Zealand, Germany, France, Italy and Japan on their understanding of phishing, their email and click habits, and how their online lives have changed since the beginning of the COVID-19 pandemic. First, we compared our new data with answers from our survey last year, featured in the report Hook, Line, and Sinker: Why Phishing Attacks Work. We then worked with Dr. Prashanth Rajivan, assistant professor at the University of Washington, to get his take on why 8 in 10 people worldwide claim to take adequate steps to determine the legitimacy of emails, yet 3 in 10 admit to having fallen for a phishing scam in the last year.

According to Dr. Rajivan, what we need to consider is that human beings aren't necessarily good at dealing with uncertainty, which is part of why cybercriminals capitalize on upheaval (such as a global pandemic) to launch attacks.

In this report, we'll dive into the survey results, present insights and analysis from Dr. Rajivan and our own cybersecurity experts and reveal real-world concerns from workers around the globe. Finally, we'll offer steps to help businesses and individuals stay resilient against phishing attacks.

Global Review

3 in 10 global respondents are certain they've clicked a phishing link in the past year. ***Among Americans, it's 1 in 3****.*

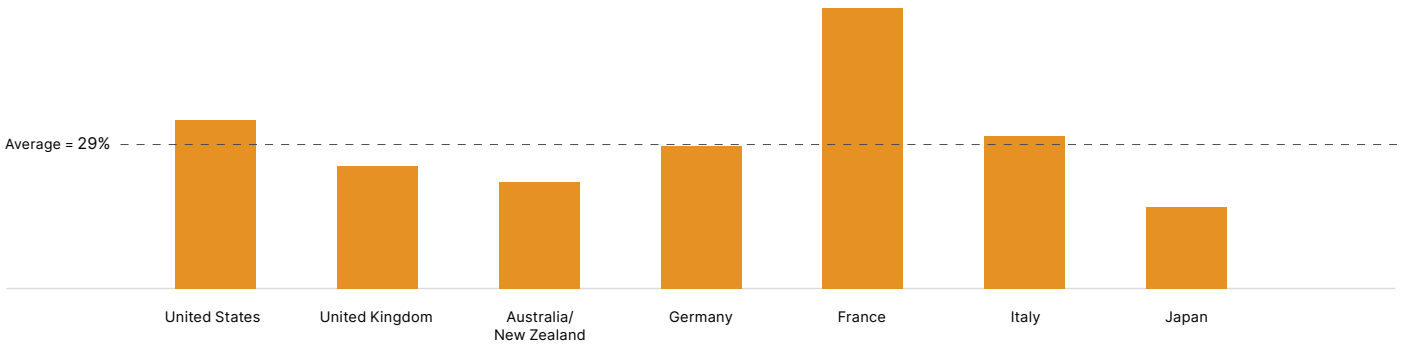
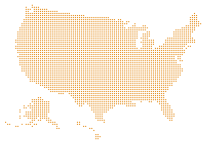


Figure 1: Percentage of people who admit to having fallen victim to a phishing scam on either their personal or work email accounts in the last year



United States

44% of respondents are more concerned about phishing attempts this year, but 1 in 3 admit they have clicked a phishing link in the last year. 8% of those didn't report it.

France

A full 55% of French respondents admitted to clicking a phishing link in past year, even though 8 in 10 say they take steps to determine if messages are malicious when checking email.

United Kingdom

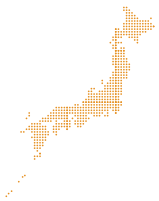
UK respondents have the highest level of confidence in their ability to keep themselves and their data safe from cyberattacks. 1 in 4 have clicked a phishing link in the last year.

Italy

Of Italians who clicked on a phishing link, 23% did not report it. While many recognize the cyber risks COVID-19 has brought, they aren't really worried about them.

Australia/New Zealand

1 in 5 AU/NZ respondents reported having received phishing emails specifically related to COVID-19. But only 1 in 3 respondents are more concerned about phishing now than they were at the beginning of the year.



Japan

Japanese respondents were the least likely to fall for a phishing scam, with only 16% of people having clicked a phishing link in the last year. They were also the least confident about their cyber-safety knowledge.

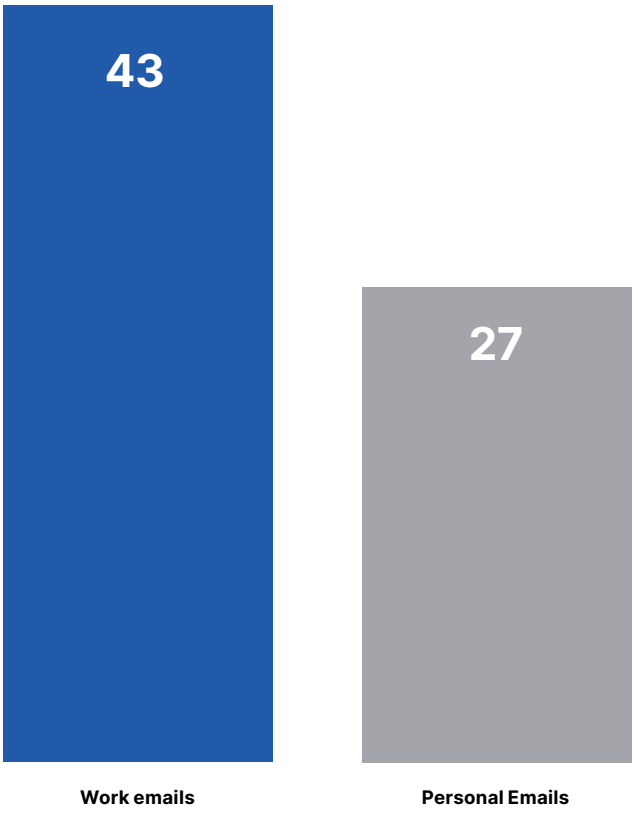
Germany

79% of German respondents say they open emails from unknown senders. Of those, 13% said they do so all the time, while 15% said they do so only rarely.

The State of Risk

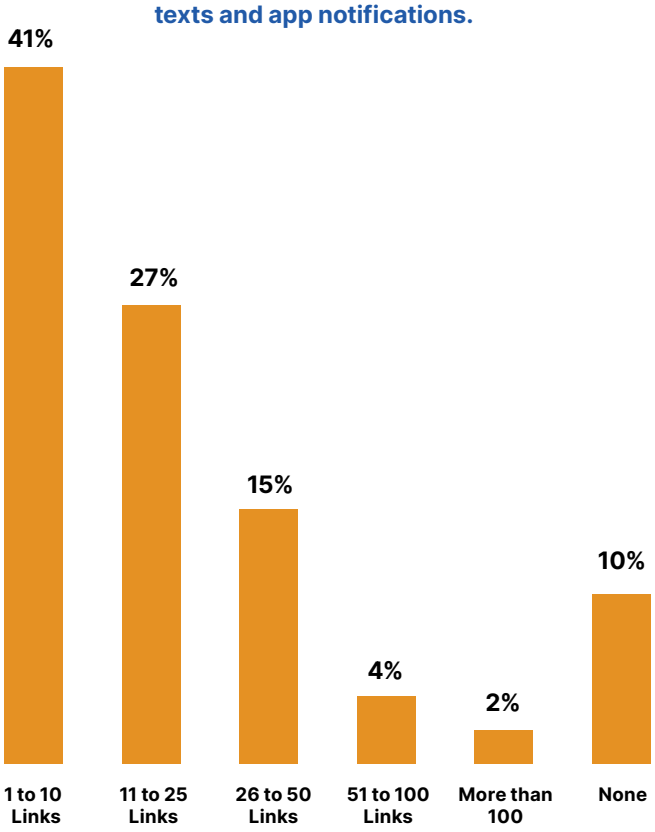
On average, people in our survey said they receive approximately 70 emails per day, which is a 34% increase over last year's responses.[2] Despite this increase, it's interesting that the number remains so low. According to Webroot threat research, phishing continues to grow at astonishing rates, particularly since the start of the COVID-19 pandemic, so one would expect that the number of emails received would have increased more significantly. Overall, however, the majority of respondents in this year's survey (83%) reported they typically click on 50 or fewer work-related or personal life-related links in an average day, which is not a statistically different change compared to last year.[3]

Approximately how many emails do you receive per day on average?



GLOBAL AVERAGE

Approximately how many work-related or personal life-related links, if any, do you click on a typical day? This includes all links in emails, chats, social media, or texts and app notifications.



GLOBAL AVERAGE

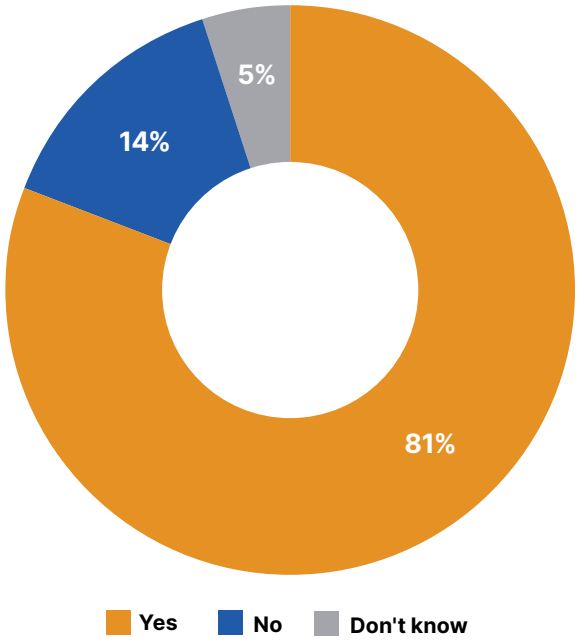
Getting Schooled in Phishing

Per our last global phishing survey, a sense of urgency is one of the primary tactics that ensures the success of a phishing email.[4] In general, 1 in 4 respondents in this year's report said they open new emails within the first few minutes of having received them, and 3 in 4 will have done so within the first hour.

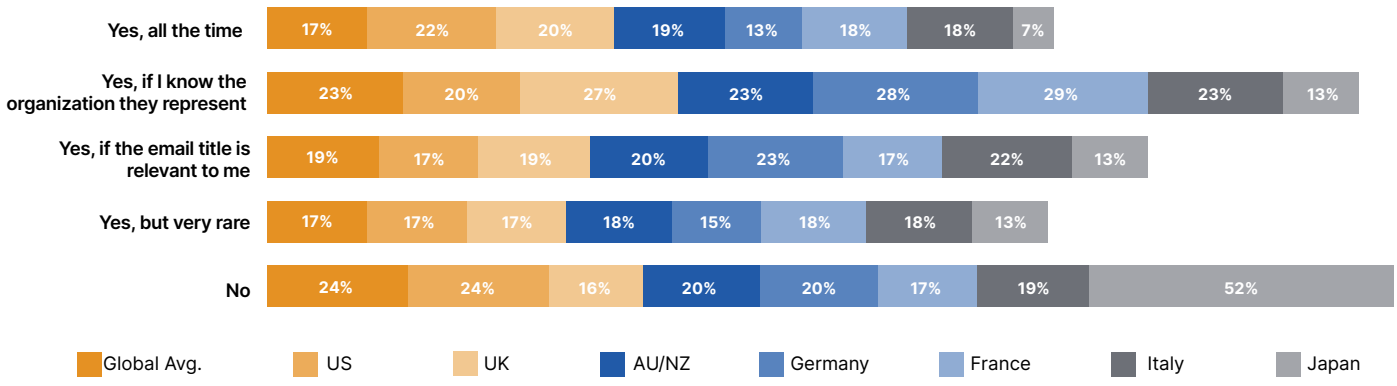
Overall, nearly 3 in 10 people worldwide report having clicked a phishing link or fallen victim to a phishing scam in the last year, which is statistically lower than last year's number (49%)[5], indicating improvement. In fact, 81% of people worldwide say they take steps to determine if an email message is malicious. And yet, an astonishing 76% say they open emails and click links from unknown senders.

When we asked Dr. Rajivan for his take on the discrepancy between respondents' self-reported level of caution and their click habits, he said the distinction is between knowing what you should do and actually doing it.

When checking your email, do you take any steps to determine if an email message could be malicious?



Do you click on an email if you don't know the sender?

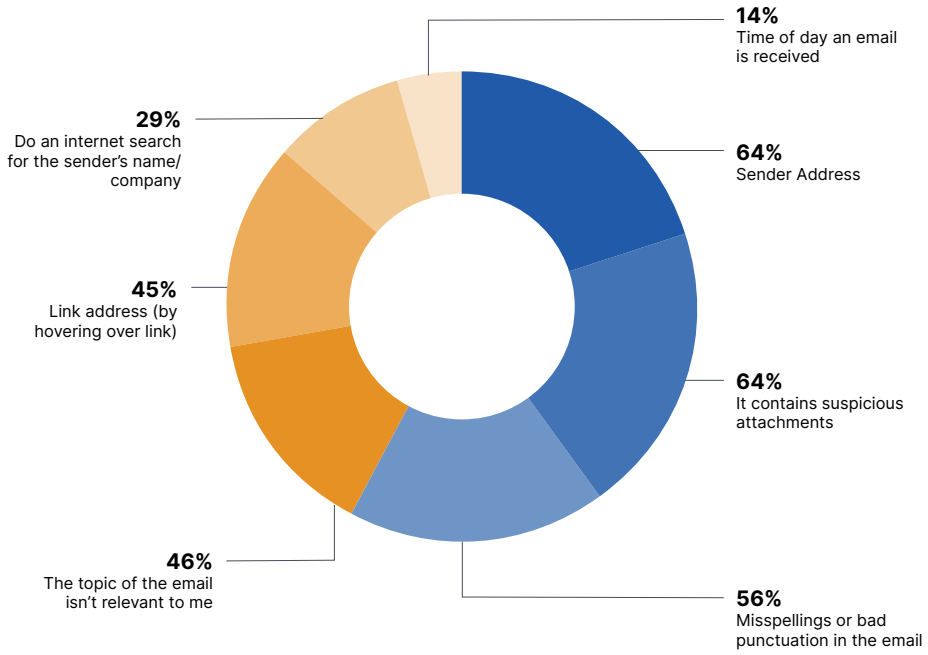


There are huge differences between knowing what to do and actually operationalizing that knowledge in appropriate scenarios. I suspect many people don't really take the actions they reported, at least not on a regular basis, when they receive suspicious emails.

Prashanth Rajivan, Ph.D.

Dr. Rajivan stresses that, while awareness of these steps is certainly important, it's critical to use what he calls a "healthy dose of suspicion" while processing emails. He explains, "Humans, by nature, have a propensity towards truth. We generally assume the communications we receive from other people are honest. By developing a healthy dose of suspicion with regard to emails, it'll help us be more alert, and actually put our phishing knowledge into practice."

What cues do you use/look at to determine if an email is malicious or not? (Check all that apply.)



54% of workers *spend more time working from home now than they did before the pandemic.*

Blurred Lines Increase Uncertainty

Before the COVID-19 global pandemic began, many businesses were already adopting part-time and full-time remote work schedules for employees. But some still shied from these schedules due to perceptions that it would decrease productivity.[6] The latter concern has now largely been dispelled due to companies around the world reporting significant productivity increases since instituting large-scale work from home policies[6], but Dr. Rajivan still cautions that we should be aware of maintaining clear boundaries between our work and personal lives, if we're to maintain the kind of awareness we need to stay safe from opportunistic threats like phishing.

Have you increased or decreased the amount of time you spend working from home as a result of the COVID-19 pandemic?

	Global Avg.	US	UK	AU/NZ	Germany	France	Italy	Japan
Increased	54%	59%	56%	54%	49%	58%	54%	50%
About the same	41%	34%	38%	41%	45%	37%	40%	48%
Decreased	5%	7%	6%	5%	6%	5%	6%	1%

In many cases, working in home environments can cause potentially problematic blurring of boundaries between work life and home life. Not only are there issues of stress and mental health, but performing work tasks on improperly secured personal devices, or, alternatively, performing personal tasks on a work device, can present security risks for individuals and businesses alike. Three out of four people (76%) worldwide admit they use personal devices for work tasks, use work devices for personal tasks, or both, underscoring the boundary concerns mentioned previously.

Do you use your personal device for work or work device for personal tasks like checking email?

	Global Avg.	US	UK	AU/NZ	Germany	France	Italy	Japan
I use my personal device for work related matters	25%	32%	24%	24%	27%	26%	19%	23%
I use my work device for personal matters	15%	8%	13%	12%	15%	14%	28%	12%
Both	37%	43%	35%	43%	26%	39%	51%	20%
Neither	24%	18%	29%	21%	33%	21%	2%	44%

What gets people to click?

The answer is still an email from their boss, even on a personal account.

As in last year's survey[7], the most common answer to the question, "which kinds of emails do you open first?" is an email from one's boss. When checking their work email accounts, 64% of this year's global respondents said they would open an email from their boss before anything else.

But when we asked about their personal email accounts, the highest priority was still an email from respondents' bosses (32%).

According to Dr. Rajivan, the willingness to open emails from bosses in personal accounts is worrisome. "Context is a big part of how we identify threats," he says, echoing a similar sentiment from Dr. Cleotilde Gonzalez, the expert featured in last year's report: "a shopping offer in your work inbox might raise suspicion; same with a message from your boss in your personal inbox [...] this gets infinitely more complicated as people mingle accounts and the lines of context blur."[7]

> *There's also the matter of attentiveness. Like with distracted driving, working while doing other household chores or even watching TV seems easy enough when doing mundane tasks, such as email processing. But this type of distraction can also make people vulnerable. People might be less likely to properly notice and weigh the risks of a potential phishing message. That doesn't mean they need to physically be in the office to be productive, but it does mean that the lines between work and home need to be front and center.*
>
> **– Prashanth Rajivan, Ph.D.**

Gradients of Risk

Just 16% of Japanese respondents *fell victim to a phishing scam in the last year. They also are the least confident about their ability to spot these scams in the first place.*

Something that stands out as we examine the data is that, as in last year's survey, Japan continues to be an outlier in many scenarios.[8] For example, this year's data shows that Japanese respondents reported the lowest number of successful phishing attacks in the last year.

Do you believe you know enough to keep yourself and your personal data safe from cyberattacks?

	Yes	No	Don't know
Global Avg.	59%	24%	17%
US	70%	17%	14%
UK	75%	13%	13%
AU/NZ	67%	21%	13%
Germany	60%	22%	19%
France	44%	37%	19%
Italy	71%	15%	14%
Japan	26%	47%	27%

Individualism Increases Risk

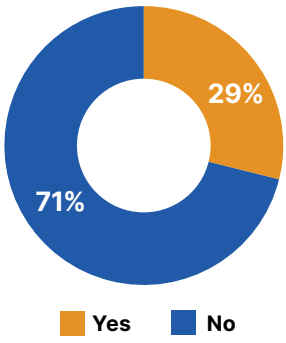
Ultimately, a business is a collective of individuals striving toward a common goal. If the collective's goals are aligned, then a business is more likely to succeed in achieving them. In contrast, "individuals who perceive themselves to be responsible only for themselves and no one else tend to take greater risks," says Dr. Rajivan. While risk taking certainly has its place in business, it's not something you want employees doing in their cybersecurity habits.

According to Dr. Rajivan, the disparities in terms of confidence vs. real-world incidence of phishing could be chalked up to a case of cultural differences. Using a popular cultural difference scoring mechanism[9], he pointed out that countries with more individualistic cultures, which are also generally more self-confident and have a lesser tendency to avoid uncertainty, seem to align with countries who ranked themselves highly on their ability to keep themselves and their data safe.

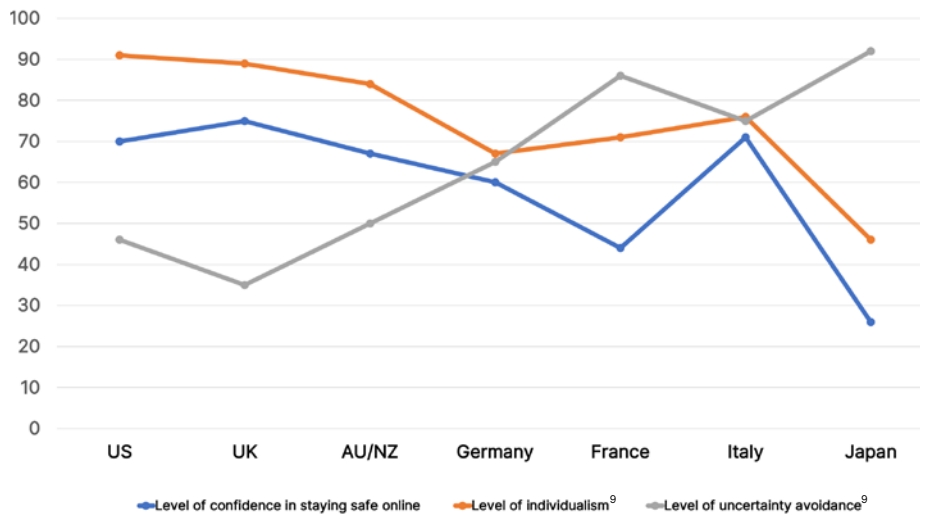
"A company is vulnerable to attacks because each employee is vulnerable."

Briana Butler, engineering services manager, Carbonite + Webroot, OpenText Companies

Have you clicked on a phishing link or fallen victim to a phishing scam in the last year?



GLOBAL AVERAGE



Individualism and Overconfidence

The correlations between overconfidence and individualism may also translate into a mentality that workers are not responsible for their own cybersecurity during work hours.

While 63% of workers surveyed stated they believe a cyber resilience strategy that includes both security tools and training for employees should be a top priority for any business, only 14% felt that cyber resilience was a shared responsibility among employees.

Who is responsible for cyber resilience within your current company?

	IT/security dept.	All employees	CEO or board	CIO or CISO	No one	Don't know
Global Avg.	57%	14%	9%	9%	3%	8%
US	61%	19%	11%	3%	2%	4%
UK	55%	24%	11%	4%	1%	5%
AU/NZ	52%	27%	9%	6%	1%	3%
Germany	66%	9%	6%	10%	2%	7%
France	52%	8%	8%	18%	3%	6%
Italy	55%	8%	9%	18%	2%	6%
Japan	55%	7%	4%	3%	8%	23%

When people adopt a less individualistic mindset and, instead, perceive themselves to have a greater responsibility to others, their average level of willingness to take risks decreases. This is especially important to note for businesses that want to have a cyber-aware culture.

Prashanth Rajivan, Ph.D.

The Dunning-Kruger Effect

According to Dr. Rajivan, another factor that could contribute to the general amount of overconfidence in people's ability to spot phishing attacks and avoid online threats might be a psychological phenomenon called the "Dunning-Kruger Effect". The Dunning-Kruger Effect refers to a cognitive bias in which people who are less skilled at a given task tend to be overconfident in their ability, i.e. we tend to overestimate our capabilities in areas where we are actually less capable.[10]

*Nearly **1 in 4 people** don't know if their company is resilient against cyberattacks.* ***1 in 5 flat-out think it isn't.***

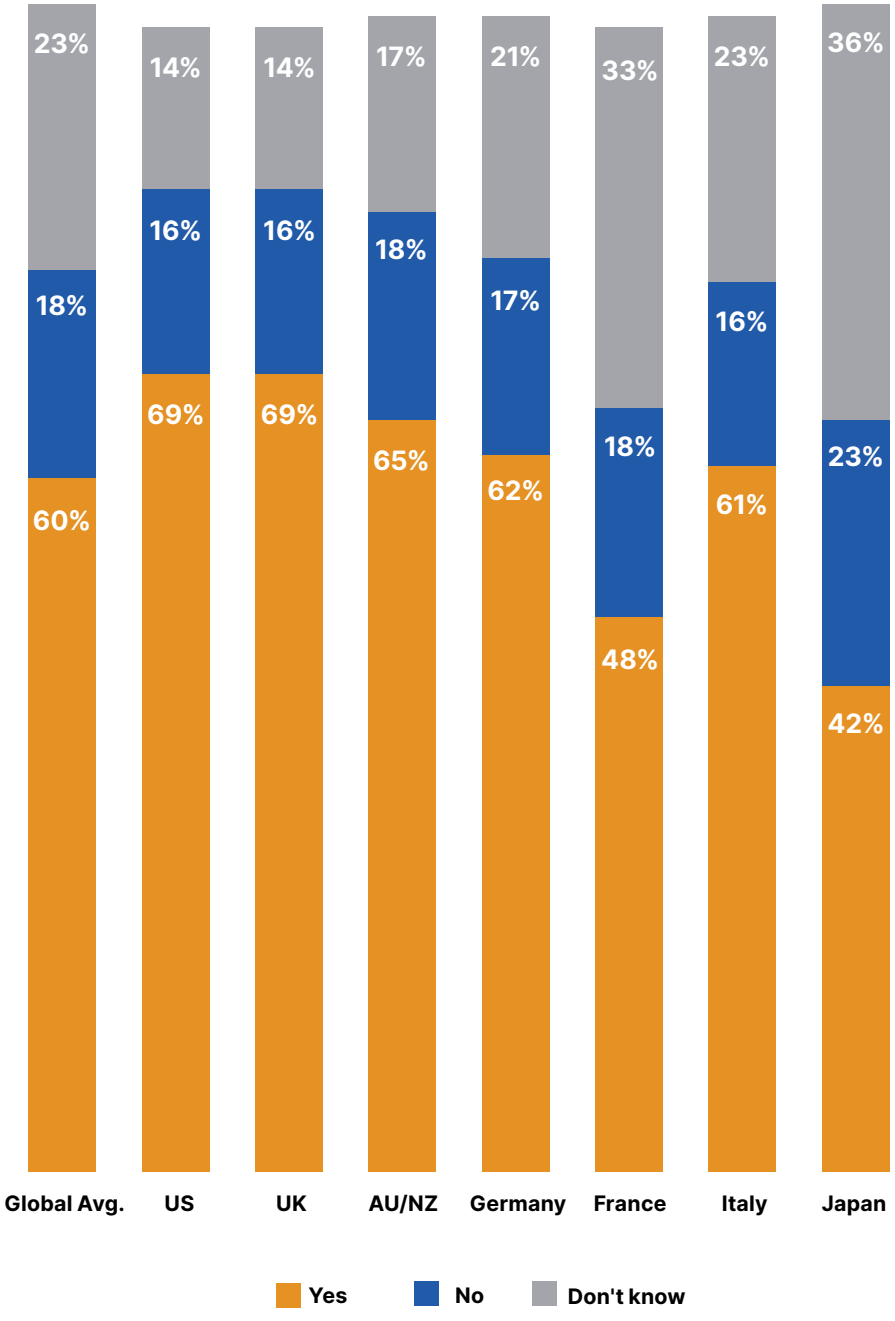
"Why do you think your company isn't resilient against a cyberattack?"

According to anonymous, write-in responses, many workers believe their employers could be doing more to support them and their security. Here are some of the responses to the question above.

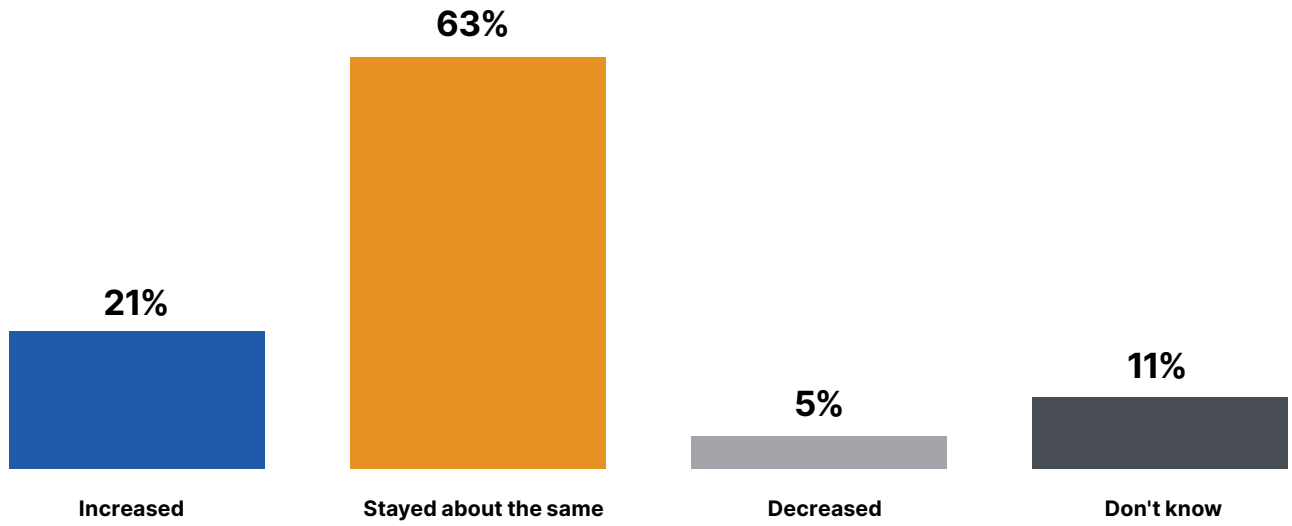
- "We have had breaches in our system several times this year alone."
- "I don't think there are enough controls in place."
- "I don't think this is something they spend much time or money on."
- "We use a third party IT company, so we're only as resilient as they are."
- "Our computers and equipment are poorly maintained. I'm betting our security is too."
- "We've been hacked before and I don't know if they upgraded our security since then."
- "I still get lots of phishing emails at work, so I don't think the filters are good enough."
- "Most of upper management would probably fall for a phishing scam."

Despite some of the more concerning numbers, there have been some improvements in people's online risk-taking behavior and their reactions to possible phishing scams. Of the 67% respondents in last year's survey who had been phished at work, 39% of those did not report it.[11] This year's numbers looked a lot better, perhaps because more companies are now implementing security awareness training, which typically includes processes for reporting phishing emails to infosec teams.

Do you think your company is resilient against a cyberattack?

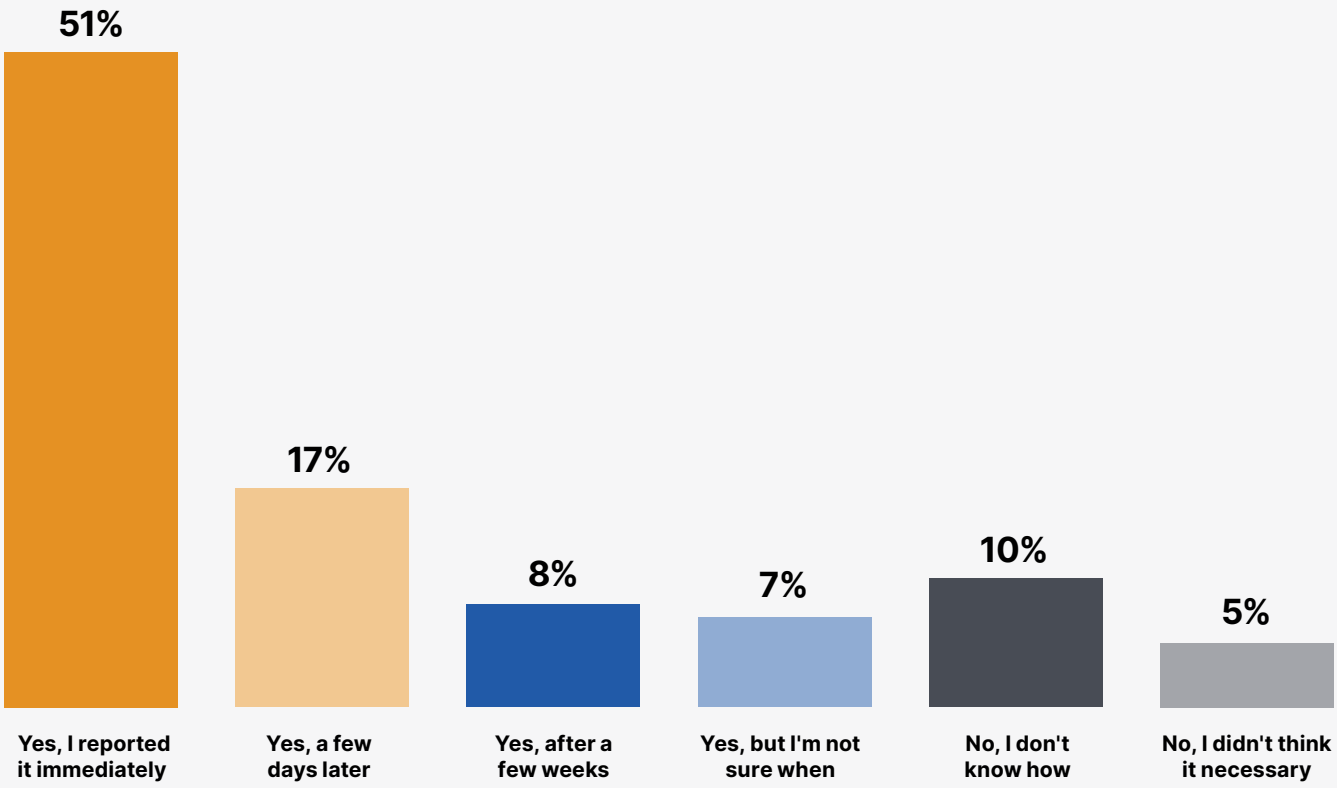


Has your company increased or decreased its amount of cybersecurity training during the COVID-19 pandemic?



GLOBAL AVERAGE

When you got phished, did you report the phishing email after you realized what it was? How soon?



GLOBAL AVERAGE

Expert Insights:
How to Make Lasting Change

I am a strong believer in reinforcement learning. Human behavior is shaped by past experiences, consequences and reinforcement.

To see a real change in human behavior related to phishing and online risk-taking habits in general, people need frequent and varied experiences PLUS appropriate feedback that incentivizes good behavior and disincentivizes poor behavior.

This feedback and incentive structure needs to be carefully calibrated. Too much could lead to heightened anxiety and false alarms, but too little could lead to underweighted risk, i.e. people knowing the correct actions, but not taking them.

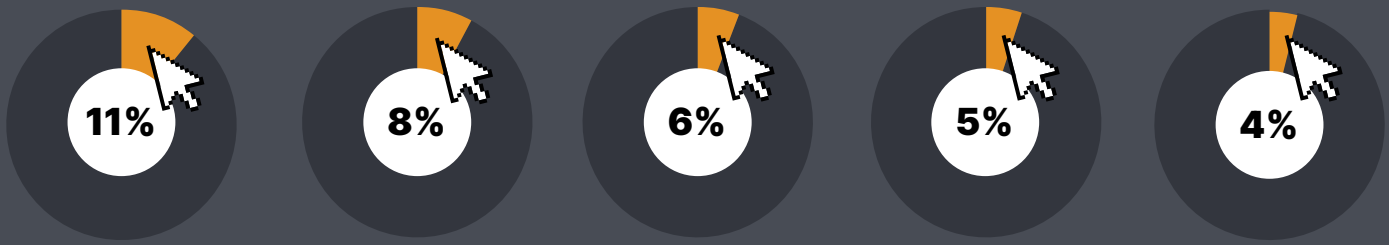
Prashanth Rajivan, Ph.D.

Data from Webroot® Security Awareness Training shows that, if you want people to make lasting changes to their behavior, you have to run consistent, relevant training courses and phishing simulations that are also varied enough that people won't get bored or find them predictable. Running a second simulation makes a dramatic impact — and it only gets better from there.

Philipp Karcher, principal product manager, Carbonite + Webroot, OpenText Companies

With consistent training, you can reduce click rates on phishing scams ***by up to 86.5%****.*[12]

The more phishing simulations you run, the more the click-through rates (%) improve.

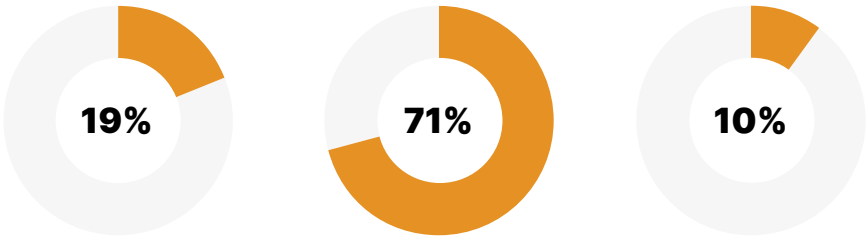


COVID-19:
The Risk We Never Expected

*At least **one in five** people have received a phishing email related to COVID-19.*

There's no doubt that the global COVID-19 pandemic has changed a lot about how we live and work. As seen in our study, more people throughout the world are working from home, and the resulting productivity increases have raised considerations that, perhaps, it should stay that way on the other side of these tumultuous times.[13] With more people connecting to the internet outside of corporate networks and away from the watchful eyes of IT teams, it's to be expected that cybercriminals would take advantage.

Have you received any phishing emails specifically related to COVID-19?



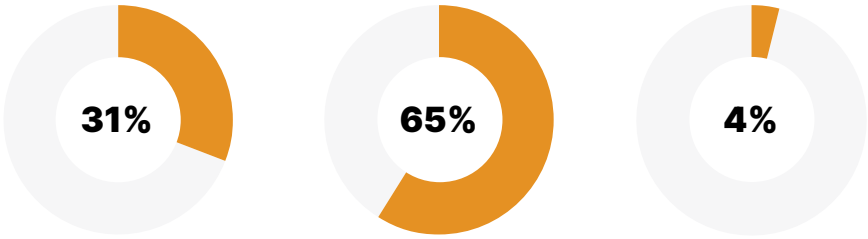
"Yes" | "No" | "Don't know"

GLOBAL AVERAGE

Precaution and Recovery

Regardless of any upticks in online threats, the majority of people surveyed still think they are at least the same level of prepared or more prepared to spot phishing email attempts, now that they've spent more time working from home.

Given the increase in the amount of time you've spent working from home, do you feel more or less prepared to spot phishing email attempts?



"More" | "About the same" | "Less"

GLOBAL AVERAGE

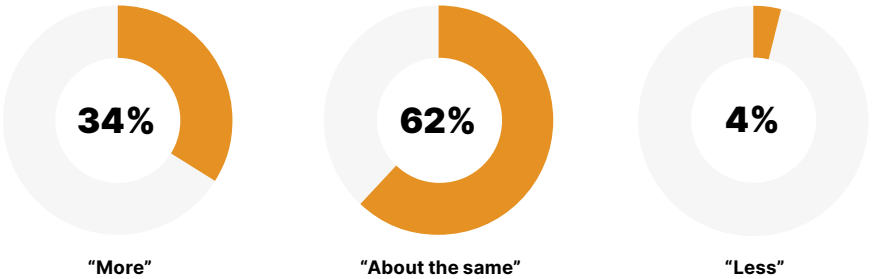
I'm actually surprised that the number of people who've received phishing emails is this low, given the massive spikes we've seen in phishing URLs targeting COVID-related topics. For example, with more people spending time at home, use of streaming services has gone up. In March alone, we saw a 3000% increase in phishing URLs with 'youtube' in the name. People may be either under-reporting or misidentifying phishing emails.

Grayson Milbourne, security intelligence director, Carbonite + Webroot, OpenText Companies

People are taking increased physical safety measures in the pandemic, including mask wearing, social distancing, more frequent hand-washing, etc. I think this heightened level of precaution and awareness could cause people to slightly overestimate their overall safety, including their safety regarding online threats.

Prashanth Rajivan, Ph.D.

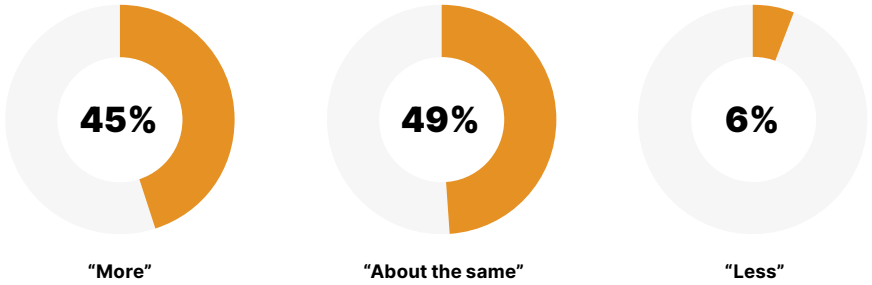
Since the beginning of the year, are you more or less concerned about phishing attempts to your work or personal email accounts?



GLOBAL AVERAGE

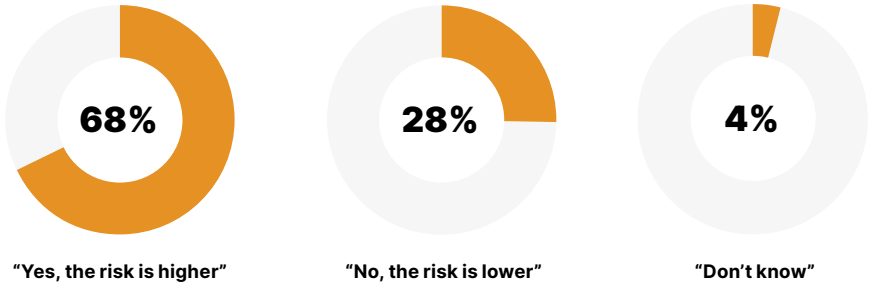
In terms of increased risk, nearly all people (94%) are online shopping more (or at least the same amount as before). Among those shopping online more often, nearly 7 in 10 (68%) think the risk that their credit and financial information could be exposed is higher than it was previously.

Due to the COVID-19 pandemic, have you done more online shopping than you did previously?



GLOBAL AVERAGE

With the increase in online shopping, do you think you face a higher risk that your credit card or financial information could be exposed to cybercriminals (hackers)?



GLOBAL AVERAGE

Regarding the relationship between the worldwide increases in online shopping and people's perceptions of increased risk, Dr. Rajivan said it's "actually to be expected. First, given the current pandemic situation, we have to consider that even people who never wanted to shop online may be doing so now out of necessity. Second, and perhaps more to the point, people show this sort of behavior all the time: perceiving risk, but taking the action anyway."

We tend to give strong preference or weight to doing something that leads to a reward, more so if it provides more immediate gratification. In this case, the gratification from online shopping is a more immediate reward. However, long-term, probabilistic consequences (such as a cyberattack in which your financial information was stolen and misused) feel like less of an immediate concern, so we naturally weight them lower.

Prashanth Rajivan, Ph.D.

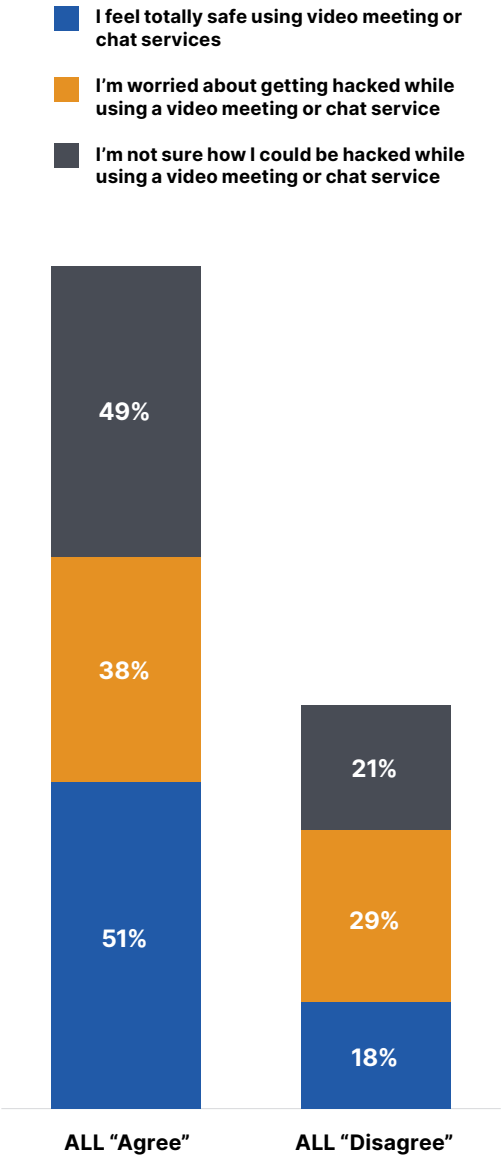
Dr. Rajivan also states that, if people are using reputable sites and brands they trust, they may also unconsciously extend that trust to the company's cybersecurity practices. "Even if people have heard of hacks at major retailers in the news, if a particular store hasn't 'betrayed' them personally or someone they know, then they are less likely to imagine that online shopping with that store would present real risk," he explains.

I received an email from a highly reputable brand with good quality products and great technology. It was offering a nice discount, so I clicked the link. Turned out to be a scam.

Anonymous survey response when asked to share a personal phishing experience

In addition to the shifts in online shopping habits, the majority of global respondents say they increased their use of videoconferencing and chat services in both work and personal settings, with a 68% increase and a 51% increase, respectively. However, many respondents expressed worry or uncertainty about the safety of using these programs.

Indicate your level of agreement with the following statements.



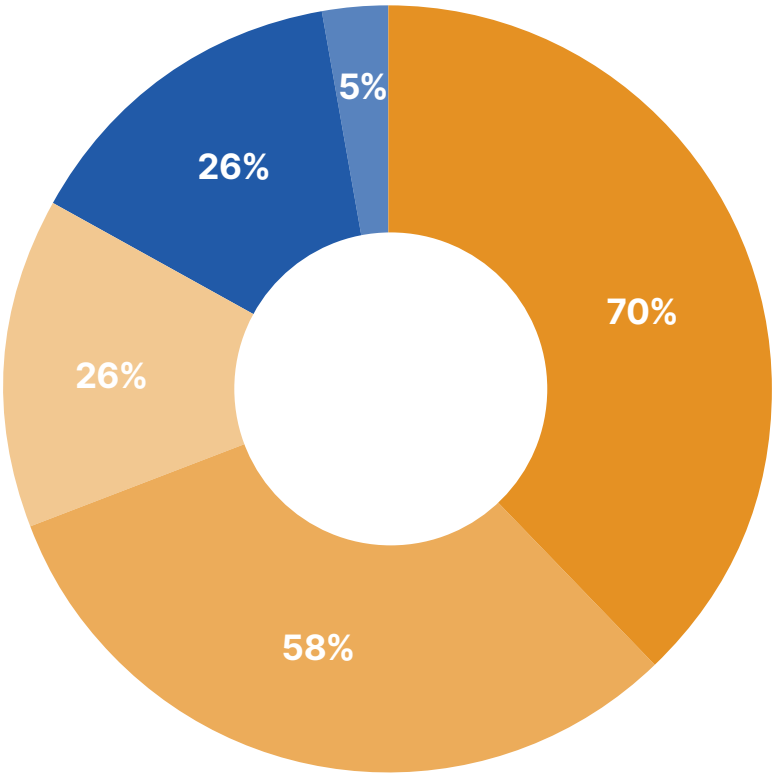
Expert Advice

We've seen videoconference executable files get faked or manipulated so that unwitting victims end up downloading malware. Between February and March alone, our data showed a 2000% spike in malicious files with 'zoom' in their filenames. It's crucial to make sure any videoconferencing software you use is up to date so you have the latest security patches.

Tyler Moffitt,
security analyst,
Carbonite + Webroot,
OpenText Companies

Overall, however, our survey indicates that the majority of people are either taking the same number or more precautions to keep themselves safe online. For instance, an average of 1 in 4 people are updating their computer operating systems and software more often than they did when they did prior to COVID-19. Additionally, an average of 1 in 5 report they plan to increase their investment in cybersecurity programs and tools for their and their families' personal devices.

How do you protect yourself from phishing attacks? (Check all that apply.)



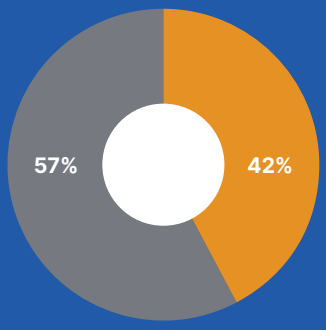
GLOBAL AVERAGE

- **I delete suspicious emails**
- **I read emails thoroughly before clicking**
- **I back up my data so it's recoverable in the event of an attack**
- **Job-mandated employee training**
- **I don't take any action to prevent phishing attacks**

Spotlight:
The Importance of Strong Backup

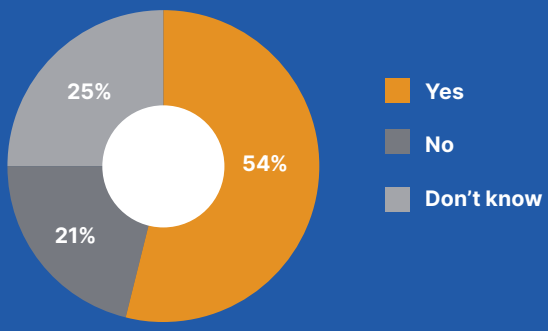
Only 26% of global respondents say they back up their data to ensure that it's recoverable in the event of an attack. However, 42% have said they needed to access backed up data to recover a file at some point since the pandemic began.

Have you needed to access your backed-up data to recover a file since COVID-19 began?



This discrepancy could be explained by the fact that, while individuals may not take specific action to back up their data, the businesses they work for may automatically perform backups in the background. However, only 54% of global respondents reported their respective companies back up their Microsoft® 365 suite, leaving a huge gap in data recovery plans.

Do you or your company back up your Microsoft® 365 (Teams, SharePoint, etc.) files?



With a mostly or entirely remote workforce, businesses and individuals can't afford not to have a strong backup.

Jamie Zajac, VP, product management, Carbonite + Webroot, OpenText Companies

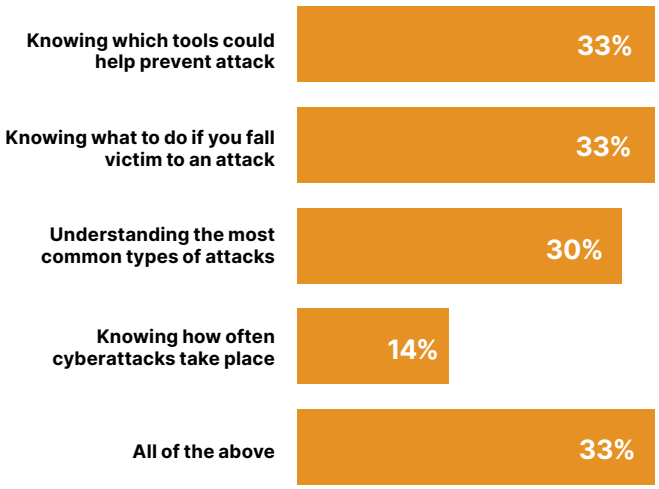
Caution: Don't assume M365 data is backed up.

While Microsoft 365 ensures the availability of their infrastructure, your data is your responsibility. Microsoft recommends a third party backup provider for the types of everyday data loss scenarios a business is likely to face.[14]

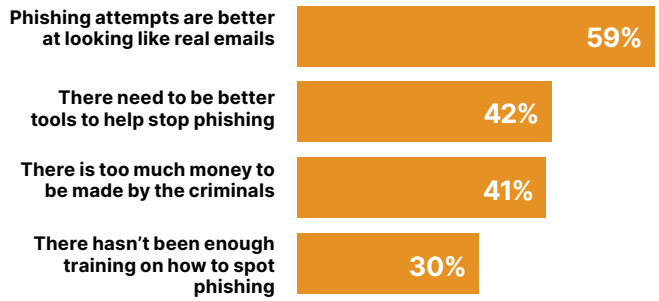
Conclusion:
The Way Forward

According to global respondents, more knowledge and better understanding is key for stronger cyber resilience. It's clear from the survey answers and write-in responses that many workers feel that, to properly prevent phishing, their employers need to invest more heavily in training and education, in addition to strong cybersecurity tools.

What would help you better prepare yourself to handle cyberattacks? (Check all that apply.)



Why do you think phishing is still an issue consumers and companies face? (Check all that apply.)



Dr. Rajivan points out that, if businesses are asking individuals to make changes to their own behavior for the greater safety of all, then they need to make it clear they are willing to invest in their people.

Additionally, in terms of training, the thing he stresses most is not the reward or penalty for certain behavior, but that positive and negative outcomes must be combined with appropriate and timely feedback. "Without appropriate feedback, no amount of training will be effective," he states. "And because the average person handles uncertainty poorly, training must include a variety of different scenarios. Human behavior is shaped through varied experiences, with a mix of positive and negative outcomes and applicable feedback."

In the end, knowledge, strong context, and both amount and variety of experience are equally important to build that "healthy dose of suspicion" which experts like Dr. Rajivan agree humans need to exercise in order to successfully identify and avoid phishing scams.

> *By creating a feeling of personal investment in the individuals who make up a company, you encourage the employees to return that feeling of investment toward their workplace. That's a huge part of ensuring that cybersecurity is part of the culture. Additionally, if we want to enable employees to assess risk properly, we need to cut down on uncertainty and blurring of context lines. That means both educating employees and ensuring we take steps to minimize the ways in which work and personal life get intertwined.*
>
> **Prashanth Rajivan, Ph.D.**

Online Safety In-Office, Out-of-Office and Beyond

TIPS FOR BUSINESSES

- **Invest in your people.** Train end users to avoid scams and exercise caution online. These programs need to be frequent, ongoing, varied and as up to date and relevant as possible. Empower your people with the tools they need to succeed.
- **Practice makes perfect.** In addition to education, end users need to practice good online behaviors. That means running regular phishing simulations and making sure all employees know how and where to report suspicious messages.
- **Keep it separated.** With so many employees working outside of traditional office settings, it can be difficult to enforce good boundaries. But by ensuring workers have clear distinctions between work and personal time, devices, and obligations, you can reduce the amount of uncertainty that can ultimately lead to phishing-related breaches.
- **Back up your collaboration tools.** It's more important than ever that employees be able to access and retrieve data no matter where they are. Make sure they can access collaboration tools, such as Microsoft® Teams and the Microsoft® 365 suite, and don't forget to back them up.
- **Know your specific risk factors.** Every business has different risk factors. If you don't have the in-house resources of expertise to conduct a risk audit, look into security auditing services or consult a managed service provider (MSP).
- **Over-prepare.** Once you've assessed the risks, you can create a data breach response plan that includes recovery strategies, security experts to contact, and communications plans to notify customers, staff, and the public.

TIPS FOR INDIVIDUALS

- **Update software and systems regularly.** Cybercriminals often exploit security holes in older software versions and operating systems. By keeping your devices and software up to date, you can help shut the door on malware.
- **Use strong, unique passwords.** Use unique, complex passwords for all accounts and change them regularly to help prevent fraud and other malicious activity. Consider using a secure password manager and enable two-factor authentication wherever possible.
- **Back it up!** Make sure important data and files are backed up to secure cloud storage or an external hard drive. In the case of a hard drive, make sure it's only connected while backing up, so you don't risk backing up infected or encrypted files. If it's a cloud back up, use the kind that will allow you to restore to a specific file version or point in time.
- **Stay on your toes.** Cybercriminals want you to be overconfident so they can take advantage of you. Don't play into their hands. By being vigilant and maintaining a healthy dose of suspicion about all links and attachments in messages, you can significantly decrease your phishing risk.
- **Educate yourself.** Even if the company you work for runs routine security awareness training, it's important to reinforce those teachings by studying up on your own. Dr. Rajivan recommends we all subscribe to cybersecurity-related content in the form of podcasts, social media such as LinkedIn, and other reputable information sources. That will help keep these issues top-of-mind, so we can all stay cyber-aware and resilient.

About the Data

The Webroot Phishing Survey was conducted by LEWIS among 7,000 office professionals, employed full-time, between June 10 and June 19, 2020, using an email invitation and an online survey. Quotas were set for 1,000 respondents in each of 7 markets: United States, United Kingdom, Australia/New Zealand, Germany, France, Italy and Japan. Results of any sample are subject to sampling variation. The magnitude of variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 1.2 percentage points overall.

About Dr. Rajivan

Prashanth Rajivan is an assistant professor in the University of Washington School of Industrial and Systems engineering. Prior to this appointment, he was a postdoctoral researcher in the Dynamic Decision Making Laboratory at Carnegie Mellon University. His research examines how human behavior affects information security and privacy to develop models of effective interventions that reduce the risk from attacks and promote safe behaviors online. With his work, he aims to characterize adversarial behaviors and strategies to inform incident response; measure teamwork and decision-making to augment security defense performance; and, uncover biases in end user decision-making that compromise security and privacy.

About the Author

Justine Kurtz has been writing and evangelizing in the cybersecurity space for over a decade. She has written or co-authored numerous technical white papers and reports on cybersecurity, and created, edited, or contributed to the majority of Webroot's written content, including each of its annual threat reports. Drawing on her background in technology, communication, and education, she works to clarify complex security topics and empower individuals, businesses, and large enterprises to take control of their security online. She holds a bachelor's degree in Computer Science from Smith College.

Note: All decimals in this report are rounded to the nearest percentage point. This may result in certain numerical totals adding up to slightly more or slightly less than 100%.

1 www.phishing.org/history-of-phishing

2 Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (Sep 2019)

3 Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (Sep 2019)

4 Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (Sep 2019)

5 Previous year's number derived from "Hook, Line, and Sinker: Why Phishing Attacks Work," which surveyed respondents in the U.S., U.K., Australia, and Japan, but did not survey Germany, Italy, or France.

6 www.nytimes.com/2020/06/23/business/working-from-home-productivity.html

7 Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (Sep 2019)

8 Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (Sep 2019)

9 www.hofstede-insights.com/product/compare-countries/

10 www.sciencedirect.com/science/article/pii/B9780123855220000056

11 Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (Sep 2019)

12 Webroot Inc. "2020 Webroot Threat Report." (Feb 2020)

13 www.nytimes.com/2020/06/23/business/working-from-home-productivity.html

14 www.microsoft.com/en-us/servicesagreement

About Carbonite + Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.