DARKREADING
REPORTS

DECEMBER 2024

Understanding Social Engineering Attacks and What to Do About Them

Social engineering attacks are getting more sophisticated. Enterprise security teams are adapting to the latest threats with multi-layered defenses and improved training.

Sponsored by
Google Cloud
Security

informatechtarget

NEXT

TABLE OF CONTENTS

FIGURES

Strategies to Defend Against Social Engineering Attacks

By Yihao Lim, Lead Threat Intelligence Advisor, Google Threat Intelligence Group

Users remain the weakest link in a robust security environment as they are vulnerable to compromise via social engineering — exploiting vulnerabilities in human behavior to convince people to perform activities they would not normally conduct.

Social engineering has been deployed in virtually every industry globally to compromise accounts, infect victims with malware, steal proprietary information, or collect data for future criminal or espionage activity.

It is also leveraged for reconnaissance purposes targeting a specific victim, lasting for days or months, depending upon the perceived value of the target. In recent years, we observed a shift to social media to bolster campaigns and for increasingly aggressive post-compromise social engineering operations by ransomware operators.

The prevalence of this activity is a strong indicator threat actors will continue to leverage social engineering operations for the foreseeable future, particularly by less-sophisticated actors or against organizations with a strong security posture that have reduced other attack surfaces.

Recent Social Engineering Attack Trends

Gone are the days of generic phishing emails riddled with grammatical errors and other inaccuracies. Attackers now leverage large language models (LLMs), social media, and other publicly available information to craft highly personalized messages, imagery, or audio that appear to come from trusted sources.

Spear phishing is a type of social engineering attack that targets specific individuals or organizations, including VIPs such as high-profile executives. Targets are usually people who possess highly privileged access or information. These attacks often involve extensive research and reconnaissance to gather information that can be used to create highly convincing lures. Attackers might impersonate IT staff, vendors, or even colleagues to gain access to sensitive information or systems. We assess with high confidence that this tactic will continue to persist for the foreseeable future.

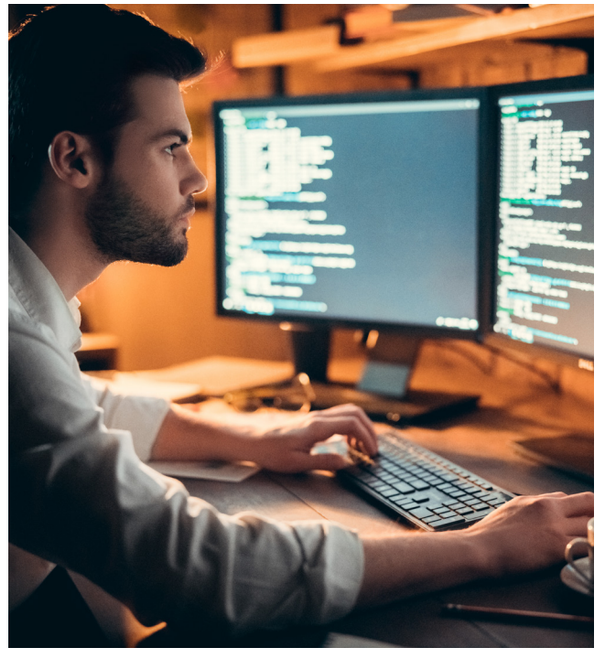
Business email compromise attacks involve compromising legitimate business email accounts to conduct fraudulent activities. This can include requesting wire transfers, diverting payments, or accessing confidential information. Attackers often use social engineering techniques to gain access to these accounts, such as phishing or exploiting weak passwords. Actors commonly employ various TTPs in their operations, including phishing emails and websites hosting phishing kits to harvest user

credentials, multi-factor authentication (MFA) fatigue attacks, registration of typo-squatted domains, email spoofing, and the creation of email forwarding rules to reduce the likelihood of their activity being discovered by the victim.

Then there is OAuth and Token Interception. We have observed session hijacking incidents involving abuse of OAuth and interception of tokens during multi-step social engineering campaigns, and we regularly observe actors advertising one-time-password (OTP) bypassing services that can retrieve passwords from organizations worldwide, leveraging bots. We expect that this activity will continue for at least the near- to midterm.

Voice phishing ("vishing") and SMS phishing ("smishing") attacks exploit the immediacy and trust associated with phone calls and text messages. Attackers might impersonate banks, government agencies, or tech support to trick individuals into revealing personal or financial information. AI-powered voice spoofing can enable attackers to make their vishing attacks even more convincing.

On social media platforms, attackers will spread disinformation, create fake profiles, and build trust



with potential victims. They might leverage social engineering techniques to gather information, spread malware, or launch phishing attacks. Social media platforms such as LinkedIn provide threat actors with a user's behavioral data, general interests, personal and professional network, and employment information. This sensitive data can be used to create tailored lure content, or help profile targets in the future.

Compounding the social engineering threat is a growing number of powerful new generative AI tools, which assist attackers in performing reconnaissance, enable them to craft even more convincing lures, and strengthen disinformation campaigns with AI-generated and manipulated audio and video. Additionally, AI-powered voice cloning can effectively mimic human speech, creating far more effective voice phishing attacks.

How to Defend Against Modern Social Engineering Attacks

While social engineering attacks are constantly evolving, there are several effective strategies organizations can employ to protect employees and the business:

- **Education and Reporting:** The most critical defense against social engineering is education. Provide resources to help employees recognize the signs of these attacks, such as unsolicited requests for information, suspicious links or attachments, and unexpected phone calls or text messages. Encourage a culture of vigilance and reporting any suspicious activity.

- **Security Awareness Training:** Conduct regular security awareness training sessions to educate employees about the latest social engineering tactics and how to identify and respond to them. Include

simulations and real-world examples to help employees develop the skills they need to stay safe.

- **Strong Password Policies:** Implement strong password policies that require complex passwords and regular updates. Encourage the use of password managers to generate and store unique passwords for each account.

- **Multi-Factor Authentication (MFA):** MFA adds an extra layer of security by requiring users to provide additional verification beyond a password, such as a fingerprint, security token, or one-time code. This makes it significantly harder for attackers to gain access to accounts, even if they have obtained a password.

- **Email and Web Filtering:** Use email and Web-filtering tools to block malicious emails, websites, and attachments. This can help prevent phishing attacks and other forms of social engineering.

- **Incident Response Plan:** Have a well-defined incident response plan in place to address social engineering attacks if they occur. This should include procedures for identifying, containing, and recovering from attacks, as well as communicating with affected individuals and authorities.

- **Stay Informed:** Use threat intelligence to keep up-to-date on the latest social engineering trends and tactics. This will help you recognize new threats, under-stand the threats that matter most to your organization, and adapt your defenses accordingly.

Threat Intelligence is crucial for stakeholders in view of the evolving landscape of social engine-ering attacks. Implementing these defense strategies, you can significantly reduce the risk of falling victim to these malicious tactics.

Remember, the human element is often the weakest link in cybersecurity, so ongoing education and vigilance are crucial to staying safe in the digital age.

About the Company: Make Google part of your security team with Mandiant frontline experts, intel-driven security operations, and a secure cloud platform — supercharged by AI. Organizations can address their tough security challenges with many of the same capabilities Google uses to keep more people and organizations safe online than anyone else in the world: frontline intelligence and expertise, a modern, intel-driven security operations platform, and a secure-by-design cloud foundation. AI enhances all of these components, personalizing intelligence for your business, automating manual tasks, and assisting security professionals in effectively addressing complex cases.

ABOUT THE AUTHOR

Fahmida Y. Rashid
Dark Reading

Fahmida Y. Rashid specializes in stories that pull insights from areas outside information security to help security professionals do their jobs. As managing editor at Dark Reading, she focuses on in-depth analysis and features about cybersecurity strategy and technology. She has over 10 years of prior experience as an IT professional — as a network administrator, software developer, management consultant, and product manager.

EXECUTIVE SUMMARY

The survey paints a picture of a cybersecurity landscape that is growing increasingly complex, with organizations facing multifaceted challenges that demand sophisticated, proactive approaches. From sophisticated social engineering to the threat of AI-powered attacks, today's security professionals navigate a minefield of risks. While most organizations have implemented foundational security controls, there are areas of improvements such as passwordless authentication, security awareness training, and identity and access controls.

As cybersecurity professionals look to the future, they must adopt a holistic approach to security that recognizes human factors as a critical component of cybersecurity. Technical controls are not enough, and security awareness training should not be considered the be-all-and-end-all of security. The road ahead demands strengthening technical defenses and also investing in human-centric security strategies that focus on education, awareness, and response mechanisms to report threats. Organizations must remain vigilant, agile, and committed to developing robust, comprehensive security infrastructures that can protect against an ever-changing threat landscape.

The following are some key data points from the survey:

- 43% of IT and security managers name phishing, social network exploits, and other forms of social engineering as the biggest threats facing their organization. 25% of respondents strongly believe their organization or industry will see disinformation campaigns in the coming year.
- Malicious attachments or links in emails pointing to malware or phishing sites were the most common type of attack seen over the past year (82%). A little over a quarter (26%) say they have received phone calls from someone pretending to be an internal employee such as IT staff.
- There is room for improvement in security awareness training programs. While 36% say they conduct training two to four times a year, 43% of respondents say their organization's security awareness trainings typically last less than an hour.
- For many organizations, security awareness training is required by law (34%) or some kind of regulatory body (23%). Respondents recognize that training can help prevent reputational damage (65%) or financial loss (64%).
- Organizations are deploying better security controls. Around half of the respondents say they are using multi-factor authentication in some form as a result of recent social engineering attacks.

ABOUT US

Dark Reading Reports offer original data and insights on the latest trends and practices in IT security. Compiled and written by experts, Dark Reading Reports illustrate the plans and directions of the cybersecurity community and provide advice on the steps enterprises can take to protect their most critical data.

Dark Reading Reports

DARKREADING REPORTS

RESEARCH

SYNOPSIS

Survey Name: 2024 Dark Reading Cybersecurity Awareness Survey

Survey Date: October 2024

Number of Respondents: 106 cybersecurity and IT professionals from organizations of all sizes primarily located in North America. The margin of error for the total respondent base was +/- 9.5 percentage points.

Methodology: The survey queried cybersecurity and IT professionals about the top cybersecurity challenges cybersecurity professionals face, how their teams are dealing with threats, and security awareness programs. Respondents' job titles spanned from executive level cybersecurity and IT titles (such as CSO/CISO and CIO/CTO), to cybersecurity and IT management and staff.

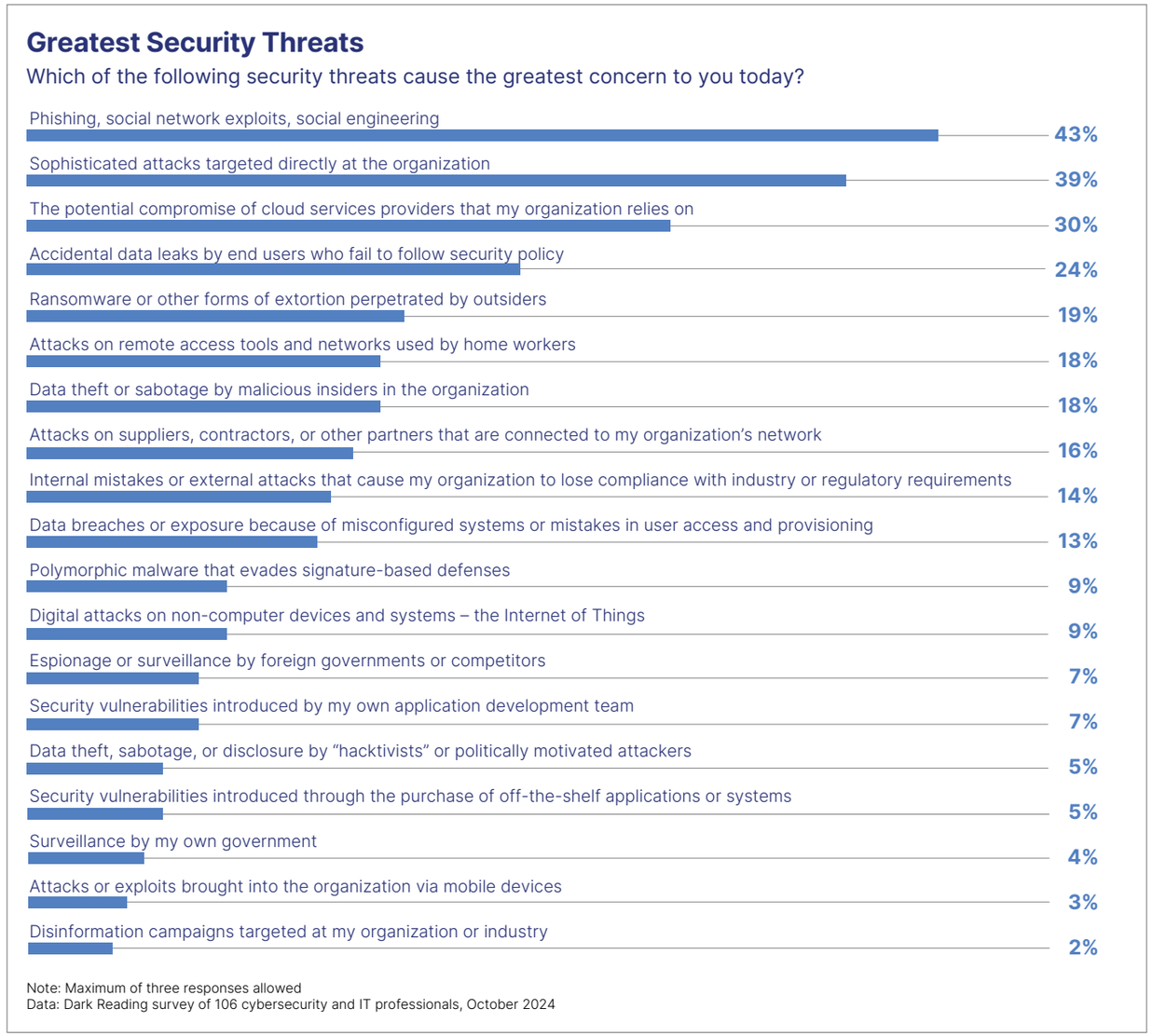
Dark Reading conducted the survey online in October 2024. Respondents were recruited via email invitations containing an embedded link to the survey. The email invitations were sent to a select group of past and present attendees of the Black Hat conference, a cybersecurity-focused conference by Informa, the parent company of Dark Reading. Dark Reading was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

Introduction

Highly effective and difficult to defend against, social engineering attacks have emerged as one of the most persistent and pernicious threats facing organizations today. The results of the *2024 Dark Reading Cybersecurity Awareness Survey* highlight the kinds of social engineering attacks organizations have been dealing with over the past year as well as the multi-layered approach cybersecurity professionals are taking in response.

While cybersecurity professionals have to contend with a variety of threats against their organizations, different forms of social engineering attacks are one of their biggest concerns. Respondents in this year's survey listed social engineering attacks (43%), sophisticated attacks targeted directly at the organization (39%), and breaches at their cloud providers (30%) as their three biggest concerns **(Figure 1)**. Some respondents listed threats such as ransomware or other forms of extortion (19%), attacks on remote access tools and networks used by home workers (18%), and attacks on suppliers, contractors, or other partners (14%). It's important to remember that these attacks often involve social engineering — for example, to trick users into clicking a malicious link or enter login credentials into a malicious application.

Figure 1.

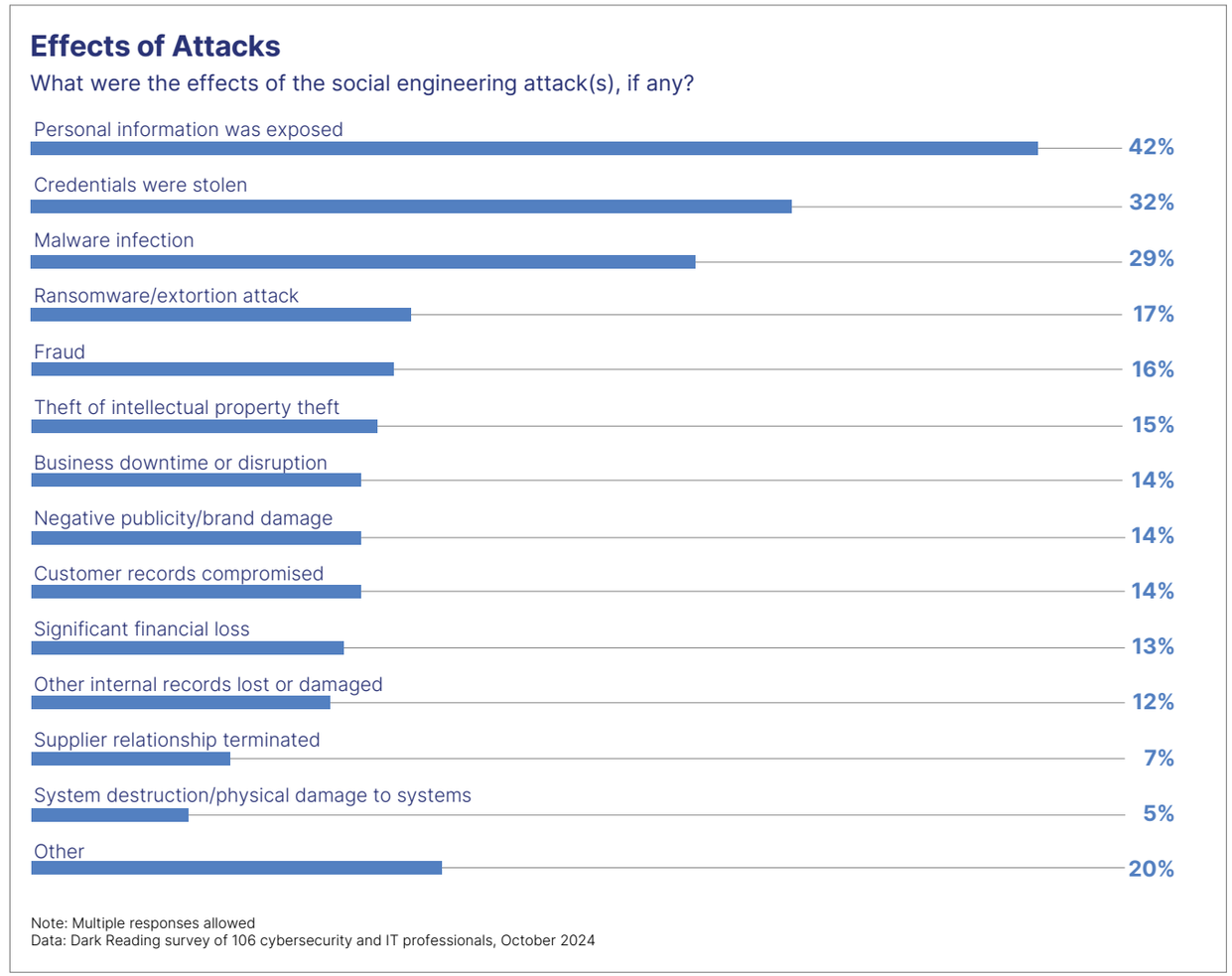


In this year's Verizon Data Breach Investigations Report, phishing and pretexting via email contributed to social engineering attacks in approximately 73% of all breaches. And 68% of the breaches analyzed by Verizon Business involved some kind of human error — either someone clicked on a phishing email, fell for an elaborate social-engineering gambit, was tricked by a deepfake, or made some other mistake.

Consider the attacks against casino giants Caesars Entertainment and MGM Resorts in 2023. The criminal group behind those attacks is known to employ social engineering techniques against enterprises. The casino incidents involved a combination of credential phishing and social engineering to capture one-time password codes before deploying ransomware.

The consequences of social engineering attacks are severe as they tend to have a wide blast radius. Respondents report a range of damaging outcomes, such as the exposure of personally identifiable information and financial details (42%), stolen credentials (32%), malware (29%) or ransomware (17%) attack, financial fraud (16%), and theft of intellectual property (15%) **(Figure 2)**.

Figure 2.



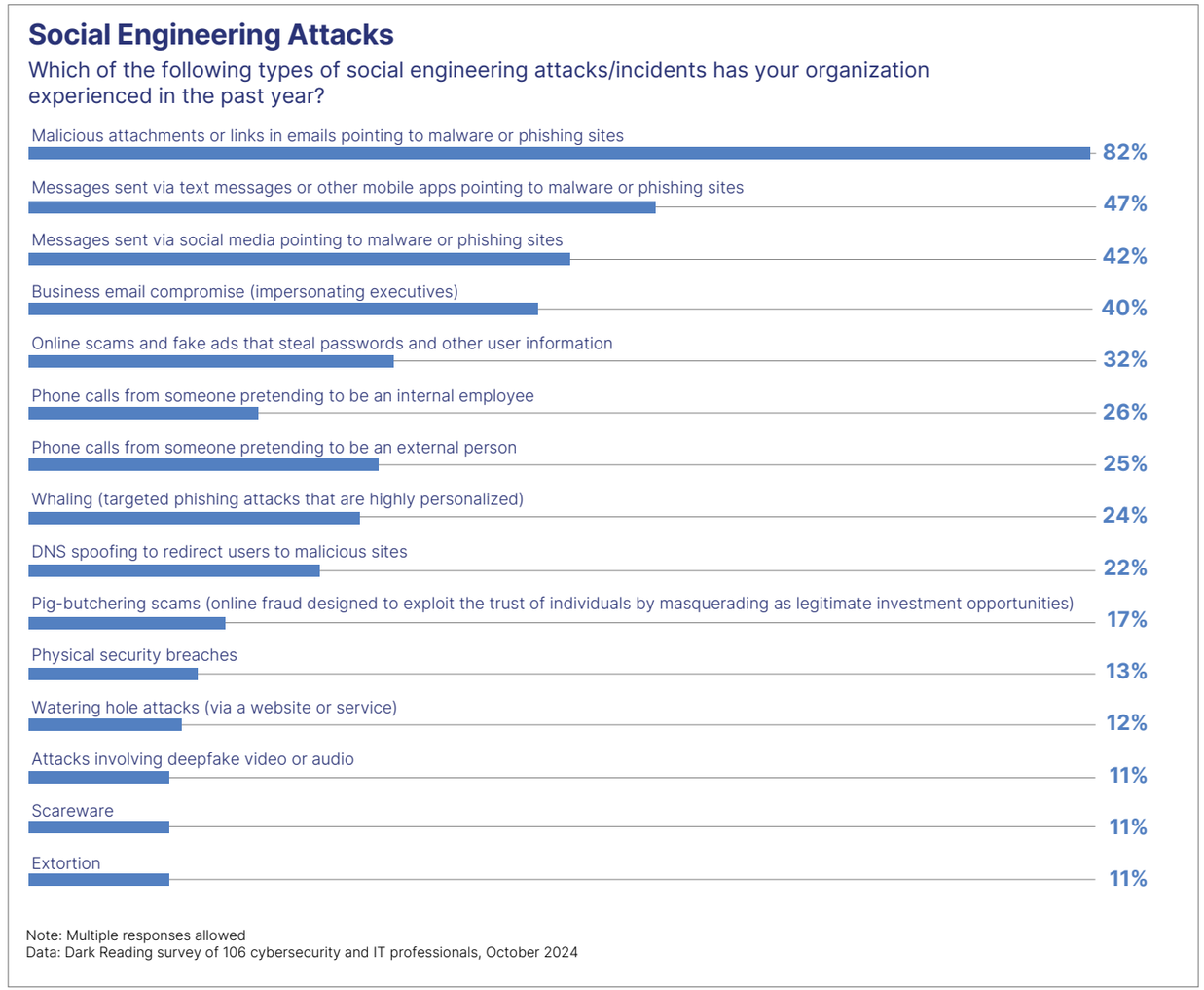
Anatomy of Social Engineering Attacks

The survey results indicate that attackers are getting creative with social engineering; it's not just malicious emails anymore. While the majority of respondents (82%) report their organizations have experienced malicious emails or messages pointing to malware or phishing sites over the past year, a significant number also report malicious messages sent via text messages (47%) and social media (42%) as well **(Figure 3)**. Nearly a third of respondents (32%) say they have seen online scams and fake advertisements designed to steal passwords and other user information.

Attackers are also making phone calls. Roughly a quarter of respondents say their organization received phone calls from someone pretending to be an internal employee such as IT staff (26%) or from someone pretending to be an external person such as a member of law enforcement or a supplier (25%).

Two-fifths of respondents (40%) say their organization experienced business email compromise (BEC) scams where the attackers impersonated executives, and 24% say their organization experienced whaling attacks (highly personalized phishing attacks that

Figure 3.

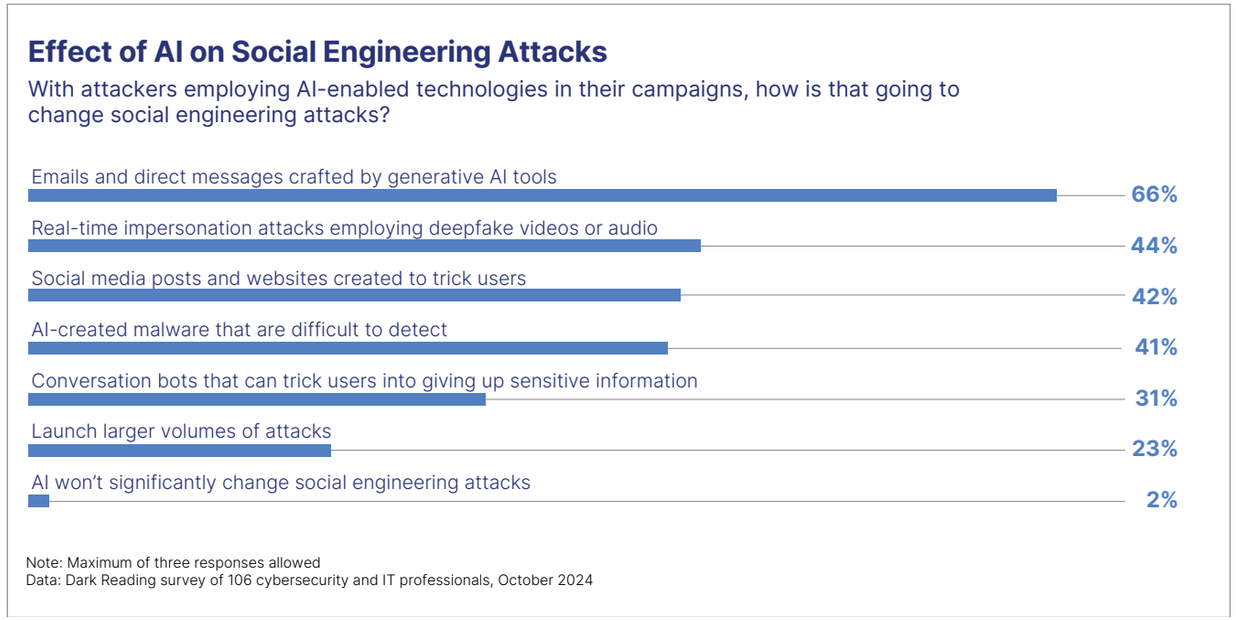


target high-profile executives in the organization, such as the CEO).

Falling for these social engineering attacks can be costly. Verizon's DBIR analysis found that the median loss in the past two years for BEC scams is $50,000.

There is a growing concern about adversaries using AI for social engineering attacks as well. Respondents say they are concerned about emails and direct messages crafted by generative AI tools (66%) and real-time impersonation attacks employing AI-generated voices or deepfake videos (44%) **(Figure 4)**. One respondent expressed concern that AI would make it easier for adversaries to better craft and launch personalized attacks.

Figure 4.



Considering AI-generated audio and video is still in the early stages in terms of what it can do, it is notable that 45% of respondents say their organization has responded to an incident involving deepfakes in the past year **(Figure 5)**. Each iteration of the AI model is getting better at generating audio and video — which means it is getting harder for organizations to detect them. Just 60% expressed confidence in their organization's security team to detect and mitigate disinformation campaigns, but what's worrying is that just half of the respondents feel their tools are up to the task.

Looking ahead, the survey suggests that the cybersecurity challenges facing organizations are unlikely to subside anytime soon. A significant number of respondents (79%) say disinformation is a serious threat and almost impossible to prevent **(Figure 6)**. A majority of respondents (88%) believe the industry needs to find ways to combat disinformation, even if it's not directly impacting their own company.

Organizations Step Up Their Defenses

While 90% of respondents say their team has been able to successfully block, or minimize, the impact of social engineering attacks over the past year, they remain concerned about their defensive capabilities **(Figure 7)**. A little less than two-thirds of

Figure 5.

Social Engineering Attacks

How strongly do you agree or disagree with the following statements about social engineering attacks?

	Strongly agree	Agree somewhat	Disagree somewhat	Strongly disagree
My team has been able to successfully block/ minimize the impact of social engineering attacks against my organization over the past year.	37%	53%	9%	1%
My organization has had conversations with suppliers and partners about their plans for dealing with social engineering attacks.	31%	37%	25%	7%
My organization's cyber insurance policy covers incidents involving social engineering.	21%	42%	23%	14%
My organization has responded to an incident involving deepfakes in the past year.	12%	33%	19%	36%

Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

respondents say their organization's cyber insurance policy covers incidents involving social engineering (63%), illustrating just how pervasive these attacks have become.

In the 2024 Cybersecurity Decision Makers survey from Omdia, a majority of CISOs and senior security practitioners were confident in how their organization would respond to phishing and BEC attacks and other types of credential theft. There was a split in the degree of confidence, with 47% saying there could be some business interruption (compared to 14% who say business will definitely be interrupted), and 37% saying business would continue to operate without any issues.

Organizations are taking a multi-layered approach to fortify their defenses against ever-evolving social engineering threats. There is a heavy emphasis on foundational controls such as firewalls, antivirus, endpoint security tools, and email security (which includes anti-spam filtering as well as scanning for phishing links and malicious attachments). More than four-fifths of respondents (83%) say they rely on their organization's security awareness training program to help defend the organization from social engineering attacks **(Figure 8)**. Three-quarters of respondents also use phishing simulations. It is promising that a sizeable number of organizations are deploying advanced controls such as passwordless technologies (38%) and FIDO2 security keys (22%).

Attackers rely heavily on social media sites for their social engineering attacks. They may collect publicly posted information to gather the details they need to trick the targeted individual. They may also reach out to the victim via social media to lure them into some kind of action, or to siphon out sensitive information such as credentials. Despite all that, just 22% of respondents say their organization currently uses social media security tools.

And 31% of respondents say their organization has no plans to adopt social media security tools, which would hamper their ability to identify and

mitigate impersonation attempts and disinformation campaigns against their employees and executives.

Real-World Impact on Defense

When it comes to social engineering threats, enterprise security defenders don't have the luxury of focusing on just corporate-managed devices. Attackers can scrape LinkedIn profiles and send spam and phishing emails to personal accounts — and then steal credentials or infect the personal device with information-stealing malware. Another common attack vector that bridges personal device and corporate accounts is the fake delivery notification telling users about an impending package directing them to sites loaded with malware designed to steal credentials. While security awareness training is important, enterprises have other methods for protecting personal devices or services.

A little shy of half, or 48%, of respondents say personal devices must be registered with IT before they can access work resources **(Figure 9)**. People are also prompted to regularly update their devices (48%) and use VPNs before accessing corporate applications from personal devices (45%). In fact, 42% of respondents say their organization imposes heightened access requirements or extra layers of authentication when personal devices are used to access corporate applications. A similar number of respondents say their organization restricts access to enterprise applications if the personal device does not meet minimum software requirements, such as having the latest version of the operating system and installing security software.

Figure 6.

Combating Disinformation

How strongly do you agree or disagree with the following statements about disinformation?

	Strongly agree	Agree somewhat	Disagree somewhat	Strongly disagree
I believe the industry needs to come up with ways to combat disinformation even if it isn't affecting our organizations directly.	55%	33%	8%	4%
I believe that disinformation is a serious threat to industry and almost impossible to prevent.	36%	43%	16%	5%
Attackers will launch disinformation campaigns against my organization or industry in the coming year.	25%	40%	25%	10%
Attackers will launch disinformation campaigns against my organization or industry in the coming year.	16%	44%	30%	10%
I believe we have the tools necessary to detect and mitigate disinformation campaigns.	10%	40%	30%	20%

Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Social engineering attacks — whether against the organization or reports of attacks against other organizations — are driving improvements in enterprise defenses. Roughly half of respondents (55%) say that recent attacks have influenced their

organization to enable multi-factor authentication on critical accounts and services, and 48% say their organization now mandates multi-factor authentication across all accounts and services **(Figure 10)**. Just shy of half (47%) of respondents say their organization changed their security awareness training program, such as adding new training material, changing the training format, or increasing the frequency of training. Another positive change was the number of organizations deciding to move to a zero trust architecture (45%) to verify user identities and limit access privileges to only what is necessary.

The focus on training — and re-training — is important in making sure end users understand how to avoid social engineering attacks. For many organizations, security awareness training is required by law (34%) or some kind of regulatory body (23%), but most of the respondents say that training helps prevent reputational damage (65%), financial loss (64%), and protects customer data (57%) **(Figure 11)**.

Frequent training is necessary to ensure employees are learning the material and retaining the concepts. A little over a third, 36%, of respondents conduct security training two to four times a year, which could be every six months, or once a quarter **(Figure 12)**. Awareness training should also not be too long, but in some areas, it may be too short. Note that 43% say the typical duration of security awareness training in their organization is less than an hour **(Figure 13)**.

Figure 7.

Social Engineering Attacks

How strongly do you agree or disagree with the following statements about social engineering attacks?

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
My team has been able to successfully block/minimize the impact of social engineering attacks against my organization over the past year.	37%	53%	9%	1%
My organization has had conversations with suppliers and partners about their plans for dealing with social engineering attacks.	31%	37%	25%	7%
My organization's cyber insurance policy covers incidents involving social engineering.	21%	42%	23%	14%
My organization has responded to an incident involving deepfakes in the past year.	12%	33%	19%	36%

Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Conclusion

Ultimately, the survey data underscores the critical importance of a multi-layered, proactive approach to defending against social engineering threats. By combining technical controls, employee education, and robust third-party risk management, organizations can strengthen their resilience against these increasingly sophisticated attacks. As the threat landscape continues to evolve, staying ahead of social engineering tactics will require a sustained, comprehensive effort from cybersecurity teams.

APPENDIX

Figure 8.

Use of Security Controls

Which of these security technologies and controls is your organization using to protect against social engineering attacks?

	Currently using	Plan to deploy	Don't plan to deploy	Not sure
Firewalls	95%	2%	3%	0%
Antivirus	93%	5%	1%	1%
Multifactor authentication	93%	5%	2%	0%
Email scanning and filtering (for phishing links, malicious attachments)	90%	6%	2%	2%
Endpoint security tools	88%	7%	2%	3%
Anti-spam filtering	87%	7%	4%	2%
Security awareness training program	83%	12%	4%	1%
User access controls, privilege management	81%	15%	2%	2%
Phishing simulation testing	75%	12%	7%	4%
Third-party penetration testing	71%	15%	9%	7%
Data leak protection	51%	21%	10%	18%
Passwordless technologies	38%	27%	16%	19%
FIDO2 Security Keys	22%	24%	15%	39%
Social media security tools	22%	19%	31%	28%

Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 9.

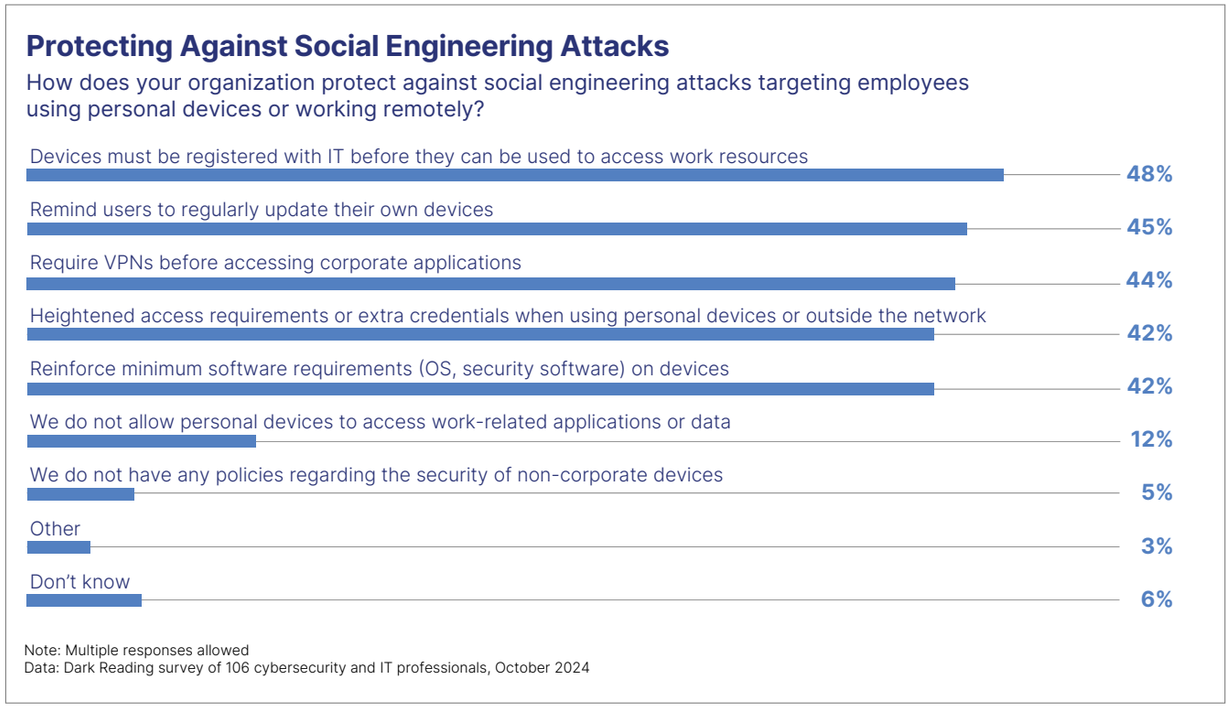

Protecting Against Social Engineering Attacks
How does your organization protect against social engineering attacks targeting employees using personal devices or working remotely?
Devices must be registered with IT before they can be used to access work resources
48%
Remind users to regularly update their own devices
45%
Require VPNs before accessing corporate applications
44%
Heightened access requirements or extra credentials when using personal devices or outside the network
42%
Reinforce minimum software requirements (OS, security software) on devices
42%
We do not allow personal devices to access work-related applications or data
12%
We do not have any policies regarding the security of non-corporate devices
5%
Other
3%
Don't know
6%
Note: Multiple responses allowed
Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 10.

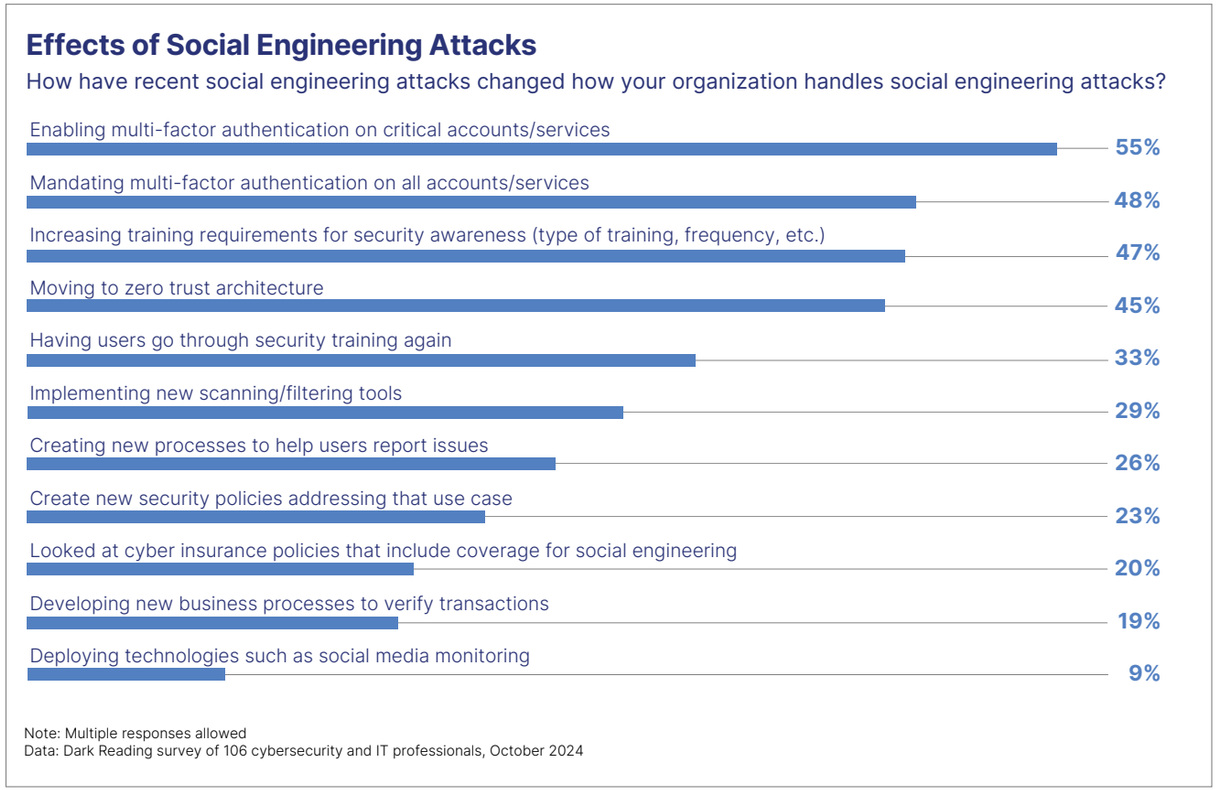
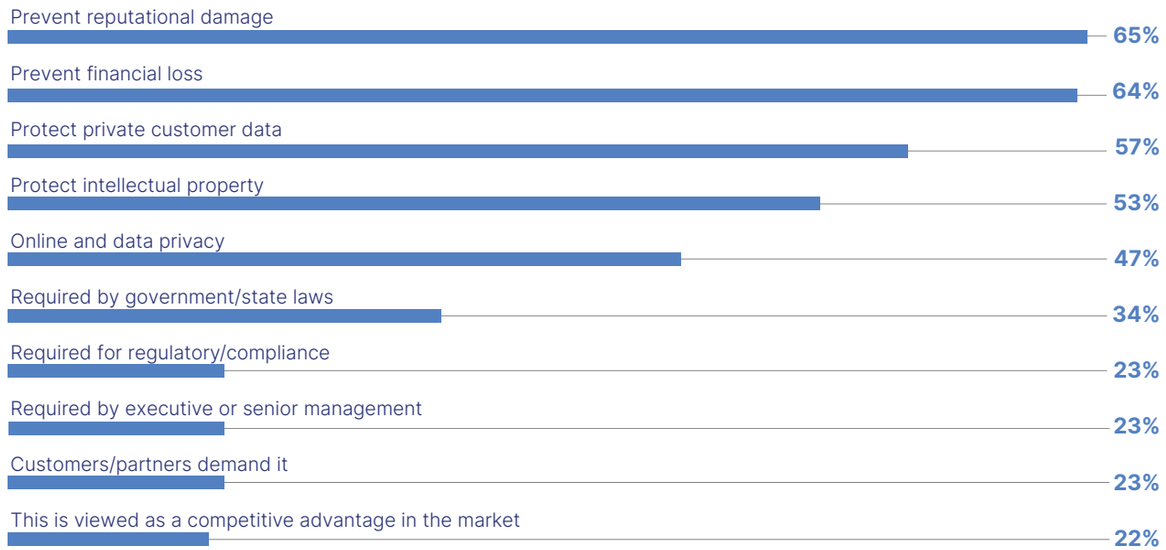

Effects of Social Engineering Attacks
How have recent social engineering attacks changed how your organization handles social engineering attacks?
Enabling multi-factor authentication on critical accounts/services
55%
Mandating multi-factor authentication on all accounts/services
48%
Increasing training requirements for security awareness (type of training, frequency, etc.)
47%
Moving to zero trust architecture
45%
Having users go through security training again
33%
Implementing new scanning/filtering tools
29%
Creating new processes to help users report issues
26%
Create new security policies addressing that use case
23%
Looked at cyber insurance policies that include coverage for social engineering
20%
Developing new business processes to verify transactions
19%
Deploying technologies such as social media monitoring
9%
Note: Multiple responses allowed
Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 11.

Important Reasons for Security Awareness Training

What are the most important reasons for security awareness training at your company?

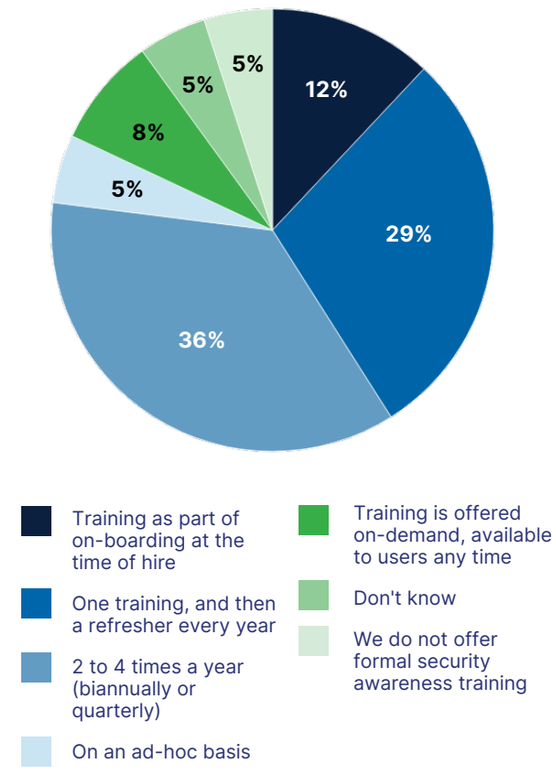


Note: Multiple responses allowed
Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 12.

Frequency of Security Awareness Training Programs

How frequently do your employees take part in security awareness training programs in your organization?



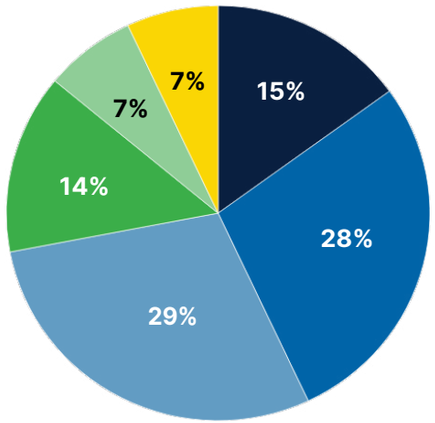
Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

DARKREADING REPORTS

Figure 13.

Security Awareness Training Timeframe

What is the typical duration of security awareness training in your organization?



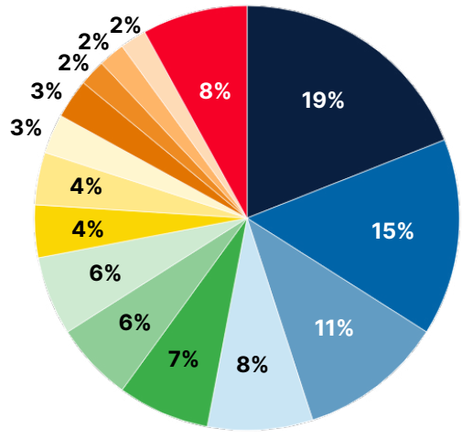
- 15 minutes or less
- Between 15 minutes to under an hour
- Between 1 hour and 2 hours
- More than 2 hours
- Don't know
- We do not offer formal security awareness training

Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 14.

Respondent Job Title

Which of the following best describes your role in the organization?



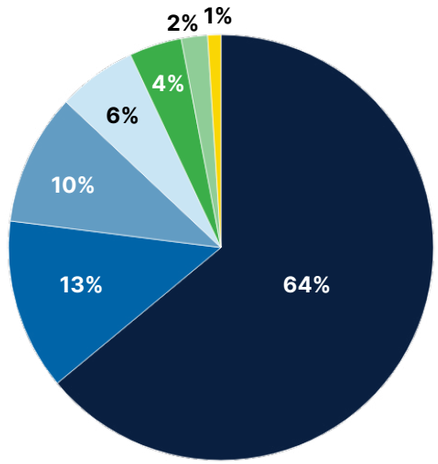
- Cybersecurity staff
- CSO/CISO/CPO
- IT staff
- CIO/CTO
- Cybersecurity manager
- Cybersecurity director/head
- Engineer
- IT/cybersecurity VP
- Network/system adm.
- IT director/head
- Software/AppDev
- IT manager
- Corporate executive
- Internal auditor
- Other

Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 15.

Respondent Geographic Location

Where are you located?



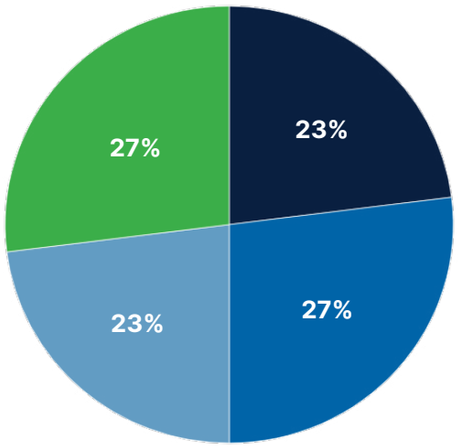
- North America
- Europe or Central Asia
- South Asia
- Latin America, Mexico, or South America
- East Asia or Pacific
- Middle East or North Africa
- Sub-Saharan Africa

Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 16.

Respondent Company Size

Approximately how many employees are in your organization in total?

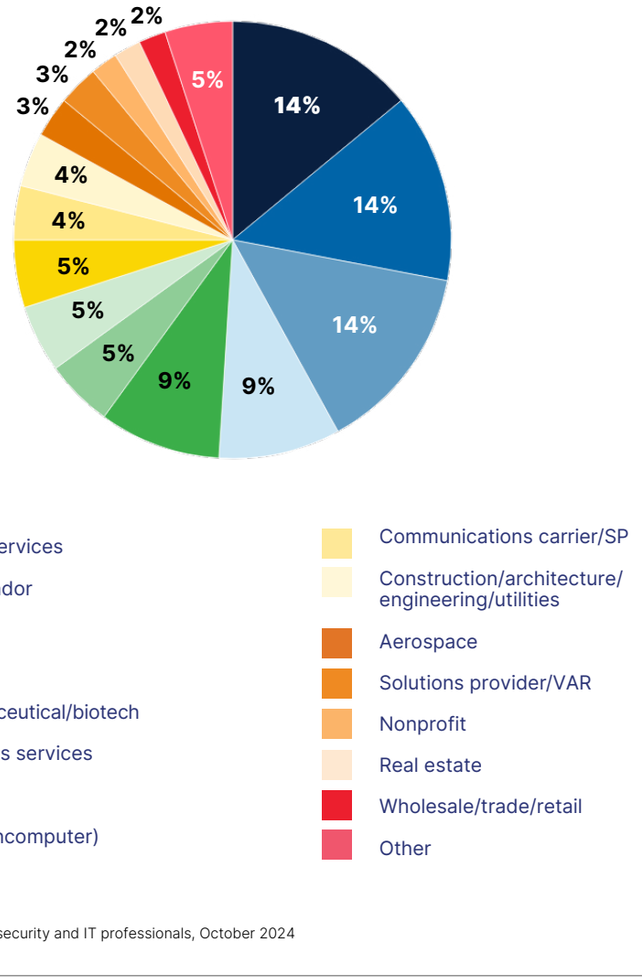


Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

Figure 17.

Respondent Industry

What is your organization's primary industry?



Data: Dark Reading survey of 106 cybersecurity and IT professionals, October 2024

DARKREADING REPORTS