WEBROOT®
Smarter Cybersecurity™

HOOK, LINE, AND SINKER

Why Phishing Attacks Work

Introduction

When we talk about phishing, it might conjure up memories of scam emails from foreign princes, chock-full of terrible typos, grammar mistakes, and other easy-to-spot signs that the message might not be legitimate. If you're thinking in those terms, it might shock you to find out how many people actually fall for such attacks.

But these days, phishing attacks are getting increasingly believable. More scams are being reported in which an employee receives a message from their boss, CEO, or another higher-up, typically demanding that they take an action right away. And with strong pressure to perform well at work, people are more likely to take this kind of bait.

In partnership with Wakefield Research, we surveyed 4,000 office workers across the U.S., U.K., Australia, and Japan on their phishing knowledge and clicking habits. We then consulted with Dr. Cleotilde Gonzalez, research professor in the Department of Social and Decision Sciences at Carnegie Mellon University, to gain a deeper insight into the question: what is it that makes people click?

According to Dr. Gonzalez, the short answer to the question is "urgency, familiarity, and context."

In this report, we'll dig deeper into the survey results and present our own understanding of these statistics, as well as analysis from Dr. Gonzalez, insights from cybersecurity experts, real-world phishing stories from our customers and partners, and tips on how to stay safe from phishing threats.

Ultimately, urgency, familiarity, and context have a strong impact on decision making. If you already expect to receive emails from your boss at your office (context and familiarity), and you are accustomed to messages that request quick action (urgency), then you are likely to assume the message is real. It might never occur to you to suspect that it could be phishing.

– Cleotilde Gonzalez, Ph.D.

Global Findings

49% OF RESPONDENTS ADMIT THEY HAVE CLICKED LINKS IN MESSAGES FROM UNKNOWN SENDERS WHILE AT WORK.

Of those messages, 74% were emails, which are commonly used to drop malware or steal credentials.

Professionals surveyed are nearly 50/50 on whether they would be more likely to click a link or open an attachment from an unknown source on a work device vs. a personal one (44% and 56% respectively).

> *Overall, responses from the U.S., U.K., and Australia show a general overconfidence in their phishing know-how, and a tendency to prioritize work over all else. Meanwhile, Japanese survey-takers understated their security savvy, and would appear to prioritize family and friends.*
>
> **– Cleotilde Gonzalez, Ph.D.**

REGIONAL HOT TAKES

UNITED STATES

Overall, more professionals in the U.S. have had their personal or financial data compromised than respondents in other regions.

Here's a shock: of those whose information was stolen or exposed, nearly 1 in 3 (32%) didn't change their account passwords afterward.

UNITED KINGDOM

Nearly 9 in 10 (89%) U.K. professionals believe they could accurately distinguish between a phishing message and a legitimate one, but they may be overconfident. Results indicate fewer than half of respondents identified phone calls, postal mail, app notifications, and video chats as possible phishing attack paths.

AUSTRALIA

More than half (56%) of workers down under say they are more careful about clicking links or attachments at work than they are on personal devices (45%), but 3 in 5 have clicked a link from an unknown sender at work. More Australian workers have opened links in text messages than U.K. or Japanese counterparts.

JAPAN

Japanese survey respondents report receiving fewer emails and clicking fewer links from unknown senders than their counterparts in other regions. However, only 50% believe they could identify a phishing message vs. a safe one, and many are uncertain if their data has ever been compromised.

The Odds Are Hacked Against You

NEARLY HALF OF OFFICE WORKERS HAVE HAD THEIR DATA COMPROMISED.

Every day we're likely to hear about another massive data breach affecting millions of consumers—and if you have an office job, there's a good chance you're one of them. Nearly half of office workers (48%) have had their personal or financial data compromised as part of a breach or hack.

FIGURE 1: As far as you know—have you ever, even once, had your personal or financial data compromised as part of a breach or hack?*

Yes, more than once	26%	36%	30%	28%	9%
Yes, once	22%	26%	25%	28%	10%
Not that I'm aware	52%	38%	46%	44%	81%

Unfortunately, despite the prevalence of data breaches, office workers still aren't taking adequate precautions to prevent it from happening again. While Japan scored the worst on post-breach action (with 13% reporting they did nothing at all), there's clearly room for improvement in all regions.

MORE THAN 1 IN 3 HACKED OFFICE WORKERS (35%) DIDN'T BOTHER TO CHANGE THEIR PASSWORDS FOLLOWING THE BREACH.

Additionally, fewer than 3 in 10 (29%) of respondents informed legal authorities or the appropriate government agency.

EXPERT INSIGHT

If your data is breached, here's the order of operations **George Anderson, product marketing director at Webroot**, recommends:

1. Change your account passwords immediately! That includes accounts you don't believe were breached, but are using the same or a similar password.
2. Set up alerts with your credit agency.
3. Void existing credit cards, order new ones.
4. Engage a credit security service.
5. Notify law enforcement or the appropriate government agency.

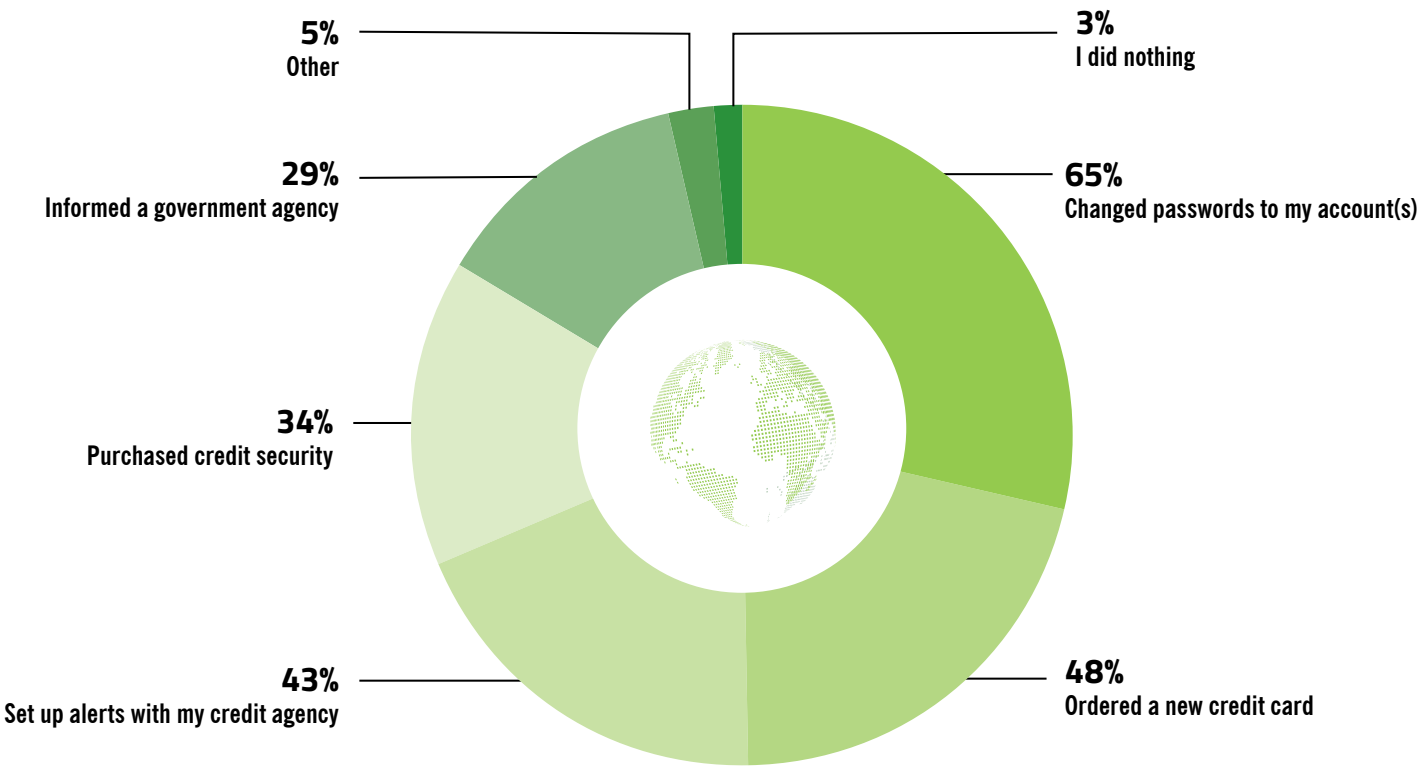
It also helps to enable two-factor authentication on all accounts, especially financial.

*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%.

FIGURE 2: Global responses to the question:

"When your personal or financial data was compromised in a data breach, which of the following, if any, did you do as a result?"

(Asked among those who know they have had personal or financial data compromised as part of a breach or hack)



The fact that 35% of survey respondents who were certain they're personal or financial data had been compromised didn't even take the basic action of changing account passwords is pretty alarming. Steps like using strong passwords at least 8 characters long (preferably closer to 16), which contain upper and lowercase letters, symbols, and numbers—and also enabling two-factor authentication wherever possible—are relatively simple ones, and can make all the difference

One factor that may contribute to this lack of action: in another survey conducted by Webroot earlier this year, more than one-third (34%)[1] of respondents reported they maintain more than 15 online accounts that require passwords, with one-third of those maintaining more than 30. If you're actually using unique passwords for each one, it means you only have to change one password when an account is compromised. But let's face facts; if you have at least 15-30 logins to remember, how likely are you to keep totally unique, strong passwords for each one?

PRO TIP

Use a secure password manager. It'll help you create, manage, and securely store your passwords, so there's less for you to worry about.

[1] Wakefield Research, commissioned by Webroot. "2019 Riskiest States Report." (March 2019)

Inbox Invasion

OFFICE WORKERS RECEIVE AN AVERAGE OF 52 EMAILS EVERY WORK DAY.

Phishing emails are one of the most commonly used methods of dropping malware or stealing personal data. But the volume of emails office workers receive each day, coupled with strong pressure for high performance and so-called efficiency, may make professionals even more susceptible to attacks. After all, if you only have enough time to take a quick glance at an email before responding, who's to say you'll look very closely? Worse still, if the email appears to be from your boss or a paying customer and is worded in a way that demands quick action, how likely are you to engage your suspicious mind and verify the message's authenticity or look for telltale markers of a scam?

"One of our clients' employees got an email that was supposedly from their CEO, asking the employee to help them purchase Google™ Play Store gift cards with the company credit card. The employee did it and sent over the codes right away, without ever questioning the request. It's important to make sure employees know they are allowed (and encouraged!) to verify all unusual requests, even from management. ***Blindly aiming to please the higher-ups could really cost you.****"*

– Larry Dukhovny, MyBizGeek Solutions

*"**I'll actually do the moral of the story first: never answer emails at 5 in the morning.** I was up early and restless, decided to go through my emails before I was fully awake. I was barely paying attention when I saw a routine-looking admin email from my Exchange hosting provider. I sure woke up fast when my Webroot web shield immediately popped a BLOCKED message because I'd inadvertently clicked a link to a malicious site. That was the day I also learned to have a little more empathy for clients who flunk their phishing simulation tests."*

– David Yates, Geeks-r-Us, Inc.

FIGURE 3: "In a typical workday, approximately how many emails do you receive?"

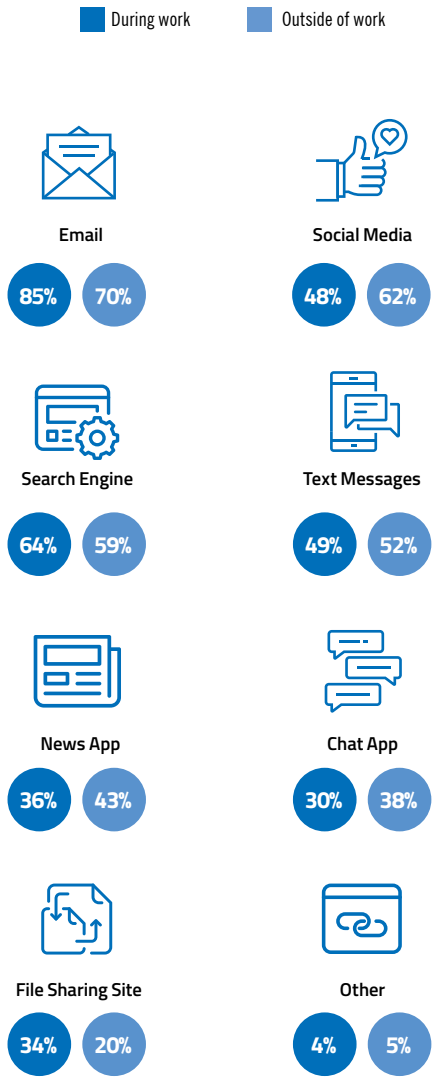
Less than 15	31%	27%	23%	25%	51%
15-34	34%	34%	37%	39%	26%
35+	35%	40%	40%	36%	24%

Although phishing emails are very common, you still get more legitimate ones than spam ones (probably thanks to better spam filters.) Because phishing emails are less common, it tricks us into thinking that there's a lower risk of being phished than there really is. There's also a difference in how we process email during and outside of work; that difference is in the context of the message. For example, a shopping offer in your work inbox might raise suspicion; same with a message from your boss in your personal inbox. However, this gets infinitely more complicated as people mingle accounts, and the lines of context blur.

– Cleotilde Gonzalez, Ph.D.

FIGURE 4: Global responses to the question:

"In a typical day, on which of the following do you click at least one link?"



If nearly everyone in the survey (85%) claims to click at least one link in an email during a given work day, and 70% of respondents click links in emails outside of work, that's already a huge opportunity for phishers to succeed. When we break that data down further, a third (33%) of office workers click more than 25 work-related links each day, and 14% click more than 50.

> *Every link in every email is a chance for a phishing attempt to hit pay dirt.*
>
> **– Briana Butler, Senior Engineering Data Analyst, Webroot**

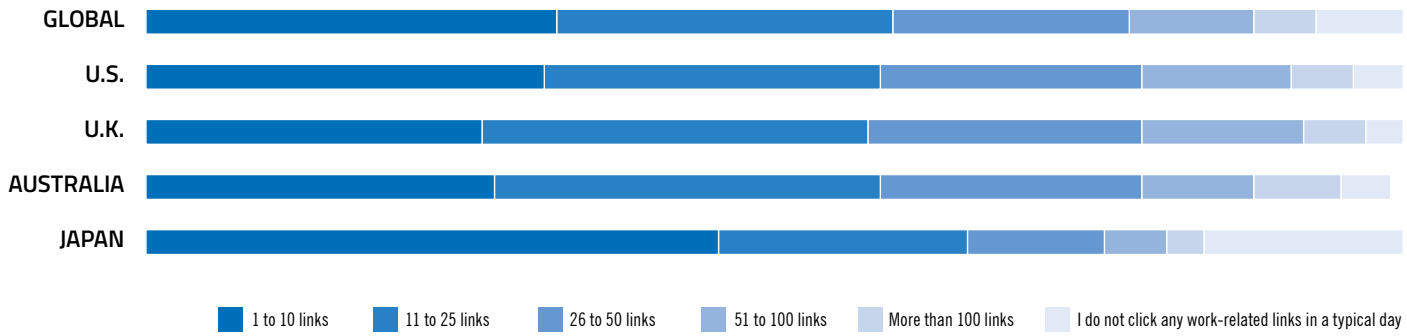
Meanwhile, workers are also click-happy outside of work. Nearly a third (31%) click more than 25 personal life-related links per day. This includes links from email (70%), social media (62%), search engines (59%), and text messages (52%.)

> *"I've gotten a few phishing attempts.* ***The worst one taught me not to open emails at 2:30 AM****. I was this close to clicking through on a phish that had me convinced my eBay account had been taken over. Thankfully, I thought twice before clicking and didn't go through with it."*
>
> **– Doug Terborg, Macatawa Technologies**

Between the survey data and the anecdotes from MSPs about their real-world encounters with phishing, it's pretty clear that pressures at work strongly contribute to the likelihood that people will fall for an attack. In particular, when we hear stories about someone getting phished in the wee hours, it begs the question: why are so many people checking work emails so late/early?

FIGURE 5: "Approximately how many work-related links, if any, do you click on a typical day?"

(Meaning all links in emails, chats, social media or texts and app notifications that you click in the course of a normal workday)



This is your Brain on Hack

THERE IS A FALSE CONFIDENCE AROUND PHISHING AWARENESS AND PROCESS. WHILE RESPONDENTS CLAIM TO BE ABLE TO SPOT A PHISHING ATTEMPT, MANY FAILED TO RECOGNIZE THE VAST AND VARIED METHODS OF PHISHING.

Nearly 4 in 5 office workers (79%) think they can distinguish a phishing message from a genuine one, but they don't seem to have all the facts on the different forms such attacks may take. Fewer than half of workers (43%) correctly identified phone calls as possible phishing vectors, and even fewer recognized app notifications (40%), postal mail (34%), or video chat (22%).

The data here shows that people are generally overconfident about their ability to spot the fakes. Overconfidence is a big problem in many human actions. In this case, this probably happens because the ratio of phishing emails to regular emails feels low, so our mind underestimates the probability of receiving a phishing email, and in turn, overestimates our ability to identify one if we do.

Humans make decisions based on experience—specifically, according to the frequency and recency with which similar events are experienced. For example, if you received a phishing email yesterday, you'd be more on-guard today. But if it's been a while, or if you've never knowingly received one, you wouldn't be so vigilant and would be more likely to fall for the attack.

And because you receive more emails than phone calls or social media messages a day, you're more likely to be able to identify a phishing email vs. a phishing call. There's also more awareness around email phishing in general, so it makes sense that people aren't as likely to recognize phishing attempts via non-email communication methods.

– Cleotilde Gonzalez, Ph.D.

FIGURE 6: Global responses to the question: "Which of the following do you believe are ways that hackers conduct phishing attacks?"

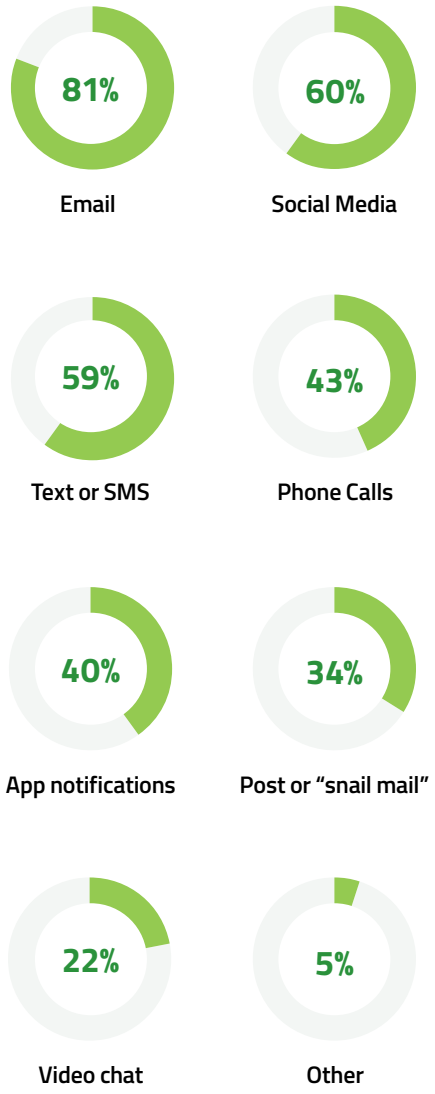


FIGURE 7: How strongly do you agree or disagree with the following statement:

I can distinguish a phishing message from a genuine one.

Agree strongly	38%	32%	36%	8%
Agree somewhat	49%	57%	55%	43%
Disagree somewhat	11%	9%	8%	35%
Disagree strongly	3%	2%	1%	15%

FOOD FOR THOUGHT:

Could overconfidence be a cultural thing?

Almost across the board, Japanese survey respondents gave lower numbers than their counterparts in other regions. In particular, they ranked themselves much more modestly about their ability to spot a phishing message, dragging the global average down significantly.

67% OF GLOBAL RESPONDENTS KNOW THEY HAVE RECEIVED A PHISHING EMAIL AT WORK.

39% OF THOSE DID NOT REPORT IT.

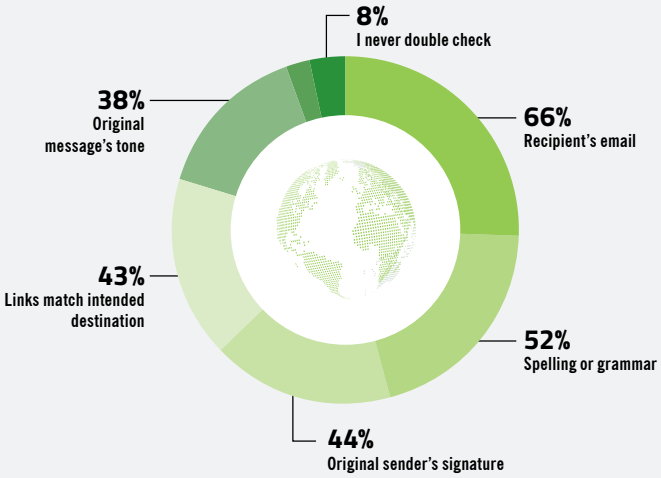
EXPERT INSIGHT

According to **Mike Trammell, deputy CISO at Webroot**, businesses need to make sure employees know how and where to report a phish. There should be a centralized and well-publicized point of contact. Additionally, some employees may not be reporting these incidents because they actually clicked through and are afraid of getting in trouble. It's important that employees are not only informed about the correct process, but are also reassured that they will not be punished if they unwittingly click.

Nearly all (92%) of global respondents claim they check for signs of phishing before sending response emails that contain sensitive information, but the self-reporting may not be terribly accurate, given the number of people who also admitted to having been phished.

Only 43% of office workers verify that links match their destinations before clicking, despite the fact that clicking malicious links is one of the primary ways a simple phishing attempt can turn into a major infection or data breach.

FIGURE 8



TALES OF TELL-TALE SIGNS

"We had a customer who received an email from someone they thought was their boss, wanting them to close out a deal and transfer money over. The employee almost did it because the email looked legitimate, except the signature used their boss' full name. ***Turns out that boss never did that in emails, so it tipped the guy off that something fishy was going on****."*

– Mike Dunn, Adtech IT Solutions

"One of our clients is a school. Their teachers got an email from the principal asking them for their phone numbers. Supposedly, the principal 'was out and didn't have the numbers at hand'. The teachers replied and started getting all kinds of texts that were worded as if they were from the principal, wanting them to purchase gift cards and text back the codes. ***Luckily, they called the principal via the phone number they already had, not the number sending the texts, before going through with the purchase.****"*

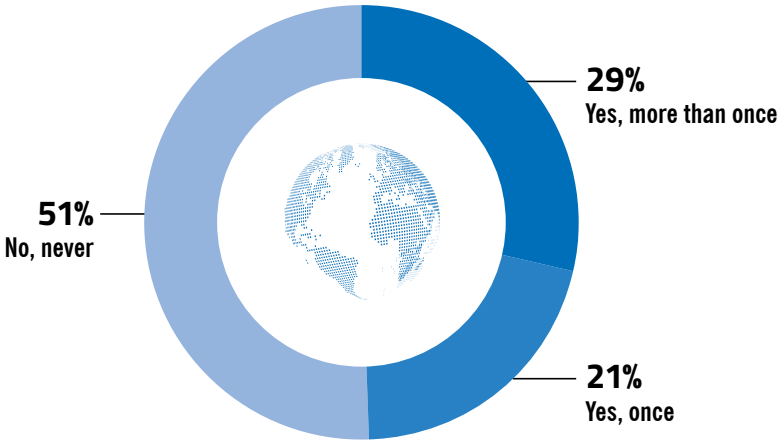
– Teri McMullen, Technical Specialties, Inc.

Taking the Bait

NEARLY HALF OF OFFICE WORKERS HAVE CLICKED A LINK FROM AN UNKNOWN SENDER, WITH 29% ADMITTING TO DOING IT MORE THAN ONCE!

FIGURE 9: Global responses to the question:

"Have you ever, even once, clicked a link in a message from an unknown sender while you were at work?"



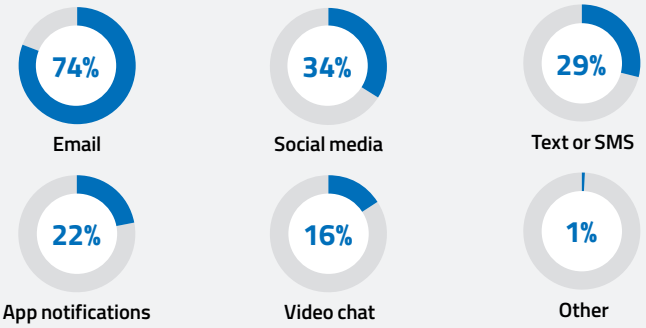
Worth noting is that, despite 81% of global respondents listing email as the number one way they believe hackers conduct phishing attacks, nearly three-quarters (74%) of workers who've clicked through from unknown sender messages admit the links were in emails. This number drops to less than half that (34%) when you ask about links in social media messages, suggesting that people trust social media, text messages, video chats, and other communication methods less than emails.

> *"These findings might seem surprising at first glance, but, again, can be attributed to expectations and context. At work, you may expect to receive emails from unknown individuals, such as inquiries from prospective customers, new contractors or partners, etc. In contrast, an unknown sender messaging your personal inbox might feel out of context or even like a violation, which might make you use more caution*
>
> **– Cleotilde Gonzalez, Ph.D.**

FIGURE 10: Global responses to the question:

"On which of the following did you click a link from an unknown sender?"

(Asked among those who have clicked a link in a message from an unknown sender while at work)



FOOD FOR THOUGHT:

Why would people who believe email is the most prevalent phishing attack vector be so willing to click links in emails from unknown senders?

"Risk and under-weighed probability are linked. Risks sometimes come with rewards, right? So if the risk seems low and the reward seems high, you'll make riskier decisions. It's like gambling; our minds explore different gain/loss experiences, then respond with risk-taking or risk-averse actions." **– Cleotilde Gonzalez, Ph.D.**

WHAT REALLY GETS PEOPLE TO CLICK? AN EMAIL FROM THEIR BOSS.

As we've seen in numerous reports from our IT provider partners: that's exactly what the cybercriminals are counting on. They commonly take advantage of employees' eagerness to please or accommodate their management structure, underscoring the importance of verifying all requests for purchases or sensitive information—even those that come from your superiors.

"I received a phishing email that was supposedly from the president of my company, saying he was in a conference and needed me to do something for him, but he couldn't talk on the phone. ***Meanwhile, the actual president of my company was standing about 20 feet away from me in the same room.****"*

– Koby Dudley, BECA, Inc.

FIGURE 11: Which of the following messages would you be most likely to open first?

An email from my boss	60%
A nice message from a family member or friend	55%
A request from my bank to confirm a transaction	31%
A discount offer from a store	28%
A link to a video from a friend or family member	27%
A prompt for me to verify/authenticate my account	25%
A notification about a fine	19%
Instructions to confirm my billing address	18%
A subpoena or legal request	16%
A link to a funny meme	13%
A message claiming to contain nudes	9%

Interestingly, very few respondents surveyed admitted to opening messages claiming to contain nude photos. However, according to Grayson Milbourne, security intelligence director at Webroot, this is an incredibly common and effective lure. In particular, he notes that criminals may even include a victim's account password (collected via data breach) to make the victim believe they are truly being watched. Input from our IT partners supports the apparent success of this type of scam.

THE SHAME GAME

"We've seen some phishing emails that try to trick you into thinking your webcam was hacked or something similar. We had one client receive one of these, and they were talking to us as if they had actually been caught doing something gross on their webcam. There are a lot of weird and inventive scams out there, and they exist because there's somebody that will take the bait."

– Adam Frielli, Springthrough

"There are a lot of scams that say they've got webcam footage of you doing nasty things, or some kind of record of nasty websites you go to. Some of them even threaten to report the recipient to their boss for using their work PC for gross or inappropriate behavior."

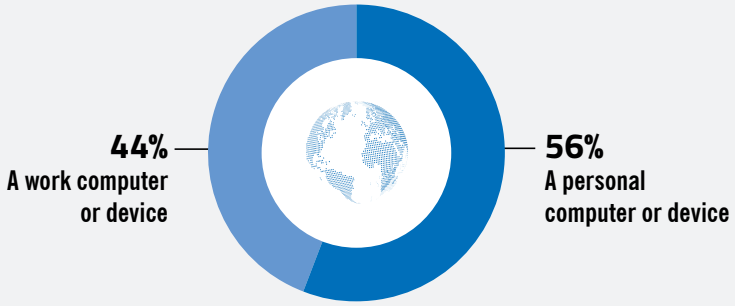
– Chris Cable, Techworks Consulting, Inc.

EXPERT INSIGHT

Grayson Milbourne, security intelligence director at Webroot, says that what's interesting about the responses to the question in Figure 11 is how well these types of "shame" attacks tend to work. He states, "think about it: the same thing that would get you to fall for it—to click through because you're concerned about your boss learning you 'misuse' your work computer for lewd or pornographic purposes, or whatever the attacker is threatening you with—is actually the same reason you wouldn't answer this question 100% honestly. People are ashamed."

Ultimately, people do seem to draw a distinction between the actions they take on their work computers versus on their personal devices. Still, the split is fairly even.

FIGURE 12: On which of the following are you more likely to click on a link or open an attachment from an unknown source?



Conclusion

According to Dr. Gonzalez, the data ultimately shows us that security and productivity are being treated as a tradeoff. Think of the number of times you've postponed a backup or an antivirus scan because you were busy doing something you perceived as more important, or something that had a more immediate reward? "You get paid to work, not to back up data or stay secure," she explains, "and those scans and uploads can take a long time or slow down your computer. Of course you'll put them off."

As long as people continue to underestimate the probability of risk, they will feel overconfident in their ability to defend against it. "It's a classic case of underweighting probabilities," says Dr. Gonzalez, "but explicit numbers speak for themselves. Providing this information might help people calibrate the risk and confidence more accurately."

Phishing scams are on the rise, and individuals who are familiar with trends, who are consistently trained via simulations and supported in their pursuit of a better work-life balance, will be the best defense against advancing and highly personalized phishing scams.

These findings illuminate the fact that what we really need here is a mindset makeover. The longer-term reward of security needs to be highlighted, front and center, not placed on the backburner. To do that, we're going to have to shift the way that people think about security and prioritize their responsibilities. We have to allow the time and brain space for security-related considerations, which means reevaluating how we interact with colleagues, bosses, and subordinates.

– Cleotilde Gonzalez, Ph.D.

How You can Stay Safe, at Work and at Home

TIPS FOR BUSINESSES

- **There's no such thing as being over-educated**. Teach your end users how to avoid scams and exercise caution online. Remember, security courses shouldn't just be once a year. These programs need to be frequent, ongoing, and as up to date and relevant as possible.
- **Get plenty of exercise.** 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.
- **Don't forget about mobile and remote workers.** As "bring your own device" (BYOD) continues to get more common, it's increasingly important to secure such devices and restrict the amount of unmonitored network access they may have.
- **Understand your risk profile.** Every business has different risk factors. If you don't have the in-house resources or expertise to conduct a risk audit, look into security auditing services or consult a managed service provider (MSP).
- **Hope for the best, plan for the worst.** 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

- **Maintain 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.
- **Keep software and systems up to date.** 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.
- **Back up, back up, back up.** Make sure all important data and files are backed up to a hard drive or cloud storage. 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.** As you can see from the data in this report, cybercriminals want you to be overconfident and complacent about your security so they can take advantage of you. Don't play into their hands. By being vigilant and maintaining a healthy level of suspicion about all links and attachments in messages, you can significantly decrease your phishing risk.

About the Data

The Webroot Phishing Survey was conducted by Wakefield Research among 4,000 office professionals, employed full-time, between August 2nd and August 15th 2019, using an email invitation and an online survey. Quotas were set for 1,000 respondents in each of 4 markets: U.S., U.K., Australia, 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 1.6 percentage points overall and 3.1 percentage points in each country from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

About Dr. Gonzalez

Cleotilde Gonzalez is a Research Professor at the Department of Social and Decision Sciences at Carnegie Mellon University. Her research work focuses on the study of human decision making in dynamic and complex environments. She is the founding director of the Dynamic Decision Making Laboratory where researchers conduct behavioral studies on dynamic decision making using Decision Making Games, and create technologies and cognitive computational models to support decision making and training.

About the Author

Justine Kurtz has been writing and evangelizing in the cybersecurity space for nearly 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 and businesses of all sizes to take control of their security online. She holds a bachelor's degree in Computer Science from Smith College.

About Carbonite

Carbonite provides a robust data protection platform for businesses, including backup, disaster recovery, high availability and workload migration technology. The Carbonite data protection platform supports businesses on a global scale with secure cloud infrastructure. To learn more, visit www.carbonite.com and follow us on Twitter at @Carbonite.

Carbonite, Inc. serves customers through three brands: Carbonite data protection, Webroot cybersecurity, and MailStore email archiving.

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.