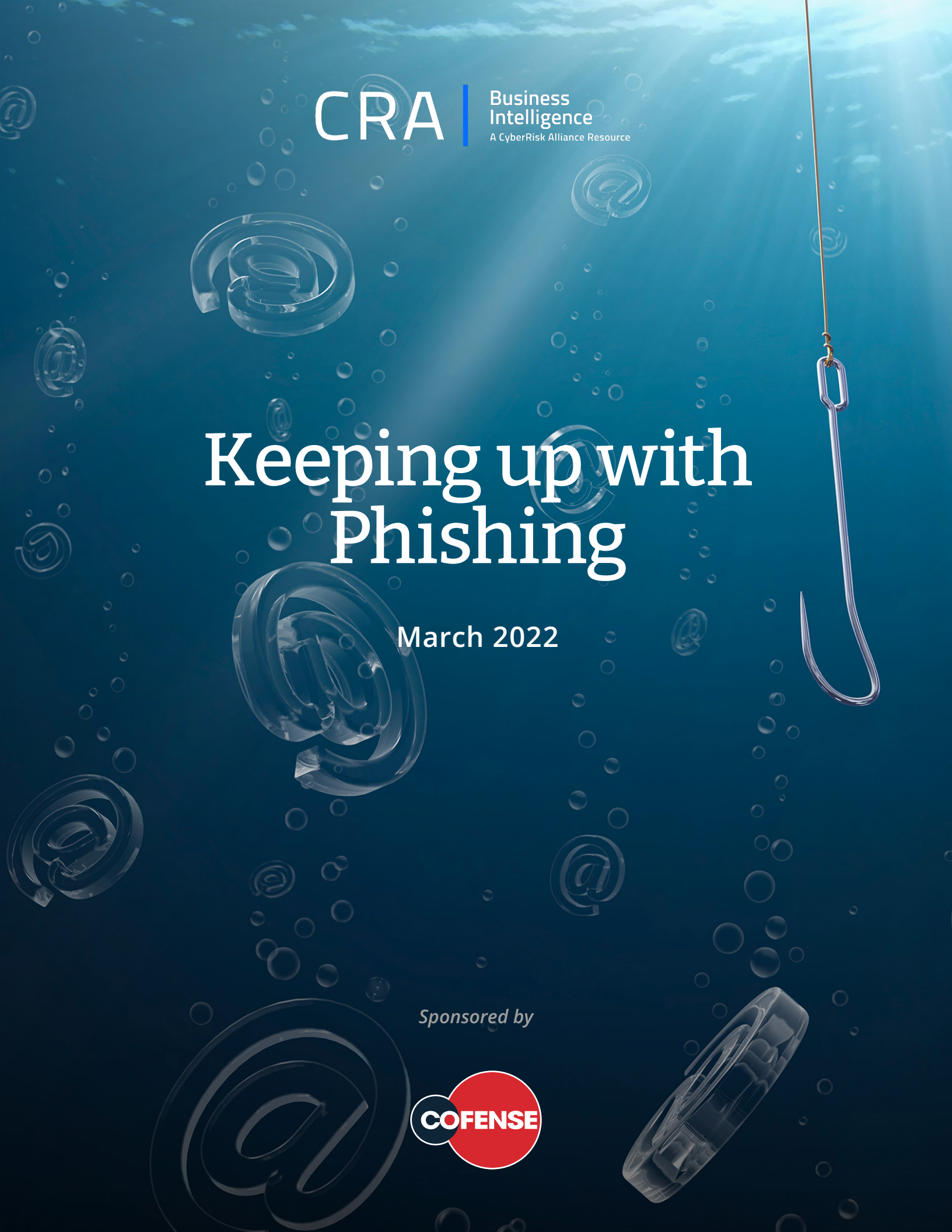

CRA
Business Intelligence
A CyberRisk Alliance Resource
Keeping up with Phishing
March 2022
Sponsored by
COFENSE

Keeping up with Phishing

FINDINGS FROM A 2021 RESEARCH STUDY

BACKGROUND

We are at a crucial juncture in phishing defense. The impact of the COVID-19 pandemic made it clear that organizations were unprepared for a worldwide data security crisis. Companies were forced into digital transformations and employees were required to operate remotely.

This unanticipated disruption to operations put extensive pressure on security teams while companies focused on business continuity rather than security compliance. Organizations were forced to adapt to new and more sophisticated phishing attacks. Many companies that were unable to adapt and defend against the quickly evolving attack vectors and tactics learned the hard way that basic security defenses were inadequate.

It was not just technological challenges security teams faced; finding the right mix of products and services that match with the expertise of the on-staff and contracted security teams continues to be a challenge.

CyberRisk Alliance explored the impact in the spring of 2021 by surveying security professionals about their struggles. We repeated the survey in the third quarter of the year and explore the differences and similarities in this report.

Two years in, the pandemic's unpredictable twists and turns have many continuing to work remotely, and security teams must continue to deal with the amped-up threats that come with it.

"Even advanced organizations are struggling to get orchestrated as tight as they'd like. At some point automation fails, and a phishing email makes it into the organization. The challenge is how do you become aware your automation system failed, and then what are you going to do about it?"

– Aaron Higbee Co-Founder & CTO, Cofense

RESEARCH METHODOLOGY

The data and insights in this report are based on two online surveys: one conducted from September-November 2021 among 351 IT and cybersecurity decision makers (69%) and practitioners (31%) from large organizations across North America, Europe, Middle East, and Asia/Pacific, and the same survey conducted in April/May 2021 among 353 respondents with similar profiles. Respondents from both surveys were employed in a variety of industries with most from the manufacturing, financial services, retail, healthcare, high tech/IT, education, and government/public sectors. The study was underwritten by Cofense, a provider of intelligent phishing defense solutions.

Survey objectives included identifying organizations' prioritized cybersecurity strategies concerning phishing defenses, tactics, and focus areas. The surveys also explored spending, phishing and malware trends, the number and types of phishing incidents, and the impact of phishing attacks. Respondents provided their responses to structured survey questions as well as various open-ended questions.

EXECUTIVE SUMMARY

Overall, nearly half of all respondents experienced an increase in phishing in Q3 2021 (significantly lower than Q1 2021) while about one in four experienced the same frequency since Q1. The average number of phishing incidents for those that experienced an incident in the past 3 months was 5 (the same as Q1). The numbers will continue to fluctuate, but that matters little, since it only takes one successful phishing attempt to cause a lot of damage.

Ransomware continues to be the top phishing incident experienced by half of all respondents.

Respondents say they are still struggling to keep up with phishing. Once phishing has been identified, it takes an average of 1.7 hours to investigate and remediate, up slightly from an average of 1.3 hours in Q1.

Managing work-from-home/remote employees was significantly more likely to be a top challenge for organizations in Q3 compared to Q1, while establishing a cybersecurity culture was significantly less likely to be a challenge.

Most respondents expect phishing attacks will become more effective in the coming year. Accordingly, many have stepped up their responsiveness to phishing since Q1 by increasing employee awareness training, email security solutions, and phishing risk assessment tools and software/platforms.

In Q3, some of the desired improvement in tools included protection of data using cryptographic controls, proactivity surrounding new and upcoming threats, more awareness newsletters and self-service customization of training materials, real-time analytics, feedback on how many cyber threats are thwarted, penetration testing, and automatic repair of high-risk vulnerabilities.

Key findings from the study:

- In Q3, ransomware remained the top phishing incident, experienced by half of all respondents.
- The average number of phishing incidents for those that experienced an incident in the past 3 months was 5 (the same as Q1 2021).
- Phishing represented an average of 29% of all cybersecurity incidents in Q3 (compared to 32% in Q1).

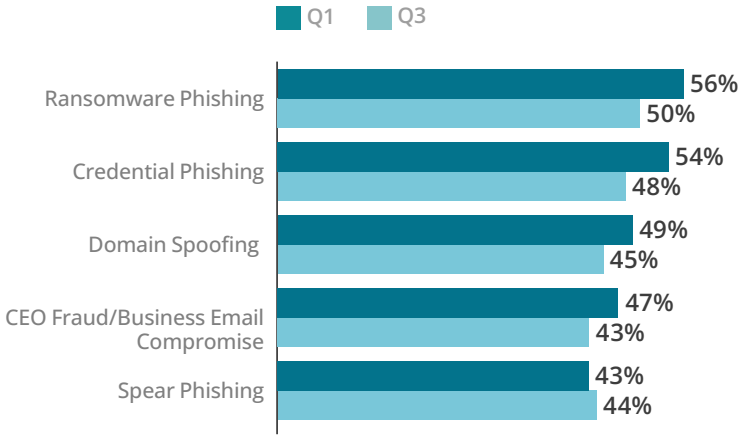
- Nearly half experienced an increase in phishing in Q3 (significantly lower than Q1); about one in four experienced the same frequency of phishing since Q1.
- Email attachments and links were the top sources for phishing, accounting for about one third of all phishing incidents (slightly more compared to Q1).
- Financial loss remains the top impact of phishing incidents; overall, Q3 impacts remained similar to Q1.
- On average, slightly less than one-third of 2021 IT budgets in Q3 were spent on phishing software/technology (similar to Q1).
- Organizations adopted more defenses in Q3; including increased employee awareness training, email security solutions, and phishing risk assessment tools and software/platforms.
- Compared to Q1, Q3 phishing responsiveness significantly increased for employee awareness training, internal communications, and incident response team activation.
- Phishing remediation time went up slightly in Q3 to 1.7 hours vs. 1.3 hours in Q1.
- Rapid reporting, increased user awareness, and reduced response time remain the top benefits of phishing defense software/technology in Q3.
- Roughly half (52%) of respondents believed they are "very" or "extremely" effective in responding to phishing (similar to Q1).
- In Q3 (vs. Q1), managing work-from-home/remote employees was significantly more likely to be a top challenge, while establishing a cybersecurity culture was significantly less likely to be a challenge.
- In Q3, more than half of all respondents said they struggled to stay ahead of the phishing volume, and most (56%) believed phishing attackers will be more effective in the next 12 months.

A VARIETY OF PHISHING TACTICS

In Q3, ransomware remained the top phishing incident, experienced by half of all respondents. Many also said their organizations suffered credential-based phishing, domain spoofing, and phishing that targeted their CEOs and business email accounts, and spear phishing. The number of those affected by these attacks changed little from the spring of 2021.

Phishing Incidents Experienced in Last 3 Months

Percentage of respondents indicating one or more incidents



Q: Please provide the following information about the number of incidents in the past 3 months: Type of Phishing Incident

Ransomware gangs have taken their attacks to a dangerous new level in recent months, targeting ubiquitous software used by business, government agencies and critical infrastructure and revealing multiple vulnerabilities in the software supply chain.

Among them was the *SolarWinds attack*, discovered at the end of 2020. In May 2021, a ransomware attack crippled the *Colonial Pipeline* for nearly a week, sending millions along the U.S. East Coast scrambling for gas. Also in May, the *JBS* meat packing company, which supplies more than one-fifth of all beef in the United States, was forced to halt operations after its plants were pushed offline. In July, the networks of at least 200 U.S. companies were paralyzed when the *REvil ransomware syndicate* attacked software supplier *Kaseya*.

Phishing themes mentioned in Q3

- Tried to access applications
- Used ransomware to kidnap and extort our servers
- Threats to divulge company's private information
- Emails containing offers for certain products or account of a partnered company
- The website of the company got hacked and the credentials of the employees were hacked
- Employees received mail that claimed to be from the CEO
- Fake emails asking to change password
- Unauthorized granting credentials to other people
- Tried to redirect to fake site
- Fake email sent to some staff to change their login details
- Email pretending to be for a member of staff
- Important information about employee benefits
- They faked our website to steal customers details
- Only one character difference, they used our website
- Phishing campaigns themed around COVID-19
- Fake notifications about rewards
- Email requesting passwords to be changed

COMPANIES AVERAGING 5 INCIDENTS IN 3 MONTHS

Among those who experienced one or more phishing incidents in the past three months (i.e., 50% of all respondents), the overall average number of phishing incidents was 5, as shown in the following chart.

Average Number of Phishing Incidents:

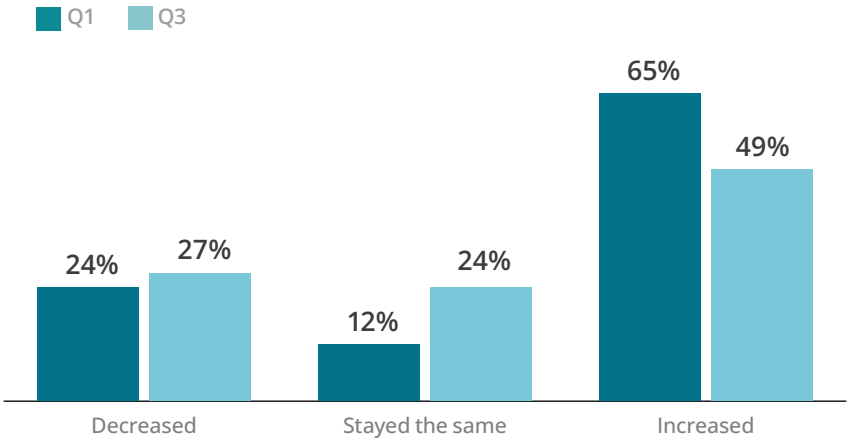
	Q1 2021	Q3 2021
Ransomware	4.3	4.5
Credential Phishing	5.3	5.3
Spear Phishing	4.5	4.5
CEO Fraud/Business Email	5.4	4.7
Domain Spoofing	6.0	6.4
AVERAGE	**5.0**	**5.0**

Looking at the number of incidents experienced over a full year, the rate of cyber attacks organizations attributed specifically to phishing was 29% between fall 2020 and 2021, compared to 32% between spring 2020 and 2021.

Phishing Incidents	Q1	Q3
	32%	29%

Nearly half experienced an increase in phishing in Q3 and about one in four experienced the same frequency of phishing since Q1:

Change in Phishing Frequency Since Previous Quarter



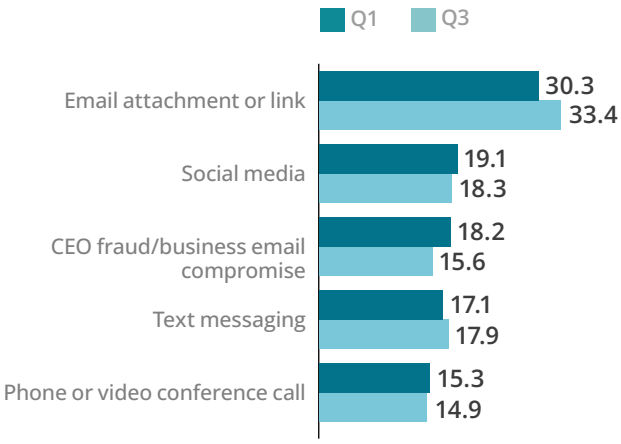
Q: How has the frequency of phishing incidents changed since the previous quarter?

EMAIL STILL A FAVORITE VECTOR

Malicious email links accounted for about one third of all phishing incidents (slightly more compared to Q1). Meanwhile Q3 survey respondents reported that nearly 16% of their phishing emails were those targeted to CEOs while nearly 18% of their phishing attacks originated from text messaging.

Phishing Origination

Average percentage of phishing incidents



Q: In the last 3 months, approximately what percent of all your organization's phishing incidents have originated from the following?

In 2022, attackers also ramped up their social media efforts:

In *one such case*, researchers uncovered a *phishing campaign* that hijacks corporate Instagram accounts along with the accounts of influencers who have a large number of followers.

In text messaging attacks, *threat actors increasingly leverage fake QR codes* to steal users' login credentials and financial data. Stolen financial information could then be used by attackers for fund withdrawals, according to the FBI.

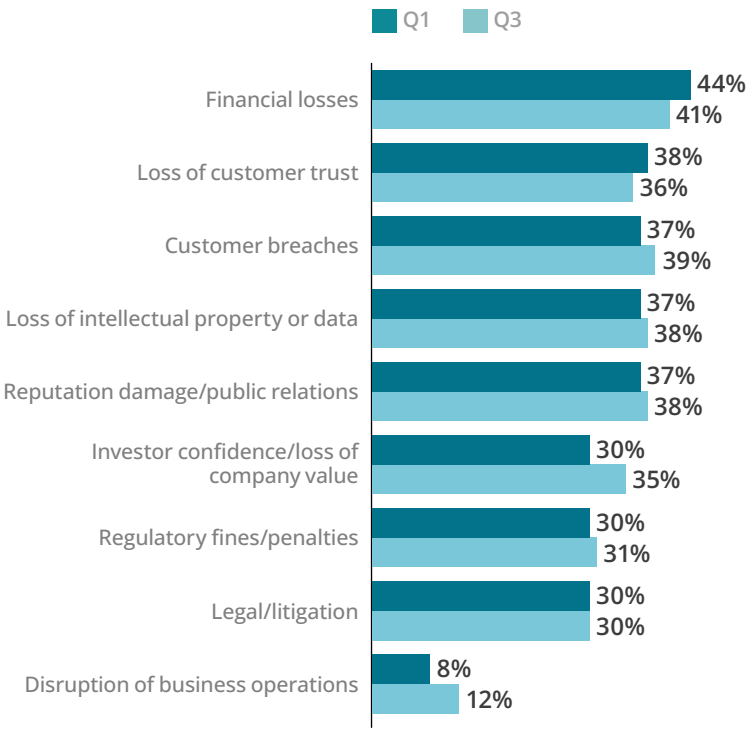
"Businesses use QR codes legitimately to provide convenient contactless access and have used them more frequently during the COVID-19 pandemic. However, cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use," the FBI said in a January statement. "Smartphone users have been urged to properly check URLs after QR code scanning, exercise care in inputting credentials and financial data on websites accessed through QR codes, and refrain from using QR codes to download mobile apps, as well as avoid QR code scanner downloads."

Respondents said they were grasping for better tools and techniques to combat these phishing types, particularly when it comes to better protecting data so attackers can't get to it even if someone clicks on a malicious link. "We need protection of the data using cryptographic controls for data at rest and data in transit," said one respondent from a U.S. healthcare organization.

TOP IMPACTS: FINANCIAL LOSS, ERODED TRUST

Financial loss remains the top impact of phishing incidents. Overall, Q3 impacts remained similar to Q1: 41% in the fall compared to 44% in the spring. The top impact for 36% of respondents was an erosion in how much their clients trusted them to protect their personal information, roughly the same (38%) in the spring. Thirty-nine percent experienced a customer data breach in Q3, nearly the same (37%) in Q1. A similar number of respondents experienced loss of intellectual property and other data, and bad press while 31% were forced to pay regulatory penalty fines.

Impacts Experienced as a Result of Phishing Incident



Q: Which of the following has your organization experienced as a result of phishing incidents? Select all that apply.

SC Media has reported extensively about these very impacts:

December 2021: A phishing attack and subsequent email account takeover at *Monongalia Health System* potentially compromised the protected health information of 398,164 patients. The incident affected Mon Health and two affiliated West Virginia hospitals, Monongalia County General Hospital Company and Stonewall Jackson Memorial Hospital Company. The investigators determined the impacted protected health information tied to patients and the Mon Health employee health plan included names, Medicare Health Insurance Claim Numbers, some Social Security numbers, contact information, patient account numbers, insurance plan member ID numbers, medical record numbers, dates of service, and other medical data.

August 2021: *Orlando Family Physicians* (OFP) notified 447,426 patients that their data was potentially compromised during a successful phishing attack in April. The breach tally makes the OFP incident among the *10 largest reported in health care* in 2021. Investigators found three additional employee emails had been accessed by the hacker and quickly terminated access to the affected accounts. By May 21, Orlando Physicians determined the attacker likely accessed the personal information contained in the accounts, though it appears the attack was designed to commit financial fraud against OFP.

STAGNANT SPENDING ON PHISHING DEFENSE

On average, slightly less than one-third of 2021 IT budgets are spent on phishing software/technology . It's likely that organizations have already invested in a variety of phishing tools in recent years. Time will tell if those investments are enough.

Average Percent of IT Budget Spent on Phishing

Q1	Q3
33%	31%

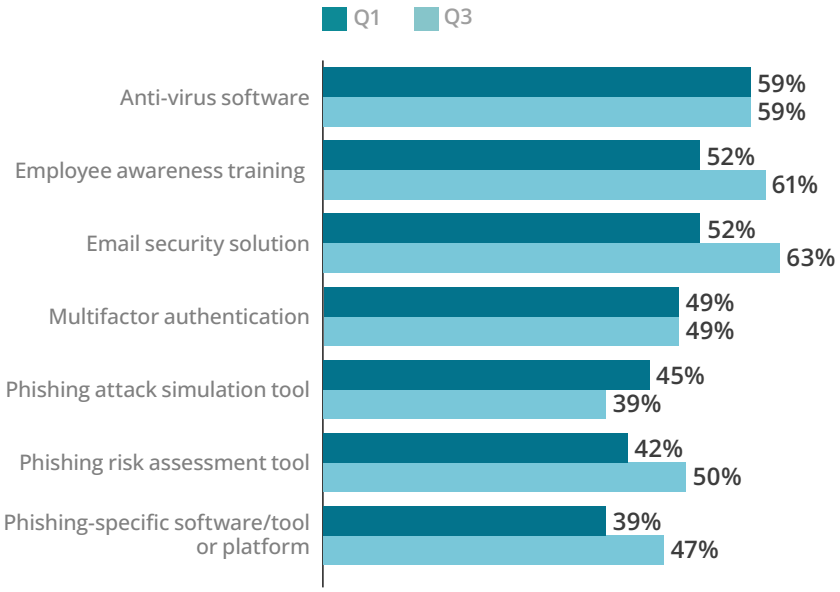
That said, security experts have increasingly recommended that companies start spending more on other things to lower their phishing risk. At SC Media's 2021 *Finance eConference* in December, a trio of guest panelists said that insurance requirements, business and reputation loss, and solution viability are among the key factors that finance-sector companies must consider when analyzing the cost of potentially implementing anti-phishing solutions and practices.

"A defense-in depth strategy or multi-layered approach generally will have a much greater payback than the potential downside if you have [a] data breach," said conference panelist Michael Bruemmer, vice president of data breach resolution and consumer protection at Experian.

RESPONDENTS EAGER FOR MORE PHISHING DEFENSE SOLUTIONS

Despite stagnant spending in 2021, security teams continue to make the usual investments. In fact, organizations adopted more defenses in Q3, including increased employee awareness training, email security solutions, and phishing risk assessment tools and software/platforms.

Used to Defend Against Phishing Threats



Q: Which of the following are used at your organization to defend against phishing threats? Select all that apply.

Respondents said that when it comes to anti-phishing tools, they are indeed eager for additional defenses. "We lack live real time analytics at this point," according to a survey respondent from a U.K. manufacturing company.

Amid the struggle, respondents continue to see benefits in phishing defense/software technology. Indeed, rapid reporting, increased user awareness, and reduced response time remain the top benefits of phishing defense software/technology in Q3.

TOP BENEFITS OF PHISHING DEFENSE SOFTWARE/TECHNOLOGY (Q3)

57% Rapid reporting of phishing attack directly from user email

56% Increases user awareness about phishing

53% Reduces security team's response time or resources to detect or remediate

52% Reduces response time or resources to respond to phishing

47% Educates users about phishing responses

Thanks to those technologies, roughly half (52%) of respondents believe they are now "very" or "extremely" effective in responding to phishing, a similar self-assessment as we saw in the spring survey results:

REMEDIATION STILL TIME CONSUMING

While that's certainly good news, it doesn't remove the suffering respondents experience when it comes to wasted time.

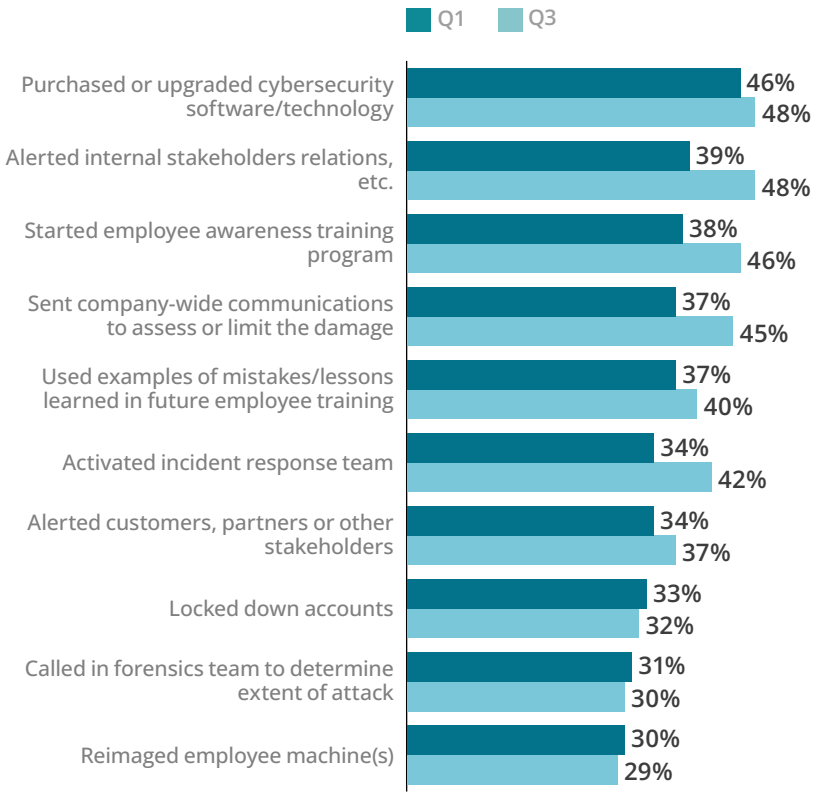
Phishing remediation time went up slightly in Q3 to 1.7 hours vs. 1.3 hours in Q1. Most believe responding to phishing is too time consuming, with nearly one in five respondents reporting a response time of 3 hours or more.

Average Time to Respond to a Phishing Incident	Q1	Q3
	1.3 hr.	1.7 hr.

When a user clicks on an infected link, the malware strains immediately try to find user credentials to move deeper into the network seeking data to sell or to steal, or otherwise move laterally until locating the requisite credentials or a hole in defenses. Every second counts. The clock starts ticking when a security analyst identifies the malicious code or when the user alerts the security team that they clicked on a potentially infected link, image or page. This could well be minutes or months after the actual infection, depending on when it is officially acknowledged as a malware incident.

Perhaps because remediation remains such a time eater, companies have more recently responded with more urgency to the need for employee awareness training, activating an incident response team, and more.

Steps Taken After Phishing Incident



Q: Which of the following steps has your organization taken as a result of a phishing incident? Select all that apply.

While security pros tend to favor technological improvements that make identifying, intercepting and remediating threats faster and more efficient, it always comes down to the one unknown that determines how well the company can defend against phishing: People. When asked about steps taken after an incident, 46% of respondents started an employee awareness training program, up from the 38% who had done so in Q1. Forty percent said they started to use examples of mistakes/lessons learned in that training, compared to 37% in Q1.

No matter how comprehensive a training program is and how effective software is at identifying potential threats, if users click on bad links, images or other triggers, malware and ransomware can and will get into an organization's network.

Training, of course, is the foundation on which all employee-focused cybersecurity is based. Unsurprisingly, a vast majority of respondents believe employee training is equally important as technology in preventing phishing incidents. Survey findings suggest that training should be directed to both technical and non-technical staff at all levels, from entry-level employees to senior management. In describing specific employee training scenarios, respondents mentioned the following requirements for their organization:

- Pre-training of new employees
- Proper training for management teams
- In-depth training to the staff of their IT departments
- Employee training tools to help identify risks and teach them to recognize phishing attempts

IN THEIR WORDS

What respondents had to say:

"We are not receiving a lot of feedback on how many cyber threats are thwarted unfortunately."

–Respondent from a U.S., manufacturing company

"Training of employees must be controlled internally by us."

–Respondent from a German retailer

"We need cloud killing, automatic repair of high-risk vulnerabilities, abnormal login reminder, anti- password brute force cracking, and physical examination reinforcement."

–Respondent from a UAE retailer

CONCLUSIONS

The lessons learned from the Q3 survey are the same as those gleaned from the Q1 survey:

Defending against phishing attacks is a never-ending effort for one simple reason: It works. Attackers know that a well-crafted phishing email eventually will find someone willing to click on it. Ransomware attacks raise the stakes.

Security experts anticipate that new attacks will be far more sophisticated in the coming year and more aggressive than we are seeing now. To address those concerns, organizations must raise the bar for employee training and education to make it more effective.

Respondents acknowledged their need for an extensive risk assessment of their environments, threat detection and threat intelligence, along with a need for greater transparency about which phishing attacks are being identified and how to identify them if they arrive in employee email boxes. While ransomware and credential phishing are currently the top two phishing vectors, security teams and senior management must continue to be vigilant about other popular phishing attacks, such as the ever-popular business email compromise — commonly called CEO fraud — domain spoofing and spear phishing.

Attackers rotate their attack vectors to try and keep defenders wrong-footed, and organizations that can maintain strong defenses for phishing and similar social engineering attacks will emerge as the victors.

ABOUT CYBERRISK ALLIANCE

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. More information is available at *http://cyberriskalliance.com/*.

ABOUT COFENSE

Cofense®, the leading provider of intelligent phishing defense solutions, is uniting humanity against phishing. The Cofense suite of products combines timely attack intelligence on phishing threats that have evaded perimeter controls and were reported by employees, with best- in-class security operations technologies to stop attacks faster and stay ahead of breaches. *www.cofense.com*.

