2019 REPORT

proofpoint®

Security Awareness Training

BEYOND THE PHISH®

proofpoint.com/security-awareness

BEYOND THE PHISH

2019 REPORT

TABLE OF CONTENTS

GAUGING END-USER CYBERSECURITY RISK BEYOND THE INBOX

A strong cybersecurity posture has many facets. The same is true when it comes to users' cybersecurity knowledge. Having the skills to identify and avoid lures in email phishing attacks is critical. But so is understanding how one's own behaviour, even beyond the inbox, can affect security. This insight matters on both a personal level and for the organisation as a whole.

That's the inspiration behind our fourth annual *Beyond the Phish*® report. In our deepest and most wide-ranging report yet, we explore user knowledge of a broad range of best practices for cyber hygiene, security and compliance. The report analyses millions of responses gathered from our Security Education Platform. These include answers to CyberStrength® Knowledge Assessments and quiz questions within our interactive training courses.

This year's report includes:

- Data from nearly **130 million questions answered by our customers' end users.** The analysis spans responses gathered between January 1, 2018, and February 28, 2019.
- Users' understanding of **14 cybersecurity topics**.
- Two new categories: users' understanding of **unintentional and malicious insider threats and a view of executives' cybersecurity knowledge**.[1]
- Results across all users compared to the **results of a selection of our Managed Services customers**. It shows how adherence to security awareness training best practices influences success.
- Knowledge comparisons across **16 industries and common business departments**.

Why We Go "Beyond the Phish"

Simulated email phishing attacks are a powerful way to assess users' weaknesses. We analyse these in detail for our State of the Phish report.

But there's more to the story.

Consider the average failure rate from the *2019 State of the Phish* report to knowledge-assessment data from this report:

Average Simulated Phishing Attack Failure Rate	VS	Average Percentage of Phishing Questions Answered Incorrectly
9%		**25%**

All users. All industries.

STATE OF THE PHISH REPORT

To learn more about how users fared in simulated phishing attacks, get our 2019 *State of the Phish* report.

The implication is clear: Simulated phishing attacks alone don't fully reflect how well users understand this wide-ranging threat. Nor do they provide insight into awareness of best practices in other key areas, including:

- Password hygiene
- Mobile device security
- Managing confidential data

[1] See the Appendix for an in-depth explanation of our 14 categories and our report methodology.

A CYBERSECURITY KNOWLEDGE SNAPSHOT

This year, users answered 22% of questions incorrectly on average across all 14 subjects. That's up from 19% in our 2018 analysis. The uptick was not much of a surprise. Since our last report, we have expanded our assessment and training programmes to include new and more advanced cybersecurity topics. In other words, this year's assessments were tougher.

22% of questions were answered incorrectly across all topic categories, including phishing, compliance and more.

Top 5 Training Topics

Of our 14 categories, these are the five most popular among our customers:

1. Identifying Phishing Threats
2. Cybersecurity Concerns for Working Adults
3. Protecting Data Throughout Its Lifecycle
4. Social Engineering and Related Scams
5. Protecting Mobile Devices and Information

Figure 1 shows the wrong-answer rates within each category. These results reflect users' comfort with and understanding of these key cybersecurity topics. (For more about what is covered in each category, see the Appendix on page 12.)

Percentage of wrong answers on security awareness training assessments

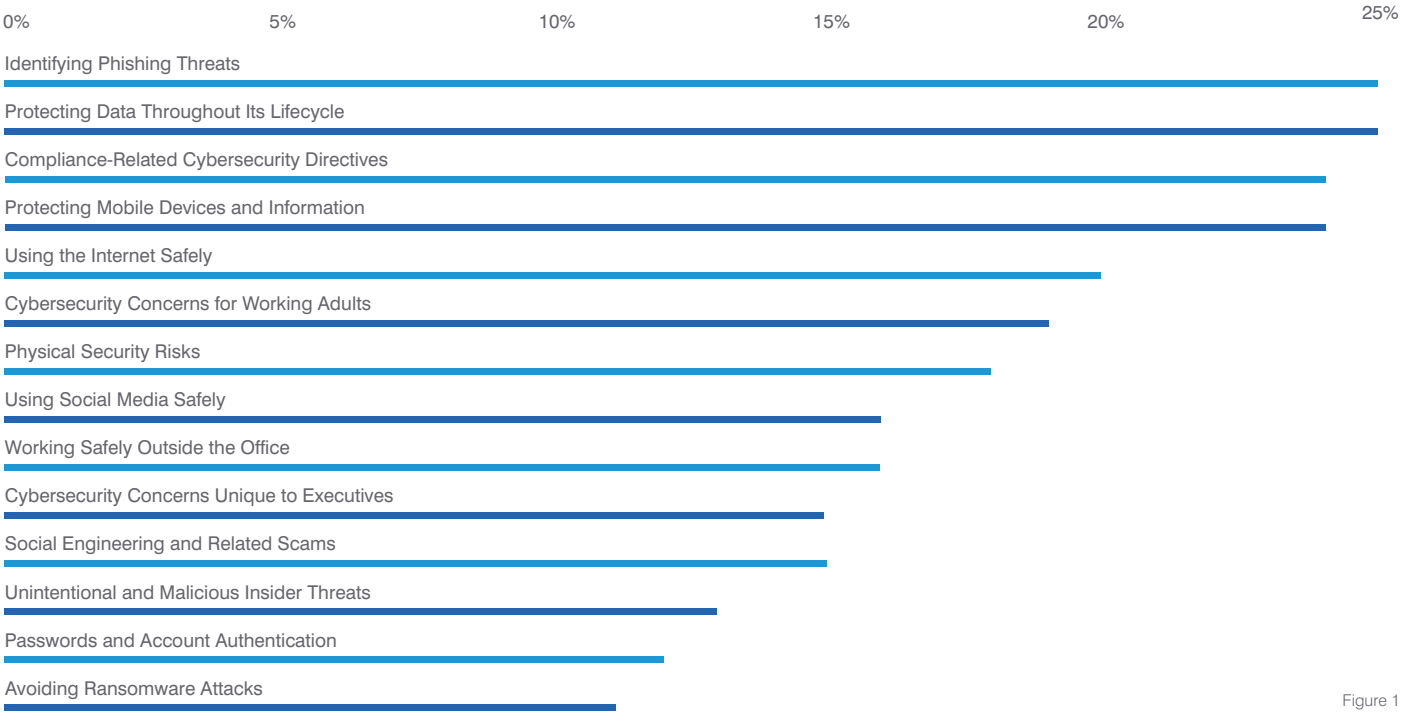

Figure 1

A Note about Ransomware

Much of our data is based on assessments and training that took place in 2018, amid a freefall in email ransomware attacks. With no signs of a ransomware rebound, is training against it a misplaced effort? Hardly. Ransomware could reassert itself at any point. And training users to spot ransomware can help them avoid other types of malware.

SPOTLIGHT: Most and Least Difficult Questions

Users often struggled to answer questions in these topics:

1. Mobile device encryption
2. Protections for personally identifiable information (PII)
3. The role of technical safeguards in preventing successful social engineering attacks
4. Distinctions between private data and public data
5. Actions to take following a suspected physical security breach

But it's not all bad news. Many users mastered these topics:

1. How to identify potentially risky communication channels
2. Physical security safeguards while traveling
3. Recognition of cyber threats such as ransomware and malicious pop-up windows
4. Risks associated with Bluetooth pairing
5. Clean-desk best practices such as "lock before you walk"

CASE STUDY: HOW ONGOING TRAINING INFLUENCES SUCCESS

We have long called for ongoing security awareness training. This research-proven approach can keep users more engaged and help them retain more of what they've learned.

Our Continuous Training Methodology includes regular assessments, education, reinforcement activities and measurement. Our studies have shown this approach can reduce risk in a meaningful way. That's why our own Managed Services team uses it when planning and executing clients' programmes.

To quantify the benefits for this report, we compared two groups:

- End users as a whole
- End users participating in fully implemented Managed Services programmes[2]

Training programme administrators in the first group may or may not apply our Continuous Training Methodology; those in the second group—our Managed Services experts—do.

The results were clear. Users who received quarterly training matched or outperformed the overall averages, in some cases markedly. Figure 2 shows the categories with notable differences.

The users within programmes run by our Managed Services experts performed markedly better in categories related to account authentication and mobile security. Investments in these areas can pay big dividends. As credential phishing attacks and account compromise rise, organisations rely more than ever on users to make good decisions.

Percentage of wrong answers on security awareness training assessments

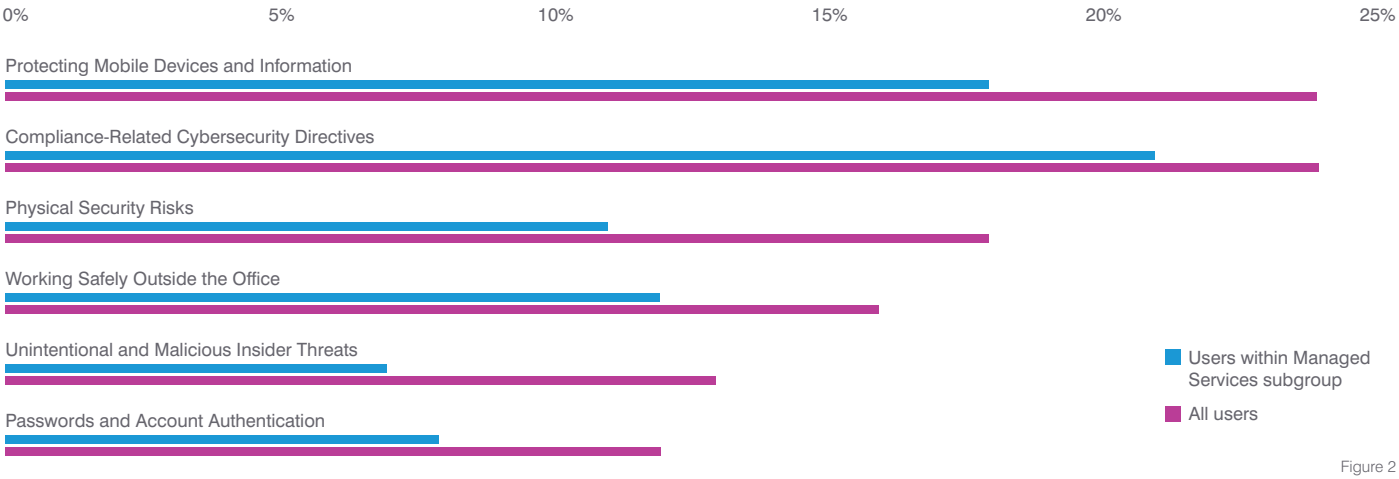

Figure 2

[2] We advise all customers to follow our Continuous Training Methodology. However, some organisations (including those who work with our Managed Services team) are not able to regularly assign training to end users. For our case study, our Managed Services team identified numerous organisations that are fully embracing our methodology, Their results are the source of our case study data.

DEPARTMENT COMPARISONS

For the first time in this report, we analysed users by department.[3] Figure 3 shows the average percentage of incorrect answers across all topic categories by job role.

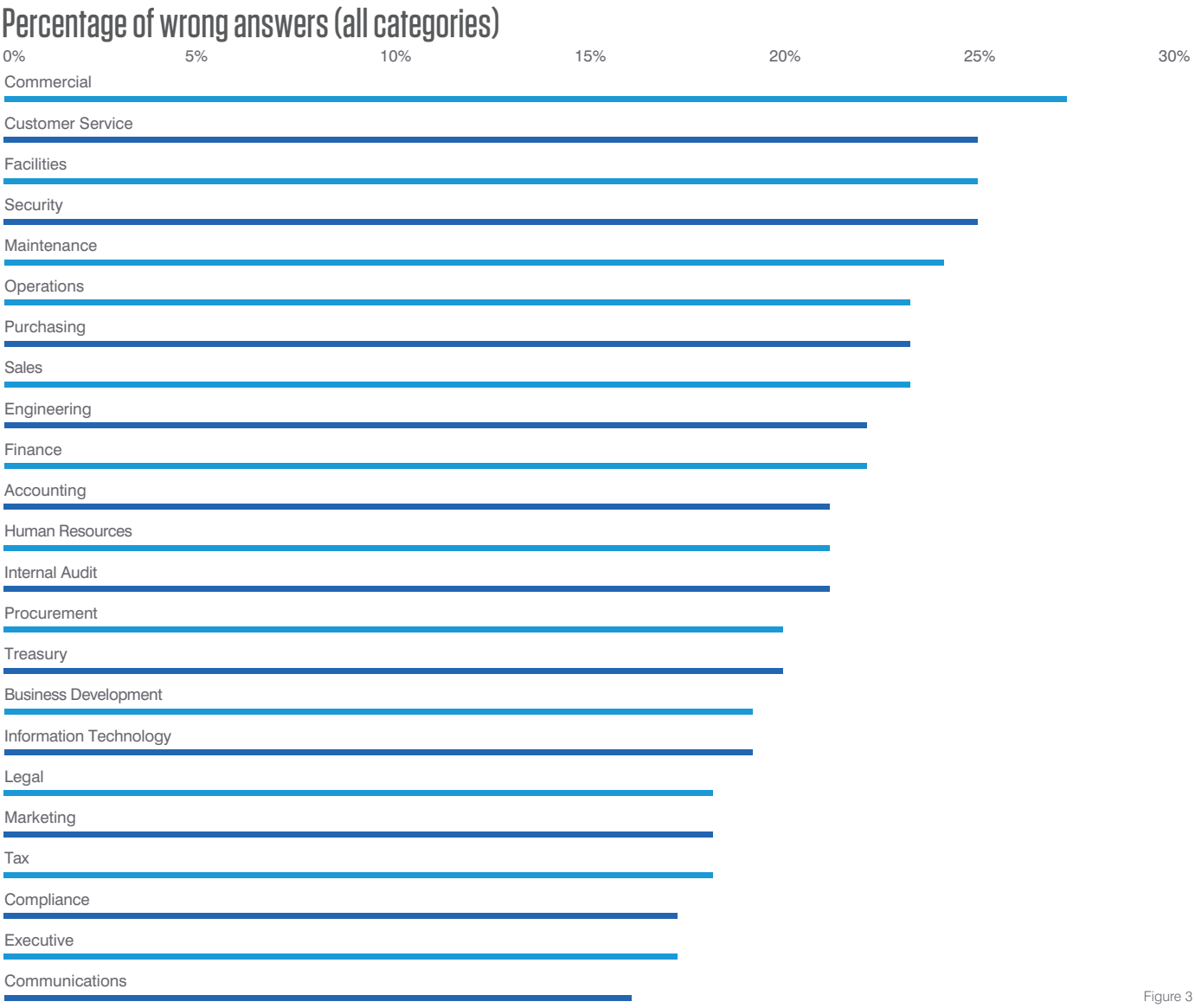

Figure 3

See our 2019 *State of the Phish* Report for average failure rates on phishing tests across these same department designations.

SPOTLIGHT: Executives' Cybersecurity Knowledge

New to our 2019 report is the "Common Security Concerns Unique to Executives" category. It's designed to gauge the cybersecurity knowledge of executives and higher-level managers. The data is based on assessments and in-training quizzes on our "Security Essentials for Executives" module. The specially tailored content covers behaviours that are key to protecting VIPs and other high-profile workers.

We developed training for an executive audience because of a clear and growing need. Executives are often excluded from security awareness training—despite needing it the most. They wield authority. They hold key relationships. And they have access to some of their organisations' most sensitive data. For these reasons, including C-suite members and other top-level workers in every cybersecurity education plan is critical.

[3] These department classifications are solely based on our customers' use of this terminology. We do not have insight into how individual organisations define these groups. This is a subset of our full data set—not all programme administrators group their end users by department. And many use internal terminology for department classifications.

INDUSTRY COMPARISONS

This section highlights user performance across 16 industries.

We examined three key areas:

- Average incorrect response rates across all awareness and training categories
- Best and worst performing industries for each category
- Knowledge levels within specific categories

Average Percentage of Questions Answered Incorrectly

Figure 4 shows the average percentage of incorrect answers, by industry.

Percentage of wrong answers, by industry

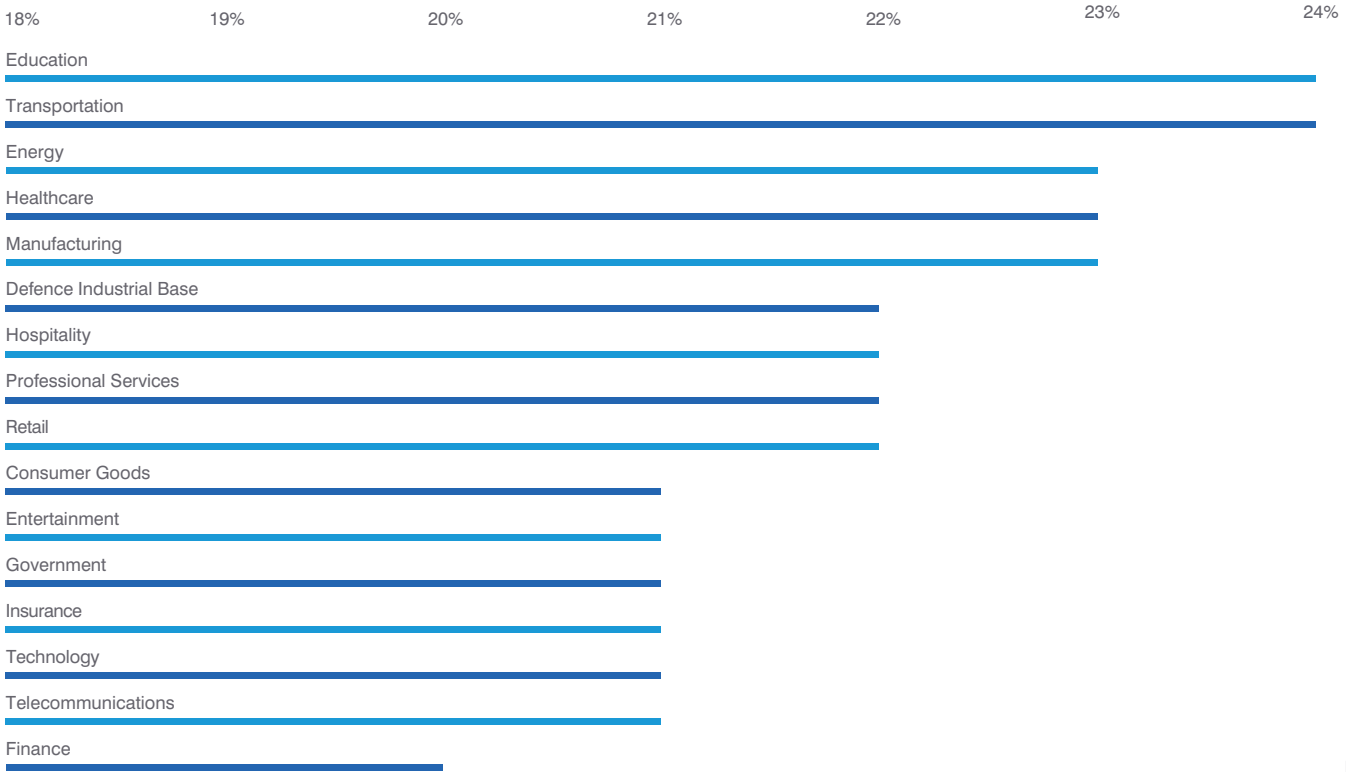

Figure 4

Best and Worst Category Performance by Industry

Figure 5 shows the best- and worst-performing industries for each of our 14 awareness and training categories.

Best- and worst-performing industries

Topic	Best Performer (% of Questions Answered Incorrectly)	Worst Performer (% of Questions Answered Incorrectly)
Avoiding Ransomware Attacks	Insurance **8%**	Defence Industrial Base **22%**
Compliance-Related Cybersecurity Directives	Defence Industrial Base **18%**	Telecommunications **30%**
Cybersecurity Concerns for Working Adults	Insurance **17%**	Education **22%**
Cybersecurity Concerns Unique to Executives	Telecommunications **12%**	Hospitality **17%**
Identifying Phishing Threats	Insurance **23%**	Transportation **27%**
Passwords and Account Authentication	Transportation **7%**	Professional Services **18%**
Physical Security Risks	Education **13%**	Hospitality **22%**
Protecting Data Throughout Its Lifecycle	Defence Industrial Base **16%**	Energy **30%**
Protecting Mobile Devices and Information	Transportation **19%**	Consumer Goods **29%**
Social Engineering and Related Scams	Hospitality **11%**	Education, Energy **18%**
Unintentional and Malicious Insider Threats	Telecommunications **7%**	Education **23%**
Using Social Media Safely	Entertainment **12%**	Defence Industrial Base **31%**
Using the Internet Safely	Education **17%**	Hospitality **24%**
Working Safely Outside the Office	Transportation **13%**	Defence Industrial Base **24%**

Figure 5

Some industries earned bragging rights this year. Insurance users earned the top scores in three categories. And in most other categories, they performed as well as or better than other industries.

Users in transportation also rated highest in three categories:

- Passwords and Account Authentication
- Protecting Mobile Devices and Information
- Working Safely Outside the Office

Still, they struggled most to identify factors related to phishing attacks.

We also saw a mixed bag of results from a couple of industries. Defence industrial base users performed best in two categories: compliance and data protection. But they struggled in three other categories:

- Avoiding Ransomware Attacks
- Using Social Media Safely
- Working Safely Outside the Office

Users from the education sector also had mixed results. They excelled in identifying physical security and internet-based threats. But they did not perform well in three key categories:

- Cybersecurity Concerns for Working Adults
- Social Engineering and Related Scams
- Unintentional and Malicious Insider Threats

Hospitality workers also struggled. They earned bottom marks in three categories:

- Physical Security Risks
- Cybersecurity Concerns Unique to Executives
- Using the Internet Safely

SPOTLIGHT: Hospitality

Last year, end users in the hospitality industry earned the dubious honour of having the highest average rate of wrong answers (24% among the 16 industries we analysed). This year, the sector improved a bit, logging a 22% wrong-answer rate.

Though this uptick is a good sign, the sector is a continuing cause of concern. Hospitality has many security demands. For one, it must protect customers' privacy. It's also expected to provide safe and secure accommodations for customers. And it must protect sensitive data such as credit card information, internal data and more.

Users in this industry didn't perform well in the categories linked to these must-dos. In one, the "Physical Security Risks" category, hospitality users actually had the worst performance of any industry.

(To compare category performance across all topics and all industries, see Figure 6.)

22% wrong-answer rate in 2019. Down from 24% in 2018.

Category Performance for All Industries

Users across all industries struggled with "Identifying Phishing Threats" and "Protecting Data Throughout its Lifecycle," with a 25% error rate for both categories. Overall scores were highest for passwords and authentication, with an 11% error rate overall on average.

Percentage of incorrect answers, by industry

Topic	Average Across All Users	Consumer Goods	Defence Industrial Base	Education	Energy	Entertainment	Finance	Government	Healthcare	Hospitality	Insurance	Manufacturing	Professional Services	Retail	Technology	Telecommunications	Transportation
Avoiding Ransomware Attacks	11%	9%	22%	8%	10%	13%	12%	9%	9%	20%	8%	10%	10%	10%	12%	13%	10%
Compliance-Related Cybersecurity Directives	24%	25%	18%	24%	24%	25%	22%	27%	19%	23%	21%	25%	22%	24%	25%	30%	19%
Cybersecurity Concerns for Working Adults	19%	19%	22%	22%	19%	18%	18%	20%	19%	18%	17%	20%	18%	20%	18%	18%	21%
Cybersecurity Concerns Unique to Executives	15%	16%	17%	17%	15%	14%	15%	17%	15%	17%	16%	16%	13%	16%	15%	12%	13%
Identifying Phishing Threats	25%	25%	23%	26%	25%	25%	24%	25%	26%	24%	23%	27%	25%	25%	24%	26%	27%
Passwords and Account Authentication	12%	12%	9%	8%	11%	11%	10%	11%	10%	15%	11%	11%	18%	15%	12%	12%	7%
Physical Security Risks	18%	18%	18%	13%	20%	17%	20%	18%	20%	22%	21%	18%	14%	11%	17%	14%	16%
Protecting Data Throughout Its Lifecycle	25%	22%	16%	23%	30%	25%	24%	23%	21%	22%	24%	24%	27%	21%	26%	25%	29%
Protecting Mobile Devices and Information	24%	29%	24%	24%	26%	24%	22%	20%	24%	27%	28%	23%	25%	22%	21%	24%	19%
Social Engineering and Related Scams	15%	14%	16%	18%	18%	15%	13%	16%	14%	11%	15%	16%	15%	14%	14%	13%	15%
Unintentional and Malicious Insider Threats	13%	18%	22%	23%	10%	21%	11%	7%	9%	22%	11%	13%	9%	15%	11%	7%	8%
Using Social Media Safely	16%	18%	31%	17%	18%	12%	14%	14%	16%	23%	15%	16%	19%	16%	17%	20%	14%
Using the Internet Safely	20%	23%	18%	17%	21%	22%	19%	21%	18%	24%	20%	21%	19%	21%	20%	22%	19%
Working Safely Outside the Office	16%	15%	24%	14%	17%	16%	15%	16%	15%	23%	15%	17%	14%	16%	16%	14%	13%

Worse — Better

Figure 6

SPOTLIGHT: Compliance Topics

Last year, compliance-related topics proved to be among the toughest for many users. That's still the case, though we did see a bright spot in this year's report.

This year, users showed a better (albeit modestly better grasp) of best practices for complying with GDPR, PCI DSS and HIPAA rules. And their progress came despite expanded (and more challenging) training in these topics.

Note: In 2018, all compliance-related questions were covered in our "Protecting Confidential Information" category. We renamed the category "Compliance-Related Cybersecurity Directives" for this year's report. We made the change to better describe the topics covered.

24% wrong-answer rate in 2019. Down 1 percentage point from 2018.

CONCLUSION AND RECOMMENDATIONS

Regardless of their size, mission or location, all organisations should seek out ways to improve their cybersecurity posture. Unfortunately, many overlook the biggest factor: people.

Cyber criminals continue to focus on people, structuring attacks to take advantage of users who are unaware and unprepared. Organisations must take a people-centric approach as well—and not just to stop external attacks. Not all security incidents are solely the result of an attack; many arise from poor user security practices and a general lack of awareness.

Treat email-based phishing threats with the care and attention they deserve—but take your security awareness training beyond the inbox. Simulated phishing attacks are an excellent tool to assess vulnerability to specific lures and traps. They can also help raise awareness of email-based attacks. But individual phishing examples cannot teach users about the nuances of these threats.

Users need to understand attackers' varied motivations and techniques. And they should appreciate the consequences of each. For instance, credential compromise, malware, and business email compromise are all serious threats. But they have different effects and implications for victims.

Education answers the "why" for users. It helps them make the connection between awareness and action. They see not just how a threat works, but how their behaviours affect security on both a personal and business level. Regular security awareness training is the best way to build users' knowledge. That's true not just of phishing, but of the wide range of security and compliance challenges users face.

To learn more about how Proofpoint can help make your users more aware, prepared and resilient, visit proofpoint.com/security-awareness.

APPENDIX

About Our Categories

These are the 14 categories and related topics analysed for this year's report. We have noted new topics and changes to category names. Except where noted, the changes are meant to better describe the topics covered.

Avoiding Ransomware Attacks

- What ransomware is and the ramifications of a ransomware infection
- Best practices for fighting malware-based cyber attacks

Compliance-Related Cybersecurity Directives

- Cybersecurity practices related to the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA)
- Data management and privacy requirements outlined in these specific standards
- 2018 category name: Protecting Confidential Information

Cybersecurity Concerns for Working Adults

- Cybersecurity issues commonly encountered in workplace situations
- Fundamental cybersecurity best practices
- 2018 category name: Identifying Common Security Issues

Cybersecurity Concerns Unique to Executives

- Cybersecurity issues and critical cybersecurity best practices unique to executive roles
- New category for 2019

Identifying Phishing Threats

- What phishing is and the ramifications of a successful attack
- Recognition of common phishing lures
- Identification of spear phishing and more advanced phishing techniques

Passwords and Account Authentication

- Differences between strong and weak passwords, PINs, and passphrases
- Best practices for password creation and management
- Benefits of using multi-factor authentication
- 2018 category name: Building Safe Passwords (adjusted in 2019 to account for expanded training topics)

Physical Security Risks

- Understanding and application of physical security safeguards
- Recognition of the link between physical security and cybersecurity
- How to identify and prevent physical security breaches
- 2018 category name: Protecting Against Physical Risks

Protecting Data Throughout Its Lifecycle

- General techniques for handling personal information at all stages of the data lifecycle
- Proper management and destruction of sensitive electronic and paper files
- Safe use and disposal of USB drives and other storage media
- 2018 category name: Protecting and Disposing of Data Securely

Protecting Mobile Devices and Information

- Best practices for securing mobile devices and mobile data
- Recognition and avoidance of unsafe mobile applications

Social Engineering and Related Scams

- Understanding of common social engineering techniques
- Identification and avoidance of electronic, phone-based, and in-person scams
- 2018 category name: Protecting Yourself Against Scams

Unintentional and Malicious Insider Threats

- Advice on recognising insider threats and the best practices to protect against them
- Real-world actions and examples that help mitigate malicious threats
- Scenario-based learning around everyday actions that cause—and prevent—unintentional threats
- New category for 2019

Using Social Media Safely

- Principles of "safe sharing" on social media platforms
- Identification and avoidance of social media imposters and unsafe content

Using the Internet Safely

- Recognition and avoidance of risky websites and online content
- Best practices for safer web browsing

Working Safely Outside the Office

- Best practices for remotely accessing corporate networks and systems
- Identification and avoidance of threats when travelling and/or working remotely

About Our Report Methodology

Data for this report draws on our CyberStrength Knowledge Assessments and security awareness training assignments in our Security Education Platform. This SaaS-based learning management system helps programme administrators plan and execute cybersecurity education programmes. We analysed nearly 130 million answers given by our customers' end users between January 1, 2018, and February 28, 2019.

Category averages are calculated individually. Overall averages that aggregate categories, industries and others are not weighted. For that reason, they will not match an "average of averages."

For example, the overall average percentage of wrong answers across all users in all categories was 22%. That figure was determined by dividing the total number of incorrect answers by the total number of questions answered.

Within each category, the wrong-answer percentages were calculated in a similar way. But because each category has a different number of total questions, the average of category or industry scores does not equal the overall average.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

proofpoint.

Security Awareness Training

0619-005