Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **March 2024**
Commissioned by **IRONSCALES**

Fortifying the Organization Against Image-Based and QR Code Phishing Attacks

Executive summary

A striking paradox lies at the heart of modern email security. Despite high levels of confidence among organizations in their defensive capabilities and in their employees' and executives' ability to spot phishing emails, image-based and QR code phishing attacks continue to breach their defenses with unsettling frequency. This discrepancy between the perceived effectiveness of security protocols and the reality of ongoing infiltrations underscores a concerning gap in current cybersecurity strategies. As these emerging attacks grow increasingly complex, the need for a comprehensive reassessment of email security approaches becomes more urgent, challenging organizations to bridge the confidence-security paradox with immediate technical and training improvements.

This research explores how organizations are positioned to respond to new and emerging types of phishing attacks, and complements our recent investigations for IRONSCALES on the business cost of phishing and business email compromise attacks.

KEY TAKEAWAYS

- **Image-based and QR code phishing attacks are after account credentials and sensitive information**
  75.8% of organizations have been compromised by image-based and QR code phishing attacks over the past 12 months. Compromising account credentials (72%) and stealing sensitive information (70.6%) are the most common motives.
- **Key threat indicators are expected to get worse—especially those controlled by cyberthreat actors**
  60% of respondents believe the number, sophistication, and evasiveness of image-based and QR code phishing attacks will get worse over the coming 12 months, and yet these threat indicators are controlled by cyberthreat actors. Organizations must respond by fortifying their email security defenses through augmentation, optimization, or a wholesale change.
- **Startling misalignment between the assertion and reality of efficacy**
  More than 70% of respondents assess their current email security stack as highly effective at detecting image-based and QR code phishing attacks, yet only 5.5% of respondents were able to detect and block all image-based and QR code phishing attacks from reaching users' inboxes over the past 12 months. This misalignment is startling.
- **Training users and augmenting email security seen as the key investments**
  80% of organizations are emphasizing training users and augmenting their current email security stack as the two highest-ranked strategies to address image-based and QR code phishing attacks over the next 12 months.
- **Better cybersecurity awareness training and phishing simulations are essential**
  Organizations must continuously evolve their phishing simulation programs to mirror the latest phishing techniques observed, providing employees with practical and current examples they may see if the organization's technical measures fail. Some email security vendors are leveraging generative AI to craft micro-targeted phishing simulation tests optimized for each individual.

Emerging image-based and QR code phishing attacks are evading current email security defenses and tricking users.

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.

What's happening with emerging image-based and QR code phishing attacks

Emerging image-based and QR-code phishing attacks are top of mind as a new attack vector at most organizations, and that is no surprise due to attacks bypassing current email defenses. The threats are significant and expected to continue.

HIGH AWARENESS OF EMERGING TYPES OF PHISHING ATTACKS

Respondents indicate high awareness of all types of phishing attacks, with image-based phishing attacks and QR code phishing attacks ranking first and third-highest in awareness, respectively.

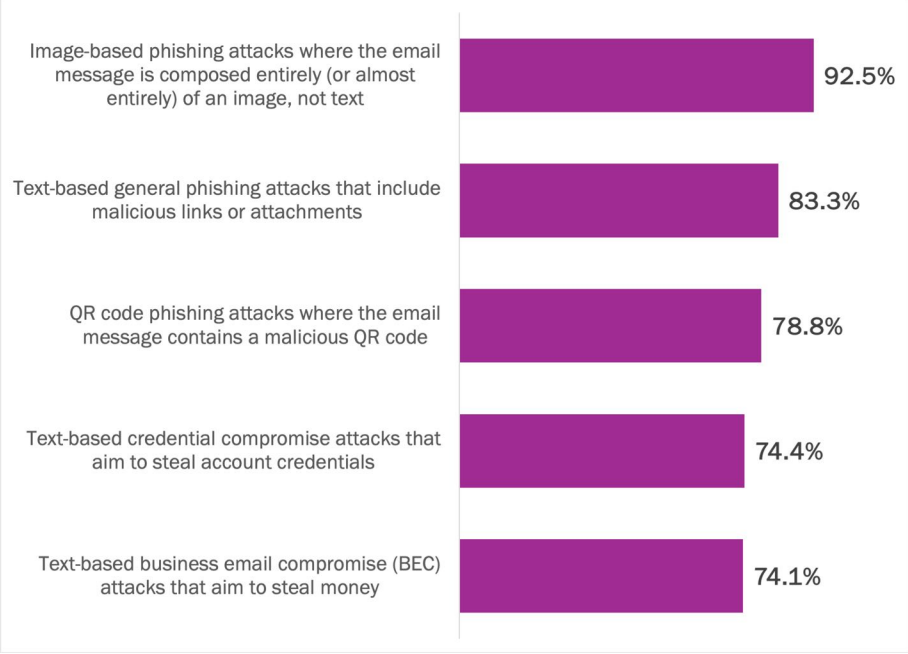
More than nine out of ten respondents are aware of image-based attacks being sent to people in their organization, and just under eight out of ten are aware that the same is happening with QR code phishing attacks. Currently, awareness of image-based phishing attacks is higher than general phishing attacks by email, and both emerging types of attacks have higher awareness than established text-based email phishing attacks emphasizing credential compromise and financial theft.

Cyberthreat actors are always on the lookout for less protected ways that allow them to evade email security defenses and have consequentially pivoted to embrace new image-based and QR code phishing attacks. With most organizations in this research finding themselves ill-prepared to deal with these new types of phishing attacks, awareness has spiked.

See Figure 1.

Cyberthreat actors have pivoted to new image-based and QR code attack methods as part of their ongoing crime strategy of finding less protected ways to get past email defenses.

Figure 1
Awareness of phishing attacks targeting their organization
Percentage of respondents



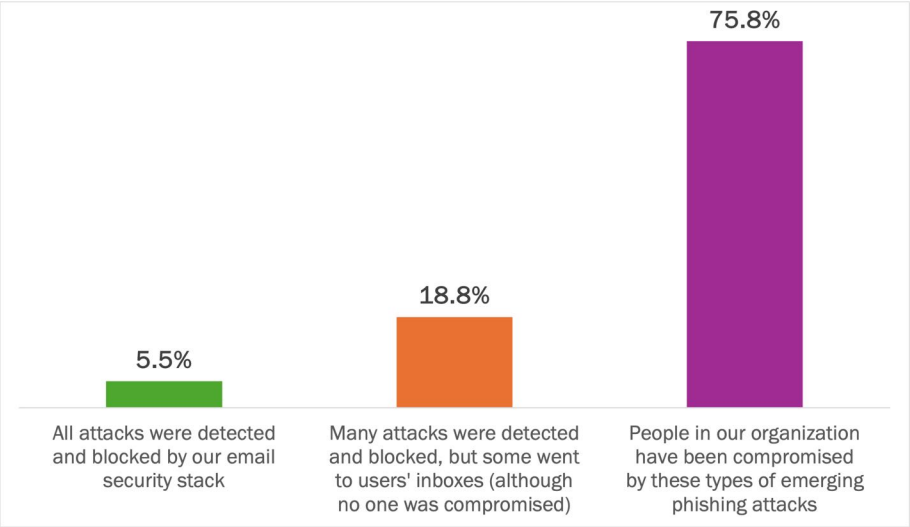
Source: Osterman Research (2024)

EMERGING PHISHING ATTACKS ARE BYPASSING CURRENT EMAIL DEFENSES

Emerging image-based and QR code phishing attacks have sailed unchallenged through the email security defenses at 94% of the organizations surveyed for this research. Once deposited into users' inboxes, training approaches used to raise awareness of cybersecurity threats have been insufficient to stop users from falling for the phish at 76% of the organizations surveyed.

See Figure 2.

Figure 2
Low efficacy of current email security stack and cybersecurity awareness training
Percentage of respondents



Source: Osterman Research (2024)

Only 5.5% of organizations in this research claim that they were able to detect and block all emerging types of phishing attacks so that none were released to users' inboxes. At a further 18.8% of organizations, while their email security stack did release phishing attacks to users' inboxes, no users fell for them. At these organizations, cybersecurity awareness training appears to have created sufficient skepticism of unexpected and abnormal email messages to stop the phish from succeeding.

When attacks were not stopped by their email security defenses, 76% of employees fell for new image-based and QR code phishing attacks.

ACCOUNT CREDENTIALS AND SENSITIVE DATA IN THE CROSSHAIRS

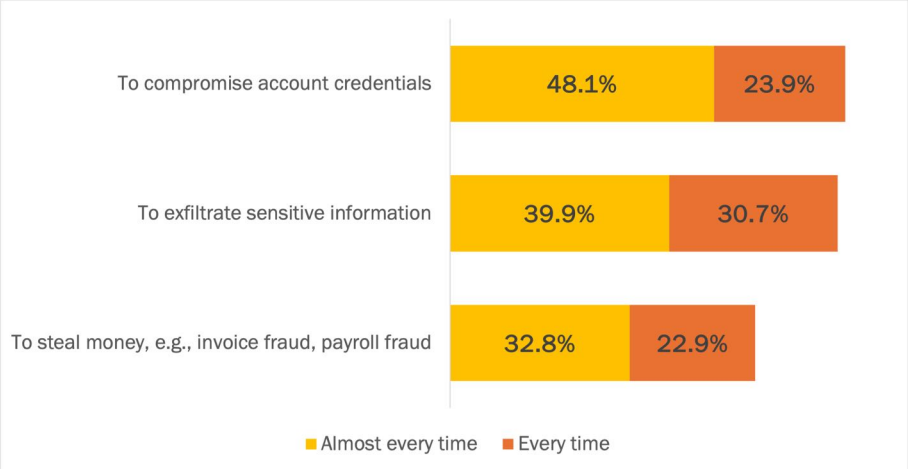
High-profile image-based and QR code phishing attacks have focused on compromising account credentials and sensitive data. For example:

- **Compromising credentials for Microsoft 365 accounts**
  Targeted victims receive an email containing a QR code with instructions requesting that they update and confirm the multi-factor authentication settings for their Microsoft 365 account. The cyberthreat actors capture these account credentials if a victim scans the QR code and enters their Microsoft 365 credentials in the fake Microsoft login page.
- **Exfiltrating sensitive information**
  Targeted victims are sent an email purportedly with updated details on their wages. The QR code inside the email links to a fake SharePoint login page. If an employee scans the code and enters their account credentials, the cyberthreat actors have access to everything in the SharePoint document libraries and sites the employee was able to access.
- **Stealing money via invoice and payroll fraud**
  A phishing email message contains no text, but rather an embedded image that is automatically displayed and looks just like a standard email message with text and instructions. Because the message is embedded in an image, standard analysis methods—including Natural Language Processing machine learning—often fail to identify the threats. The message in the image informs the victim that they are going to be charged for something they haven't ordered from a brand they are likely to be using, and to follow the instructions to phone the call center if they want to dispute the charge. Once they call, social manipulation ensues.

Cyberthreat actors seek sensitive data and account credentials through image-based and QR code phishing attacks.

These malicious outcomes are reflected in the motives reported by survey respondents, with compromising account credentials (72.0%) and exfiltrating sensitive data (70.6%) evident "almost every time" or "every time" in the attacks seen by respondents. Stealing money through invoice fraud or payroll fraud is in third place as a motive for image-based and QR code phishing attacks. See Figure 3.

Figure 3
Motives for image-based and QR code phishing attacks
Percentage of respondents indicating "almost every time" or "every time"

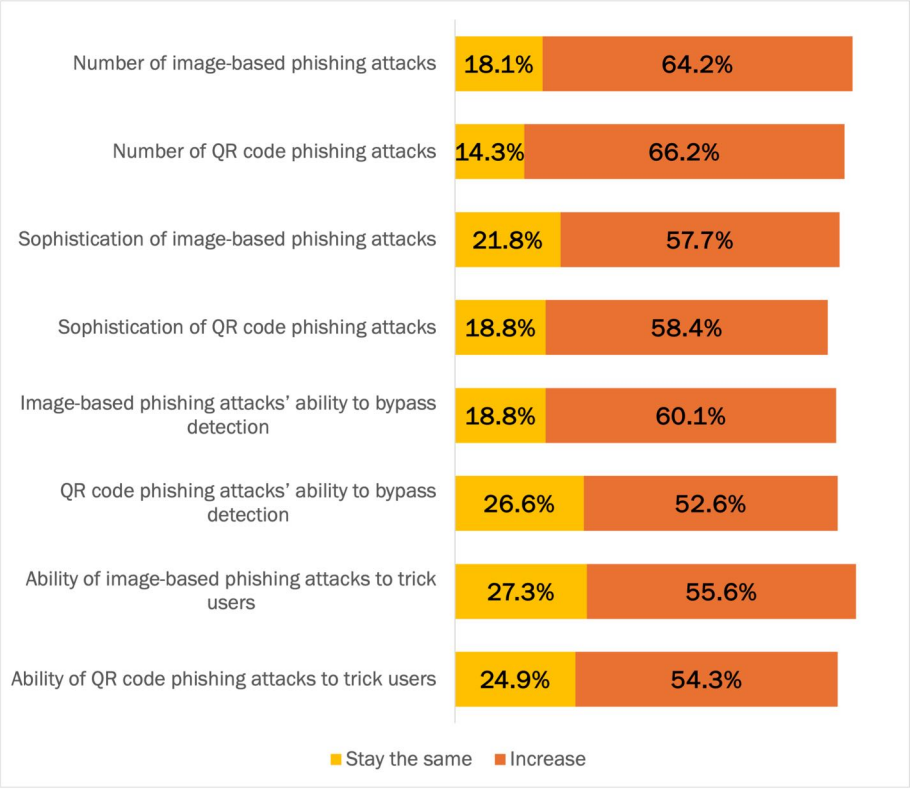


Source: Osterman Research (2024)

80% EXPECT CONTINUING HIGH THREAT FROM EMERGING ATTACKS

The threat from emerging image-based and QR code phishing attacks will remain high over the next 12 months. 80% of respondents expect the threat posed by four indicators to increase or stay the same across both types of phishing attacks (see Figure 4). Only 20% of respondents expect these threat indicators to decrease.

Figure 4
Expected change in threat indicators of image-based phishing attacks
Percentage of respondents



Source: Osterman Research (2024)

The threat posed by image-based and QR code phishing has not yet peaked—60% of respondents expect it to get worse over the coming year.

The bad news is that organizations have no control over three of the indicators: number (frequency), sophistication, and evasiveness. These indicators are controlled by cyberthreat actors, and the use of malicious generative AI (GenAI) services enables attacks at a faster cadence, with higher sophistication, and with elevated evasiveness to obfuscate the technical markings that render a message malicious.

What organizations must do in response, therefore, is to develop a strong technical defensive layer that stops increasingly frequent, sophisticated, and evasive image-based and QR code phishing attacks from getting through to users' inboxes. And this takes time to get right—either through augmenting the current email security stack, optimizing what is already deployed, or making a wholesale change.

For the fourth threat indicator above—the ability to trick users—organizations have a higher degree of proactive and preemptive control to educate and empower users on phishing threats and design supporting processes for testing and escalation. Stepping up the efficacy of the human barrier is essential in parallel with strengthening the technical foundations of email security.

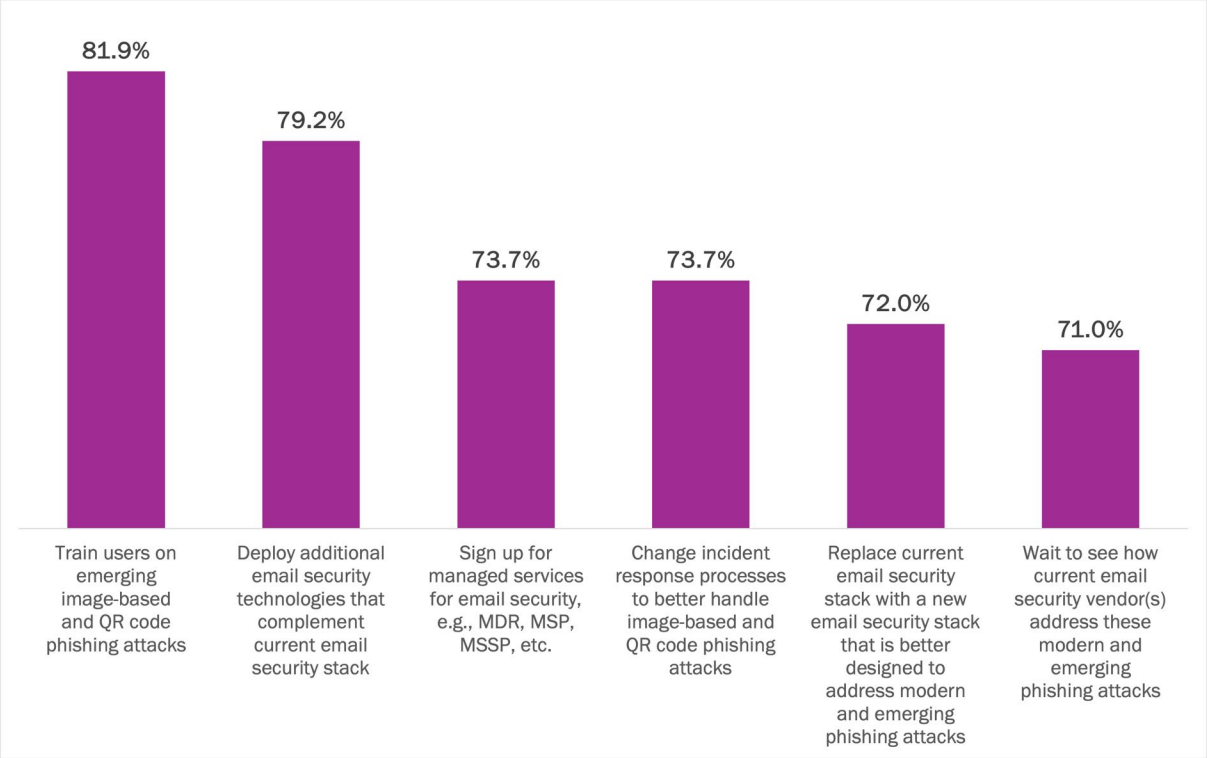
How organizations are responding to emerging image-based and QR code phishing attacks

The combination of better training and improved security technologies is seen as the key means of counteracting image-based and QR code phishing attacks. In this section, we look at what organizations need to do to move forward with planned strategic changes across fundamental people, technology, and process factors.

STRATEGIC CHANGES TO ADDRESS EMERGING PHISHING THREATS

The organizations in this research are planning a multi-pronged strategic response to shore up their defenses and strengthen their ability to respond to incidents—with the emphasis on training users and augmenting their technology for a multi-layered defensive posture. These emerging phishing attacks are bypassing current email security detection capabilities and tricking users into taking actions that incur security, financial, and reputational harm to their organization. See Figure 5.

Figure 5
Planned strategic changes to address emerging phishing attacks over next 12 months
Percentage of respondents indicating "very likely" or "extremely likely"



Source: Osterman Research (2024)

STRATEGY 1.
TRAIN USERS ON IMAGE-BASED AND QR CODE PHISHING ATTACKS

Training users on emerging image-based and QR code phishing attacks is the top-ranked strategic change in Figure 5—with 81.9% of respondents indicating they are "very likely" or "extremely likely" to embrace this strategy over the next 12 months. As an interesting correlation of this strategic intent, more than 80% of respondents answered a related question indicating that the importance of security awareness training in their organization would increase or stay the same over the next 12 months.

There are several aspects from our research to take into consideration when pushing ahead with this strategy.

Deliver role-specific and risk-contextualized training

A concerning gap exists in the confidence levels organizations have regarding their employees' ability to identify image-based and QR code phishing attacks. Specifically, one-third of organizations lack confidence in the detection skills of key departments such as human resources and finance, and among senior executives.

By contrast, confidence is somewhat higher within IT/security departments, with only 15% expressing doubts. However, this confidence drops dramatically for the broader employee base, with nearly half (46.8%) of organizations not confident in the phishing detection capabilities of general staff. See Figure 6.

Developing role-specific and risk-contextualized training for employees in these various groups is about protecting them from attacks, helping them to do their job securely (and productively), and warning them what to watch out for in their day-to-day interactions. The risks facing senior executives are different to those in finance and IT/security, and thus the training curriculum developed for each role group should reflect that.

The risks facing senior executives are different to those in finance and IT/security, and the training curriculum developed for each role group should reflect that.

Figure 6
Low confidence in groups for detecting emerging phishing attacks
Percentage of respondents indicating low confidence

Source: Osterman Research (2024)

Evolve phishing simulation programs to mirror the latest phishing techniques observed

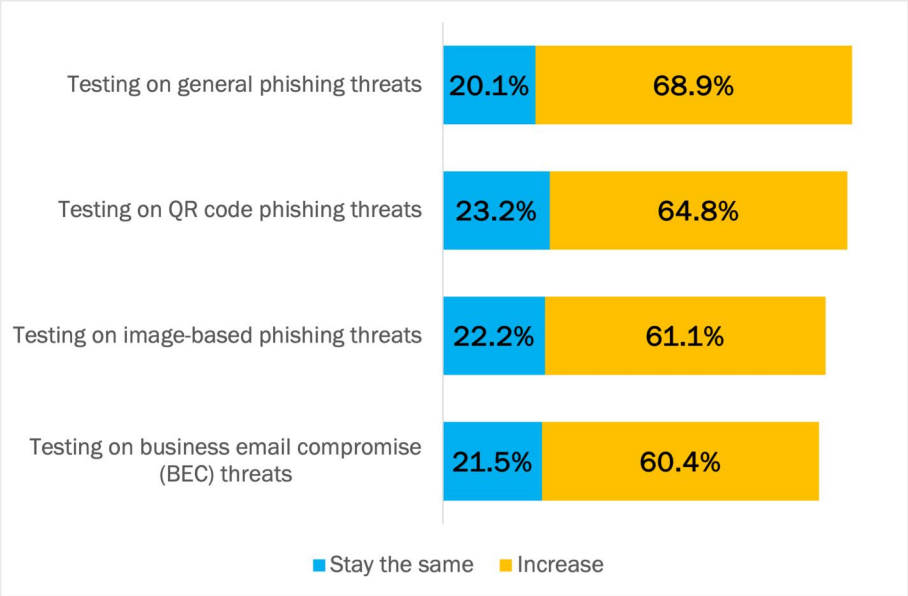
To enhance the effectiveness of cybersecurity training, it is imperative for organizations to continuously evolve their phishing simulation programs to mirror the latest phishing techniques observed. These simulations should mimic the most recent image-based and QR code phishing threats, thereby providing employees with practical and current examples they may see if the organization's technical measures fail.

To facilitate this for organizations, some email security vendors are starting to leverage GenAI to craft highly personalized phishing simulation tests that draw on the specific email traffic and behavioral patterns of individual employees. This enables organizations to move beyond generic phishing simulation tests that are easy to spot because they are contextually irrelevant to the person receiving them. Such innovations increase the relevance of phishing simulation messages to specific individuals and groups and provide highly targeted data assessing the likelihood of an employee falling for a deceptively plausible but malicious email message.

For the vast majority of organizations in this research, the importance of phishing simulation testing for all types of phishing threats is expected to increase or stay the same over the next 12 months. The expected change in importance for testing on general phishing threats is ranked highest (89.1%), followed very closely by the importance of testing on QR code phishing threats (88.1%) and image-based phishing threats (83.3%). See Figure 7.

Increase the plausibility of phishing simulation testing messages by using GenAI to craft test messages that are micro-targeted to each individual.

Figure 7
Expected change in importance of types of phishing simulation testing
Percentage of respondents

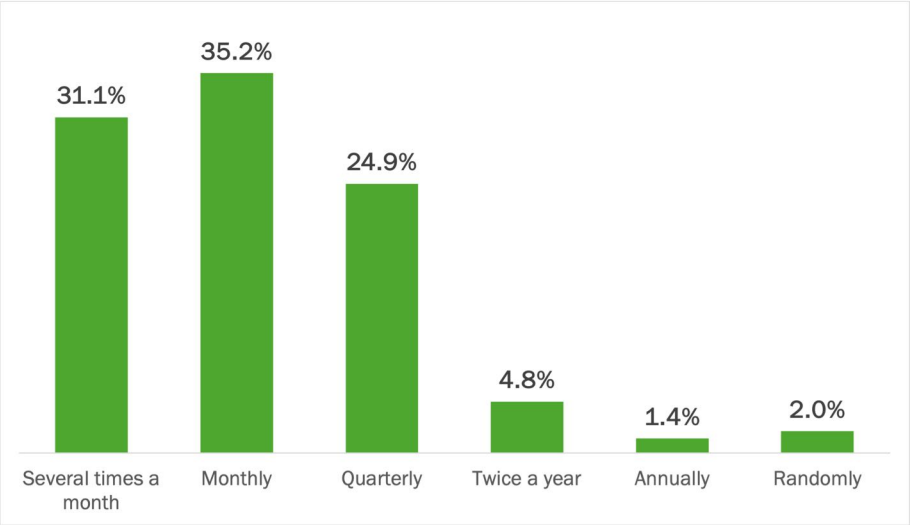


Source: Osterman Research (2024)

Increase training cadence on emerging phishing threats

Only one third of organizations send email security and phishing-related security awareness training several times a month. Another one third do so monthly. See Figure 8.

Figure 8
Frequency of sending email security and phishing-related security awareness training
Percentage of respondents



Source: Osterman Research (2024)

When new types of phishing threats are being developed by cyberthreat actors, organizations need to step up the cadence of training to cultivate up-to-date awareness of likely threats. In such a dynamic threat environment:

- **Aim for a training cadence of at least monthly**
  A training cadence of at least monthly means that employees are up to date with the latest threats being seen for their organization specifically and the rest of the market in general. This ensures they are familiar with the most recent and relevant threats very soon after they have been developed, and are best positioned to delete, ignore, or report new phishing attacks. If certain groups are more frequently targeted by phishing attacks, and if the consequences of them falling for a phishing lure are significant enough, a training cadence of multiple times a month may be needed. This should only be done with their active buy-in that regular training on phishing is a critical part of their job role.
- **Train on the specific threats that employees receive in their inbox**
  Making training relevant to the individual is essential for increasing its efficacy. Building from the approach of role-specific training above, leverage generative AI services to create targeted training content based off the particular phishing messages that specific employees have fallen for.
- **If training is only quarterly or less frequently, efficacy will be low**
  Organizations providing email security and phishing-related security awareness training quarterly or less frequently are settling for a weak human defense layer. They are not providing data on current and emerging threats that have been seen in other organizations and could already be present in theirs. To remain quiet about newly emerging threats can be read as being unhelpful at best or complicit at worst.

When new types of phishing threats are being developed by cyberthreat actors, organizations need to step up the cadence of training to cultivate up-to-date awareness of likely threats.

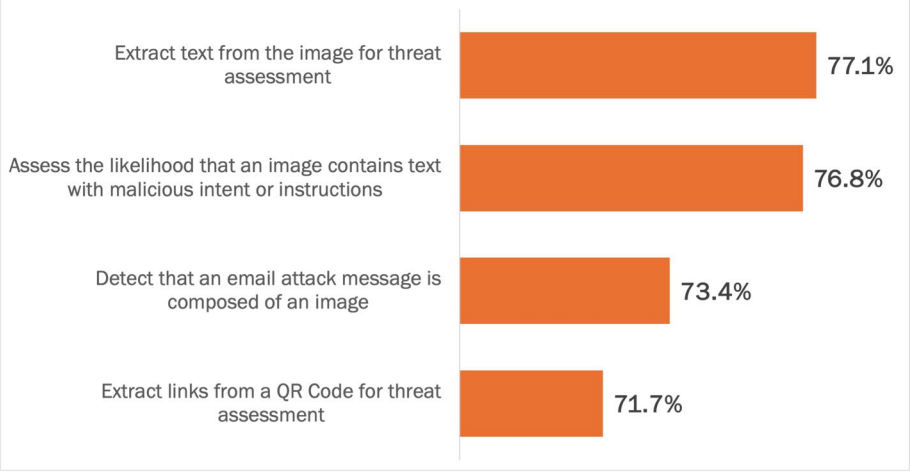
STRATEGY 2.
INCREASE EFFECTIVENESS OF EMAIL SECURITY DEFENSES

Only 5.5% of respondents indicated they were able to detect and block all image-based and QR code phishing attacks from reaching users' inboxes (see Figure 2). By implication, 94.5% of organizations are failing to catch these attacks, resulting in false negatives that are delivered to users' inboxes.

Given this baseline reality, it is worrisome—and paradoxical—that most respondents give high grades to their email security defenses, illustrating a clear confidence-security paradox. For example:

- **Detection efficacy is rated highly**
  72.7% of respondents assess their current email security stack as "very effective" or "extremely effective" at detecting image-based phishing attacks. 71.3% give the same highly effective rating for the detection of QR code phishing attacks.
- **Confidence in ability to detect malicious indicators is also rated highly**
  Equally high levels of reported confidence across a range of detection and assessment tasks for image-based and QR code phishing attacks contrast sharply with the low success rates of actual detection. The paradox deepens with 77.1% of respondents expressing they are "very confident" or "extremely confident" in their threat assessment capabilities. A similar 76.8% are convinced in their ability to assess the likelihood that an image contains text with malicious intent or instructions. See Figure 9.

Figure 9
Confidence in current email security stack to perform underlying security tasks
Percentage of respondents indicating "very confident" or "extremely confident"



Source: Osterman Research (2024)

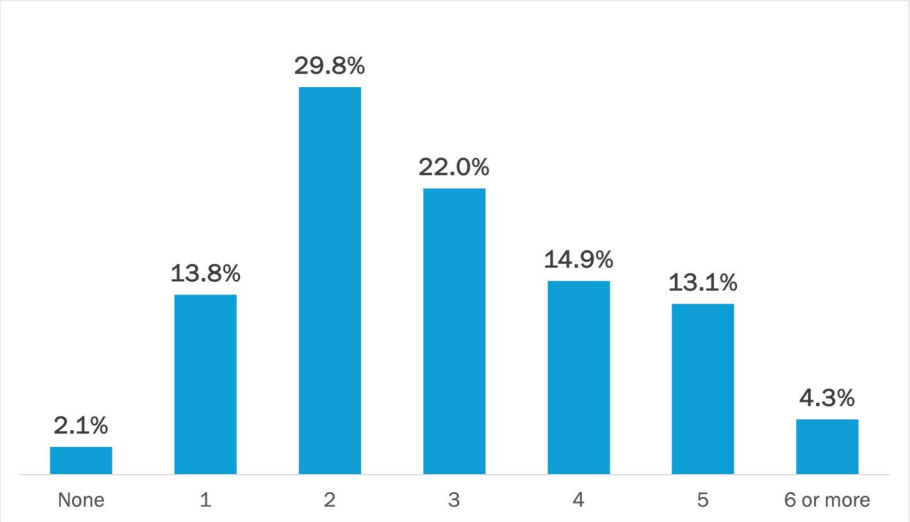
73% of respondents assert their email security stack is highly effective, yet only 5.5% say it has stopped all attacks from reaching users' inboxes.

The data leads to an unequivocal conclusion: the 25% to 30% of respondents who indicate inadequacies of their current email security stack and lack confidence in its ability to carry out essential detection capabilities must take action to strengthen current defenses. Nevertheless, there is an equally important conclusion for the remaining organizations which, despite professing high efficacy and capability, continue to experience breaches. This latter group faces a confidence-security paradox and must also take urgent action to review the current state of affairs.

Strengthen the email security stack

Almost all the organizations profiled in this research have either Microsoft 365 E3 or E5, or the Google Workspace Enterprise plan—and thus the best of what Microsoft and Google have to offer in terms of email security. Nonetheless, only 2.1% of organizations rely solely on what Microsoft and Google bundle. It is most common for the organizations in this research to rely on two or three email security solutions in addition to those available from Microsoft and Google. 55% of respondents use both a secure email gateway (SEG) and an email security suite that integrates via API with their cloud email provider. See Figure 10.

Figure 10
Number of email security solutions deployed (excluding cloud email provider)
Percentage of respondents



Source: Osterman Research (2024)

Image-based and QR code phishing attacks contain little, if any, textual content for pre-delivery analysis to determine whether a message is malicious or benign. Going forward, the key technical strategy is to leverage AI to analyze all available signals for reputation, plausibility, and anomalous communication patterns—and to detect the presence of images and QR codes embedding malicious instructions and URLs.

More than seven out of ten respondents plan on taking proactive steps to enhance their current email security stack (per Figure 5). Those actions are to:

- **Deploy additional and complementary email security technologies**
  For example, for organizations currently only using a SEG, this would mean strengthening their stack with an integrated cloud email security (ICES) offering.
- **Sign up for managed services for email security**
  Managed services offer a quick route to better technical capabilities, as well as cybersecurity expertise for incident response. Only 12.3% of the organizations in this research are currently using managed services for email security.
- **Replace their current email security stack with a more modern stack**
  72% of respondents indicated it was “very likely” or “extremely likely” that they would replace their current stack entirely over the next 12 months. If detection efficacy remains low, selecting a much better technical offering is the way to go.

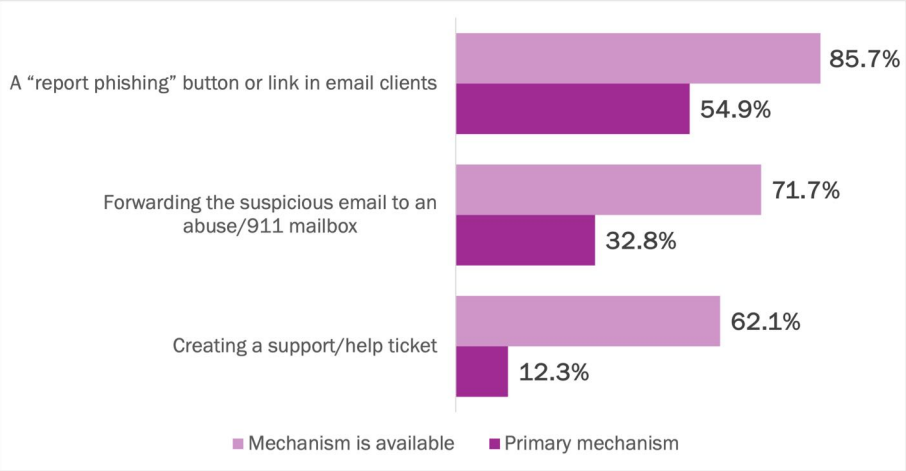
More than seven out of ten respondents plan on taking proactive steps to enhance their current email security stack over the next 12 months.

STRATEGY 3.
STRENGTHEN THE INCIDENT RESPONSE PROCESS

Most organizations plan on changing their incident response process to better handle image-based and QR code phishing attacks over the coming 12 months (73.7% per Figure 5). One specific approach that we explored in the research is mechanisms for reporting suspicious email messages.

All organizations in this research have defined one or more mechanisms that operate in parallel for users to report suspicious email messages that end up in their inbox. Almost all organizations offer a "report phishing" button or link in email clients (85.7%), and many support forwarding of a suspicious email to an abuse/911-style mailbox (71.7%) and creating a support/help ticket (62.1%). When respondents were asked to select the primary mechanism offered at their organization, more than half selected the "report phishing" button. See Figure 11.

Figure 11
Mechanisms for reporting suspicious email messages
Percentage of respondents



Source: Osterman Research (2024)

Most organizations plan on changing their incident response process to better handle image-based and QR code phishing attacks over the coming 12 months.

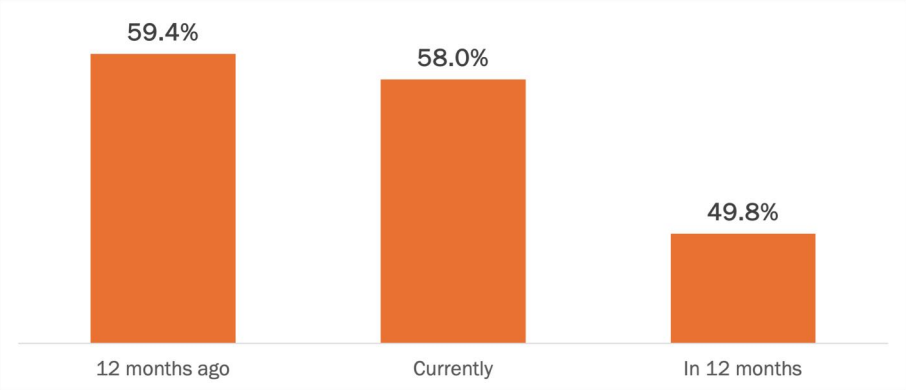
In looking the data another way, however, only 15.4% of organizations have defined a single mechanism for reporting phishing messages. Just over half (51.6%) allow two, and the remainder support all three mechanisms in parallel. To tighten mechanisms, organizations should look to the following:

- **Eliminate reliance on forwarding suspicious emails to an abuse/911 mailbox**
  Forwarding overwrites message metadata that is essential for the IT/security team to investigate the history of the message. There are also more steps involved for the user, and forwarding means a copy is stored in the user's Sent file which could be subsequently accessed with negative results.
- **Define and train around a single reporting process whenever possible**
  Following a single process simplifies training on what to do when faced with a suspicious message. Using a "report phishing" button is a prevailing best practice.
- **Optimize subsequent response and remediation processes**
  Unifying how suspicious messages are reported lays the foundation for improving process discipline metrics around responsiveness and automated remediation.

Conclusion

Emerging image-based and QR code phishing attacks have compromised most organizations over the past 12 months. There is a potential silver lining in this threat area, however, and that is the reduction in the perceived threat of these emerging phishing attacks. In 12 months' time, 49.5% of respondents believe these attacks will represent a high level of threat, down from 58.6% 12 months ago. While there is still a long way to go for many organizations, the trend line of the perceived threat level is directionally correct. See Figure 12.

Figure 12
Perceived threat of emerging image-based and QR code phishing attacks
Percentage of respondents indicating "very much a threat" or "an extreme threat"



Source: Osterman Research (2024)

But in order to turn this perception into an actionable reality over the next 12 months, organizations should be looking to follow the guidance and recommendations in this report. This means introducing role-based cybersecurity awareness training for targeted groups, micro-targeted phishing simulation tests that build off the specific phishing attacks each person receives, and augmentation and optimization of their email security stack.

To turn expectation into reality, organizations must strengthen their technical email security underpinnings and fortify human defenses.

About IRONSCALES

IRONSCALES is the leading cloud email security platform for the enterprise that uses machine learning and AI to stop advanced phishing attacks that bypass traditional security solutions. Its award-winning self-learning platform continuously detects and remediates advanced threats like Business Email Compromise (BEC), credential harvesting, Account Takeover (ATO) and more. As the most powerfully simple email security platform, IRONSCALES helps enterprises reduce risk, boost security team efficiency, and build a culture of cybersecurity awareness.

IRONSCALES is headquartered in Atlanta, Georgia and is proud to support more than 10,000 customers globally.

Visit www.ironscales.com or @IRONSCALES to learn more.

www.ironscales.com

@IRONSCALES

Methodology

This white paper was commissioned by IRONSCALES. Osterman Research surveyed 293 IT and security professionals in the United States in January 2024 on how their organization handled the threat of image-based and QR code phishing attacks.

SIZE OF ORGANIZATION

1,000 to 4,999 employees (average 2,235 employees)	68.9%
5,000 to 9,999 employees (average 5,906 employees)	24.2%
10,000 or more employees (average 17,420 employees)	6.8%
Average number of employees across all organizations	4,161

ROLES

IT manager or IT team lead	30.4%
IT security manager or IT security team lead	21.5%
Email security manager or email security team lead	16.0%
Security manager	11.6%
Email security administrator	11.3%
SOC manager or SOC team lead	5.5%
SOC analyst	3.8%

INDUSTRY

Information technology	26.6%
Industrials (manufacturing, construction, etc.)	13.3%
Retail or ecommerce	12.3%
Financial services	10.6%
Computer hardware or computer software	8.5%
Healthcare	6.5%
Data infrastructure or telecom	5.8%
Transport or logistics	5.5%
Education	2.4%
Energy or utilities	2.4%
Life sciences or pharmaceuticals	2.4%
Professional services (law, consulting, etc.)	1.0%
Government	0.7%
Other	0.7%
Agriculture, forestry or mining	0.3%
Hospitality, food or leisure travel	0.3%
Media or creative industries	0.3%
Public service or social service	0.3%