Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **October 2022**
Commissioned by **IRONSCALES**

The Business Cost of Phishing

Executive Summary

Phishing is a type of cybersecurity attack experienced by all organizations. Successful attacks result in lost account credentials, fraud, and data theft. Preventing successful attacks is proving costly for organizations, with phishing-related activities consuming one third of the total time available to IT and security teams. On average, organizations spend almost 30 minutes dealing with each phishing email identified in their email infrastructure.

The purpose of this research was to quantify the direct costs borne by organizations in mitigating the phishing threat, and to explore expectations about how phishing will change over the next 12 months.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Phishing has been, is currently, and is expected to continue to represent a significant threat to organizations**
  Current and expected levels of phishing represent a "threat" or "extreme threat" to one third of organizations due to the consequences of successful phishing incidents, such as loss of account credentials, business email compromise, and data theft.
- **Phishing represents a huge time burden for IT and security teams**
  IT and security teams spend one third of their total available time handling the phishing threat every week. At most organizations, phishing is expected to get worse over the coming 12 months.
- **Phishing is an expensive issue for organizations to address**
  On average, dealing with the threat of a single phishing email takes 27.5 minutes at a cost of $31.32 per phishing message. Some organizations are taking much longer and paying more per phishing message, and no organization sees only a single phishing attack in any given time period.
- **Phishing is expected to get more sophisticated and better able to evade detection over time**
  IT and security professionals expect the volume of phishing attacks to increase over the next 12 months, as well as getting more sophisticated and pernicious. The time and cost currently expended on mitigating phishing will increase unless organizations start relying on better phishing protections.
- **Phishing is spreading beyond email**
  Organizations are already seeing phishing attacks in new communication and collaboration tools beyond email, with phishing in messaging apps and cloud-based file sharing platforms the most common new attack vectors.

Phishing: dangerous, costly, risky, and increasingly pernicious.

ABOUT THIS WHITE PAPER

The survey and white paper were commissioned by IRONSCALES. Information about IRONSCALES and details on the survey methodology are provided at the end of the paper.

The Threat of Phishing

Phishing is a threat to organizational data, finances, and reputation. In this section, we look at how the survey respondents rate the threat of phishing.

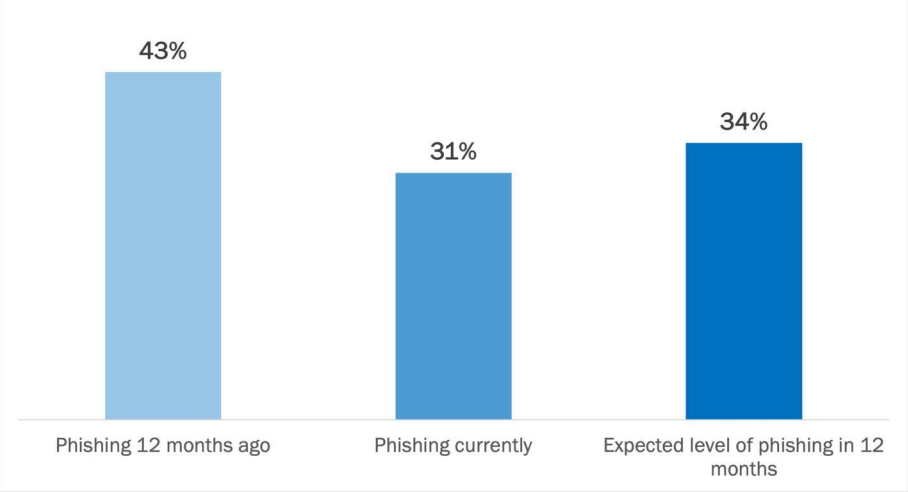
THE THREAT OF PHISHING

Current and expected levels of phishing represent a "threat" or "extreme threat" to one third of organizations. The current level of threat has declined over the past 12 months—perhaps reflective of the shift at many organizations towards office-based work again, where phishing risks are lower than for remote workers—but is expected to increase again over the coming 12 months. See Figure 1. Threats from phishing include:

- **Loss of account credentials**
  Phishing emails commonly impersonate well-known brands (e.g., Microsoft, Amazon, Apple, and banks) and ask the target victim to check their account for abnormal behavior. The link included in the phishing email instead takes the victim to a fake website that captures their account credentials, providing the phisher with full access to the victim's account and associated privileges. Sophisticated phishing attacks that circumvent multi-factor authentication (MFA) protections are becoming more commonplace.
- **Trickery of users into paying fake invoices or diverting payroll**
  Business email compromise (BEC) attacks frequently start with targeted phishing emails intended to trick a manager or finance employee into authorizing fake invoices or changing employee payroll details.
- **Compromise of corporate data**
  Phishing emails that install malware can result in data exfiltration, as can messages that compromise account credentials. Phishers gain corporate data, triggering data breach notification procedures, the risk of identity theft for customers, loss of customer trust, and reputational damage.

Phishing is seen as a significant threat at one third of organizations.

Figure 1
Evaluating the Threat of Phishing
Percentage of respondents indicating "threat" or "extreme threat"

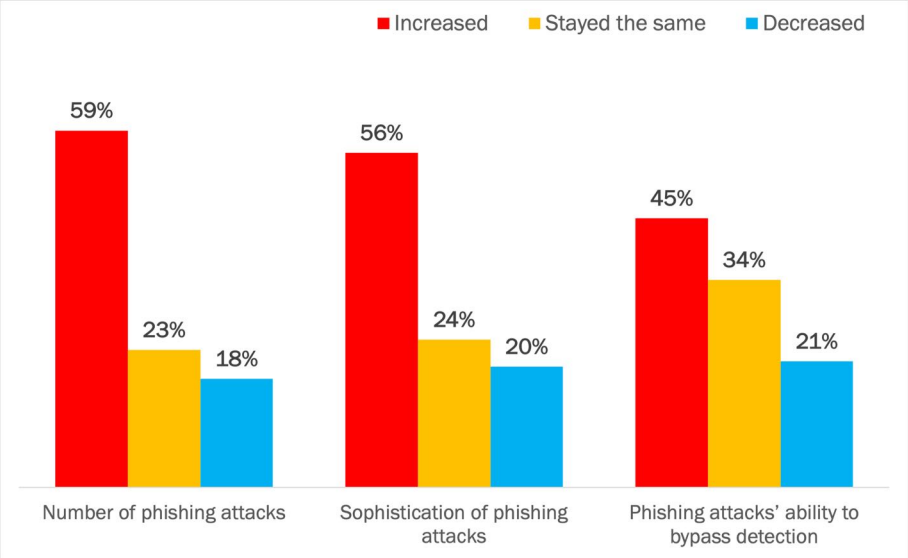


Source: Osterman Research (2022)

HOW PHISHING ATTACKS ARE CHANGING OVER TIME

Four out of five respondents reported that various dynamics of phishing attacks had gotten worse or stayed the same over the past 12 months. These dynamics were the number of phishing attacks (82% increased or stayed the same), the sophistication of phishing attacks (80%), and the ability of phishing attacks to bypass current detection mechanisms (79%). See Figure 2.

Figure 2
Dynamics of Phishing Attacks Over the Past 12 Months
Percentage of respondents



Source: Osterman Research (2022)

The increase and continuity of these various dynamics is seen in the characteristics of phishing threats rated as concerning by respondents (see Figure 3 on the next page). Half of respondents rated three characteristics as highly concerning:

- **Use of adaptive techniques by threat actors to create unique attributes for each phishing message**
  Adaptive techniques, also known as polymorphic attacks, vary each phishing message slightly as a method of increasing sophistication and decreasing the likelihood of being detected as a phishing message. Polymorphic attacks create unique messages that must be evaluated one by one, rather than being able to match using signatures or other known or trained identifiers. The use of polymorphic attack methods is ranked as the issue of highest concern.
- **Use of compromised account credentials by threat actors to hijack current email threads to send phishing threats**
  Account credentials obtained from an earlier phishing message—or purchased on the dark web—are then used to spread subsequent phishing messages on current email threads. This is a sophisticated attack, since social dynamics in the thread are already established, assuring a level of interpersonal trust and rapport that is more difficult to create between unknown parties. It is also likely to bypass detection since the messages are sent from the organization's own email infrastructure, removing many threat signals that can be evaluated when messages originate externally.

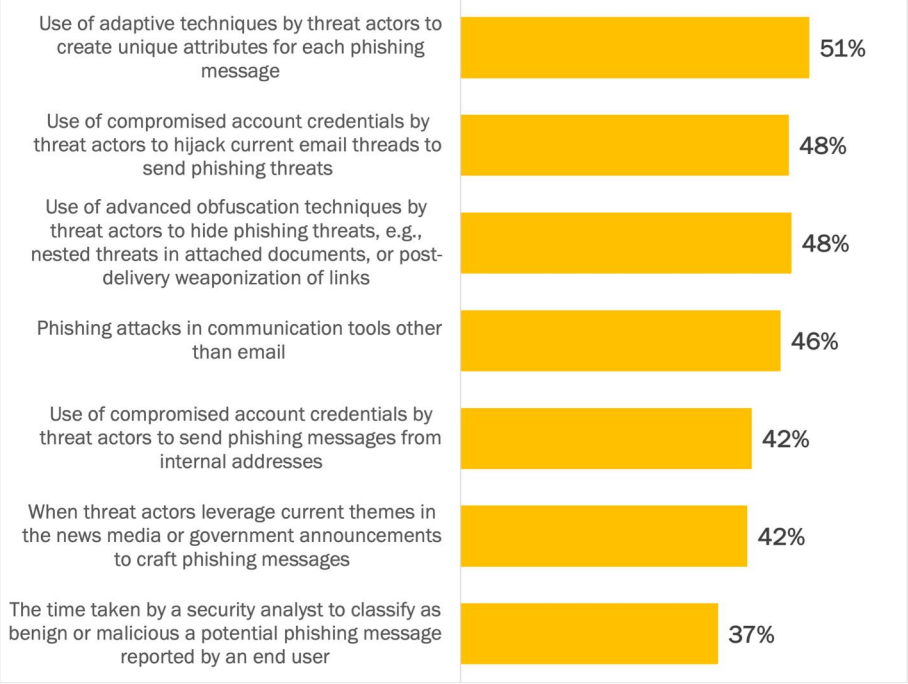
80% of organizations indicate that various dynamics of phishing have worsened or remained the same over the past 12 months.

- **Use of advanced obfuscation techniques by threat actors to hide phishing threats**
  A related method of increasing sophistication and decreasing the likelihood of being detected is advanced obfuscation, where payload and link threats are nested, initially presented as benign, or subsequently downloaded. Phishing defenses must then evaluate messages for threat signals at multiple points in the lifecycle of the message.

Several additional issues evidencing growing sophistication and bypass capabilities of phishing messages are shown in Figure 3. These include:

- Phishing in tools other than email—rendering detection capabilities focused solely on the email channel as ineffective.
- Internal phishing using compromised accounts—which decreases the detection likelihood since messages do not originate externally.
- Leveraging current themes in news media and government announcements—thereby increasing sophistication and the temptation for a targeted victim to open the message, attachments, and any links.

Figure 3
Concerns with Characteristics of Phishing Threats
Percentage of respondents indicating "concern" or "extreme concern"



Source: Osterman Research (2022)

A diverse set of increasingly sophisticated phishing threats are slipping through protections and causing havoc for organizations.

The Cost of Phishing

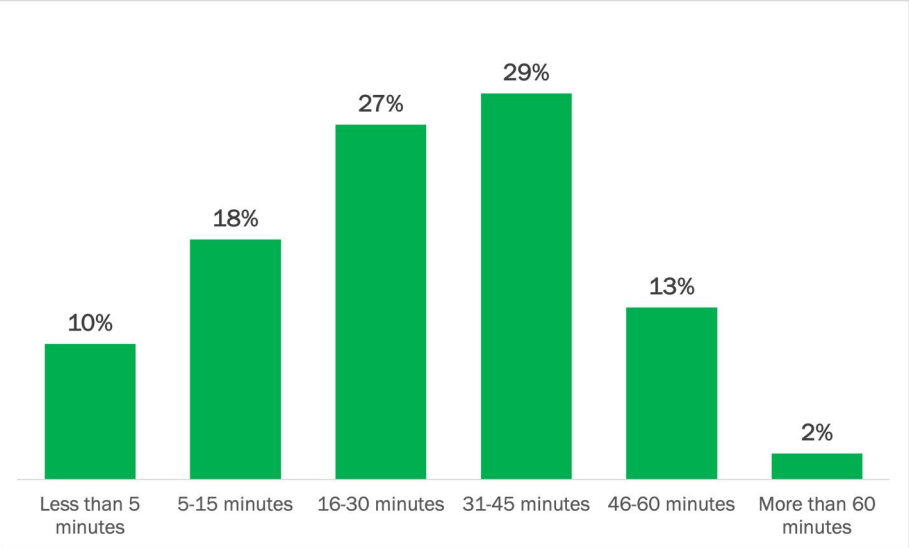
In this section, we investigate the direct cost of phishing to organizations.

TIME TO DEAL WITH A SINGLE PHISHING EMAIL

Organizations spend a significant amount of time dealing with phishing emails, with 70% of organizations spending 16 to 60 minutes for each phishing email. This covers the phishing lifecycle from initial discovery of a potential phishing email to its complete removal from the environment. It is most common for organizations to spend 31-45 minutes per phishing email (29% of respondents indicate it takes this long at their organization).

See Figure 4.

Figure 4
Total Time for IT and Security Teams to Deal with a Single Phishing Email
Percentage of respondents



Source: Osterman Research (2022)

Clearly, no organization has to deal with only a single phishing email. With several billion phishing messages sent globally every day, phishing is a significant proportion of overall email volumes.

70% of organizations spend 16-60 minutes dealing with a single phishing email message.

CALCULATING WHAT IT COSTS TO DEAL WITH PHISHING

To calculate the cost of dealing with phishing in IT and security teams, we need to determine the average salary and benefits of an IT and security professional. To do so, we created a composite based on the roles reflected in this survey who spend time each week dealing with phishing at their organization. See Figure 5, where:

- **Column 1: Roles**
  The seven roles in the survey that personally spend time each week dealing with phishing threats are listed in the first column.
- **Column 2: Percentage of survey respondents**
  The percentage of respondents in each role who completed the survey is shown in column 2.
- **Column 3: Median annual salary and benefits**
  The median annual salary and benefits reported for each role in the United States on salary.com in July 2022 is shown in column 3.
- **Column 4: Contribution to the composite IT and security professional**
  Column 4 calculates the contribution of each role to the composite fully burdened annual salary and benefits. This totals to $136,528 per year or based on an annual work year of 2,000 hours, $68.26 per hour.

A composite IT and security professional costs $136,528 per year in salary and benefits, or $68.26 per hour.

Figure 5
Calculating the Cost of a Composite IT and Security Professional

Role of respondent completing the survey	Percentage of respondents	Annual salary and benefits	Contribution to composite
IT security manager or IT security team lead	40%	$ 138,504	$ 55,512
IT manager or IT team lead	29%	$ 151,150	$ 44,385
Email security manager or email security team lead	16%	$ 141,000	$ 22,381
Security manager	8%	$ 101,329	$ 8,042
Email security administrator	5%	$ 82,781	$ 4,270
SOC manager or SOC team lead	1%	$ 134,330	$ 1,599
SOC analyst	0.4%	$ 85,324	$ 339
			$ 136,528

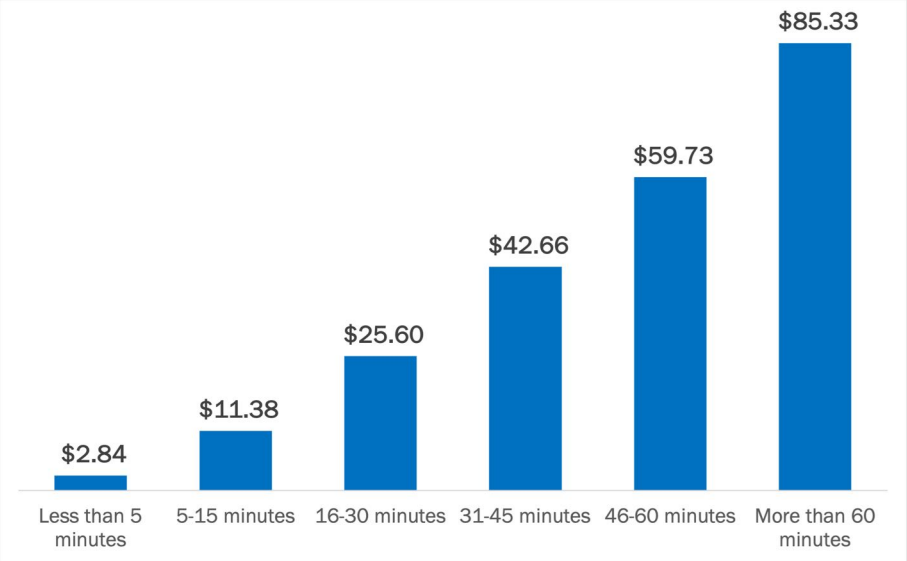
Source: Osterman Research (2022)

COST OF DEALING WITH A SINGLE PHISHING EMAIL

Dealing with phishing costs time for IT and security teams, and the professionals spending their time on phishing in these teams represent cost to the organization in salary and benefits. The fully burdened labor cost per phishing email for the professionals represented in this study is shown in Figure 6—ranging from teams spending five minutes or less per phishing email, costing $2.84 per phishing email, to teams spending more than 60 minutes, costing $85.33 per phishing email.

On average, time spent per phishing email is 27.5 minutes, at a cost of $31.32 per phishing email. This is calculated by combining the distribution of time spent with the fully burdened labor cost of the specific roles of IT and security professionals reflected in this study (as calculated in Figure 5 above).

Figure 6
Cost of Dealing with a Single Phishing Email
Fully burdened labor cost per phishing email



Source: Osterman Research (2022)

IT and security teams spend an average of 27.5 minutes to deal with a single phishing email, at a fully burdened labor cost of $31.32 per message.

The above figures are per phishing email. All organizations see many more than a single phishing email (remember, billions are sent every day), hence the costs increase as an organization receives more phishing messages. See Figure 7.

Figure 7
The More Phish, the Higher the Cost

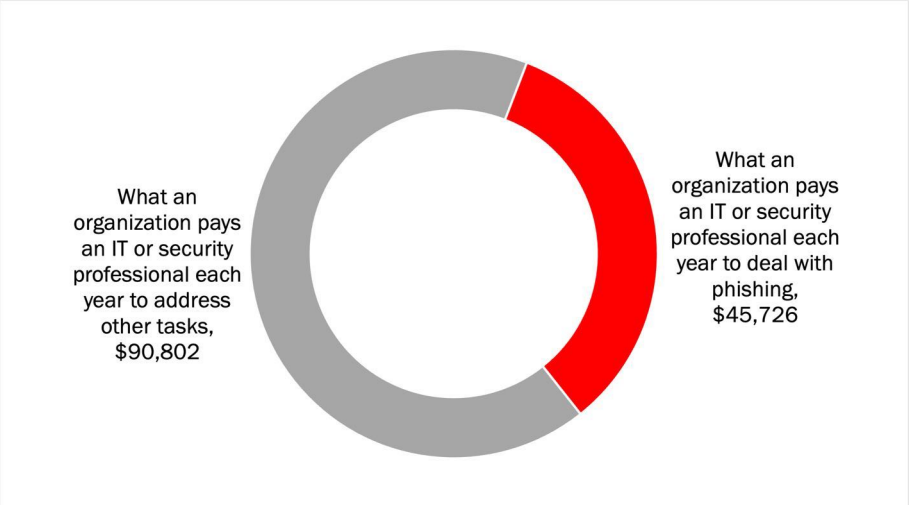
Phishing messages	Less than 5 minutes	5-15 minutes	16-30 minutes	31-45 minutes	46-60 minutes	More than 60 minutes
250	$710	$2,845	$6,400	$10,665	$14,933	$21,333
1,000	$2,840	$11,380	$25,600	$42,660	$59,730	$85,330
7,500	$21,300	$85,350	$192,000	$319,950	$447,975	$639,975
15,000	$42,600	$170,700	$384,000	$639,900	$895,950	$1,279,950
20,000	$56,800	$227,600	$512,000	$853,200	$1,194,600	$1,706,600

Source: Osterman Research (2022)

TIME SPENT PER WEEK ON PHISHING-RELATED ACTIVITIES

Respondents indicated that handling phishing-related activities consumes an average of one third of the working hours available each week for the IT and security teams at their organization. On an annual basis, for the composite IT and security professional created above, this equates to $45,726 in salary and benefits paid per IT and security professional to handle phishing. See Figure 8.

Figure 8
Annual Salary Paid Per IT or Security Professional to Handle Phishing and Other Tasks
Fully burdened labor cost per year



Source: Osterman Research (2022)

The salary amounts shown in Figure 8 are per IT or security professional in an organization, so for organizations with multiple professionals, the annual cost currently incurred for dealing with phishing only increases. For example:

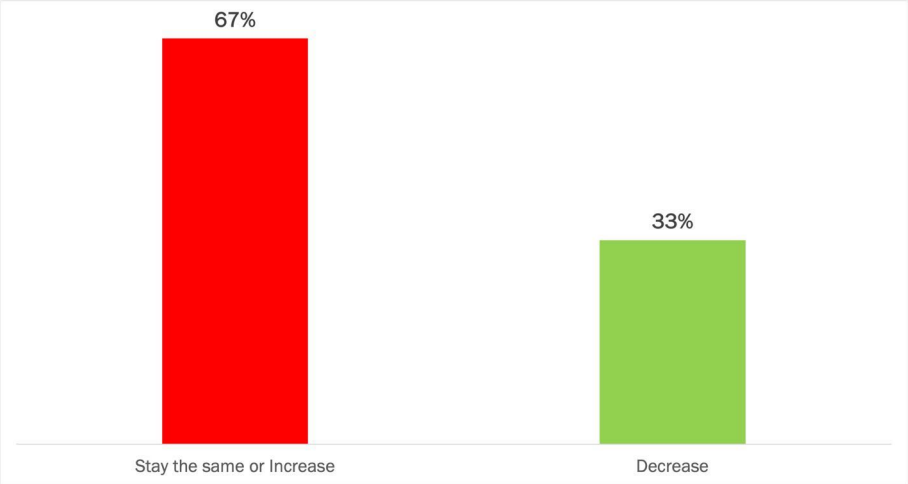
- An organization with five IT and security professionals is currently paying $228,630 of the annual salary and benefits paid to handle phishing.
- An organization with 10 IT and security professionals is paying $457,260 per year to handle phishing.
- An organization with 25 IT and security professionals is currently paying $1,143,150 per year to handle phishing.

Dealing with phishing consumes one third of the total available work hours available to IT and security teams.

EXPECTED CHANGE IN TIME SPENT PER WEEK

Most respondents expect the impact of phishing on their IT and security teams to get worse over the coming 12 months, with 67% expecting the time spent on phishing per week for IT and security teams to stay the same or increase. See Figure 9. This will drive up the proportion of annual salary paid to each IT and security professional for handling phishing.

Figure 9
Expected 12-Month Change in Time Spent Per Week on Phishing
Percentage of respondents



Source: Osterman Research (2022)

COSTS WE HAVE IGNORED

We have focused exclusively on the direct, quantifiable cost of phishing within an organization as incurred for staff time by IT and security professionals. We have not included opportunity costs of IT and security staffers, nor indirect but consequential costs. These represent the costs of successful phishing attacks that compromise account credentials, corporate data, and lead to stolen and misdirected funds. In combination, the following incur costs that are orders of magnitude greater than the direct costs profiled above:

- **Data breach notification costs**
  Email, postage, and phone call notifications to customers affected by a data breach.
- **Loss of customer trust**
  Lost sales as affected customers and disgruntled prospects shop elsewhere to avoid doing business with a tarnished organization.
- **Loss of corporate reputation and market value**
  Market value decreases on market exchanges in response to news about poor defenses and resultant breaches.
- **Regulatory fines**
  In a growing set of jurisdictions, regulatory fines are levied on organizations with insufficient technology and organizational protections against common security threats.

Indirect but consequential costs of successful phishing attacks incur costs orders of magnitude higher than only considering the direct costs.

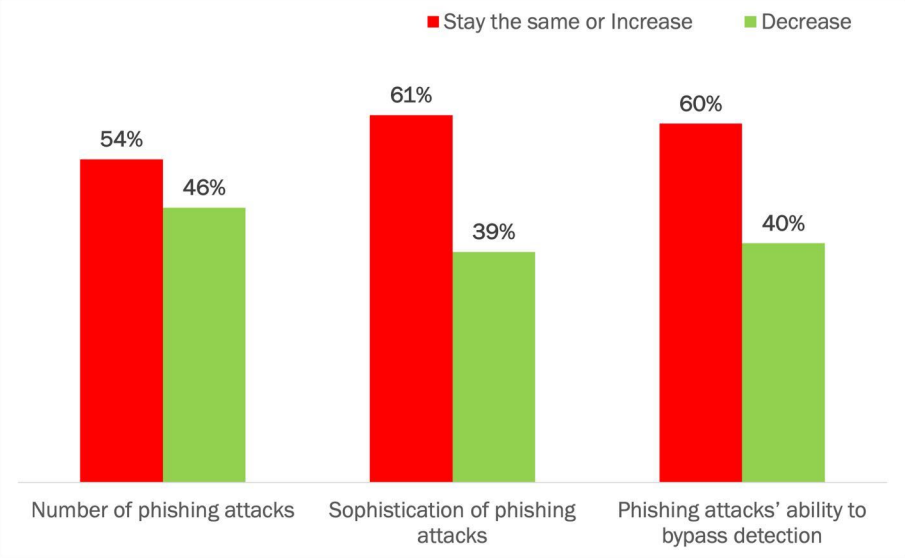
The Outlook for Phishing

Phishing is expected to remain a problem over the coming 12 months, with one worrying development the spread of phishing to new communication and collaboration tools.

PHISHING ATTACKS REMAIN A PROBLEM

We asked respondents to indicate their expectation about what will happen with three characteristics of phishing attacks over the next 12 months: the number, the sophistication, and the ability to bypass traditional email security detection technologies. In a significant departure from how respondents scored these changes over the past 12 months (see Figure 2 on page 4), twice as many expect all three to decrease over the next 12 months (see Figure 10).

Figure 10
Expected Dynamics of Phishing Attacks Over the Next 12 Months
Percentage of respondents



Source: Osterman Research (2022)

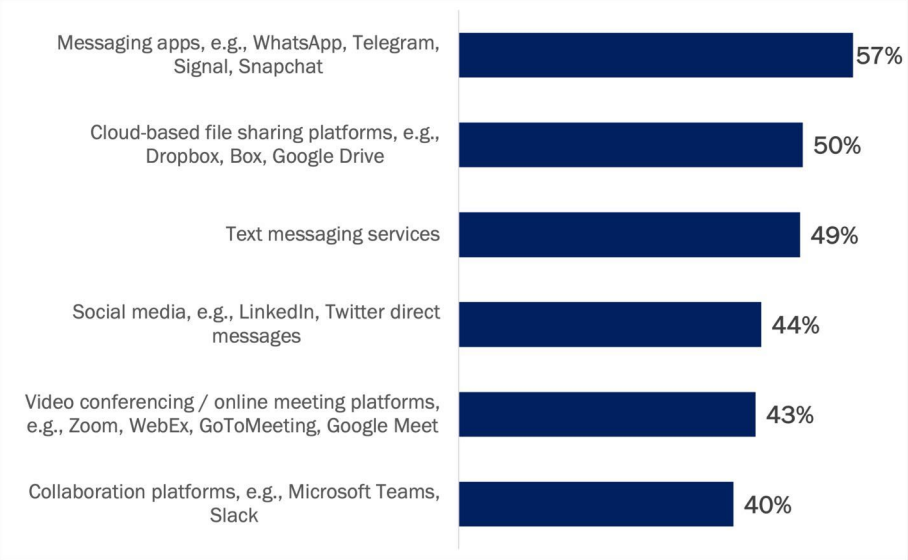
Given the question is about characteristics that are independent of the defenses employed by organizations, this expectation feels misplaced. Because phishing attacks will almost certainly become more numerous, more sophisticated, and better able to bypass traditional email security detection, a better interpretation of the data presented in this figure is that it indicates the desire of how respondents' organizations want to respond to the phishing threat and not the nature of phishing attacks themselves.

Most organizations anticipate that the phishing threat will get worse, and many would like to be better equipped to deal with it.

PHISHING IS ALREADY SPREADING TO OTHER TOOLS

A worrying development is the spread of phishing messages to tools beyond email, such as messaging apps, cloud-based file sharing platforms, and text messaging services. At least half of respondents indicated they are already seeing phishing attacks in these three communication and collaboration tools beyond email, and two in five respondents are seeing phishing attacks in social media, video conferencing/online meeting platforms, and collaboration platforms such as Microsoft Teams and Slack. As phishing spreads to these new tools—often driven by account credential compromise—IT and security professionals will have to spend even more time addressing threats and seeking to eradicate threat actors from their other services. See Figure 11.

Figure 11
Phishing Attacks Reaching End Users in Communication and Collaboration Tools
Percentage of respondents



Source: Osterman Research (2022)

Organizations are already seeing phishing spread to tools beyond email—increasing the number and sophistication of phishing threats.

Conclusion

Phishing continues to represent a time-intensive and costly problem for organizations. The number of phishing attacks is expected to increase over the next 12 months, along with attack sophistication and continued detection bypass capabilities. Organizations are also seeing phishing attacks spread to new tools beyond email. Organizations wanting to free up cybersecurity staff time for more strategic initiatives and reduce their expenditure on addressing phishing attacks should be looking for more capable solutions that detect and stop more phishing attacks, offer detection of advanced polymorphic and nested threats, and protect communication and collaboration tools via a holistic solution rather than being limited to protecting email only.

About IRONSCALES

IRONSCALES is a leading email security company focused on fighting back against today's modern phishing attacks. Our self-learning, AI-driven platform continuously detects and remediates advanced threats like Business Email Compromise (BEC), credential harvesting, Account Takeover (ATO) and more. We believe our powerfully simple email security solution is fast to deploy and easy to manage and keeps our customers safe.

Founded in Tel Aviv, Israel in 2014 by alumni of the Israel Defense Force's elite Intelligence Technology unit, IRONSCALES is headquartered in Atlanta, Georgia. We are proud to support thousands of customers globally with our award-winning, analyst-recognized platform.

Visit www.ironscales.com to learn more.

www.ironscales.com

@IRONSCALES

Methodology

This white paper was commissioned by IRONSCALES. Osterman Research surveyed 252 IT and security professionals in the United States in June 2022 on how their organization handled the threat of phishing.

Roles	
IT security manager or IT security team lead	40%
IT manager or IT team lead	29%
Email security manager or email security team lead	16%
Security manager	8%
Email security administrator	5%
SOC manager or SOC team lead	1.2%
SOC analyst	0.4%

Industry	
Technology	39%
Energy/Utilities/Oil/Gas/Minerals/Mining	10%
SaaS/Software	8%
Education	6%
Manufacturing	5%
Life sciences (Pharmaceuticals/Medical/Biotech)	5%
Construction/Architecture/Engineering	4%
Financial Services/Banking	3%
Healthcare	3%
Insurance	3%
Chemicals	3%
Aerospace/Defense	2%
Logistics/Transportation	2%
Professional Services (e.g., Legal, Marketing, Real Estate)	2%
Retail/Distribution	2%
Consumer Products	2%
Food/Beverage	1.3%
Government	0.4%
Non-profit	0.4%
Media/Entertainment	0.4%