MediaPRO
Cybersecurity & Privacy Education

2018 State of Privacy and Security Awareness Report

INTRODUCTION

Our State of Privacy and Security Awareness Report is back for a third year in a row, having originally been launched in 2016 due to the need to gain a better understanding of the cybersecurity knowledge of today's workforce.

Fast forward to 2018, and the need for such a resource has never been more important. Human-caused data breaches are still making headlines, and phishy emails are still letting the bad guys in. Increasingly popular cloud-storage tools are making it easier than ever to put sensitive data at risk, IOT devices are providing new inroads for the bad guys, and new breeds of malware continue to evolve on a daily basis. One thing connects these threats: the role that employees play in keeping their organizations secure. So, without further ado, we're pleased to announce the results of the *2018 State of Privacy and Security Awareness Report*.

SURVEY METHODOLOGY

We surveyed 1,024 U.S. employees in August of 2018 to test their cybersecurity and data privacy know-how. Respondents were asked a variety of questions based on real-world scenarios in eight threat vectors:

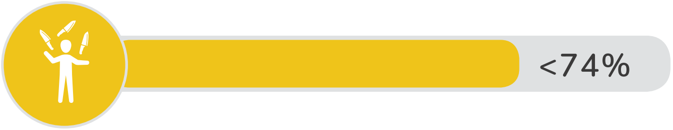
- Incident Reporting
- Physical Security
- Identifying Malware
- Cloud Computing
- Identifying Personal Information
- Phishing Awareness
- Working Remotely
- Acceptable Use of Social Media

Based upon their responses, we assigned them to one of three different risk profiles, which indicate the survey-taker's privacy and security awareness IQ. The three risk profiles—**Risk, Novice, and Hero**—are based on the percentage of privacy- and security-aware behaviors correctly identified. The more correct behaviors an employee can identify, the less of a privacy and security risk they represent. We broke out each risk profile by the percentage of questions answered correctly, displayed at the right.

Risk Profiles

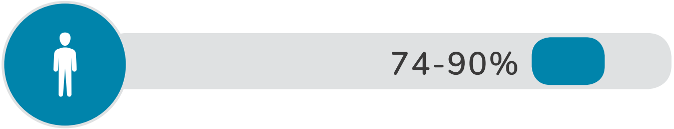
RISK (0-23)*

These individuals put their organizations at serious risk for a privacy or security incident.



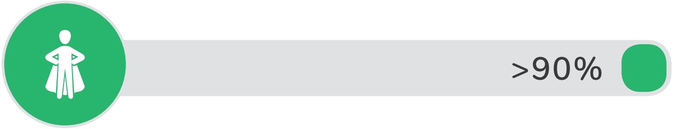
NOVICE (24-28)*

These individuals have a good understanding of the basics, but could stand to learn more.



HERO (29-31)*

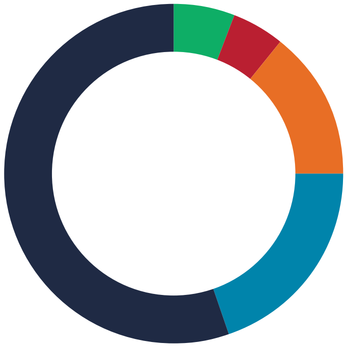
These individuals know their stuff and are likely assets to their organization's security posture.



**Range of questions answered correctly, out of 31*

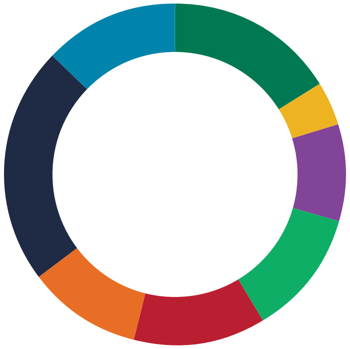
SURVEY RESPONDENTS

Responses were collected from a variety of employee populations, company sizes, and industry sectors. The breakdown of respondents by organization size, industry, and job level is as follows:



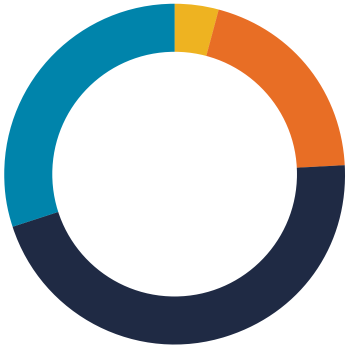
ORGANIZATION SIZE

● 0 - 1,000	55.5%
● 1,001 - 5,000	19.6%
● 5,001 - 20,000	14.4%
● 20,001 - 50,000	4.8%
● 50,000 +	5.8%



INDUSTRY

● Finance	12.9%
● Technology	22.5%
● Healthcare	10.7%
● Professional Services	12.7%
● Retail	11.9%
● Education	9.2%
● Government	4%
● Other	16%



JOB LEVEL

● Entry-Level	29.5%
● Mid-Level	46%
● Management	19.9%
● Executive or above	4.5%

EXECUTIVE SUMMARY

The 2018 State of Privacy and Security Awareness report analyzed responses to scenario-based questions across eight threat vectors.

Notable Findings:

Employees this year performed worse than in 2017 across all eight threat vectors. Specifically, those surveyed did significantly worse in identifying malware warning signs, knowing how to spot a phishing email, and practicing social-media safety.

75% of respondents struggled with identifying best practices related to correct behaviors in cybersecurity and data privacy. Three-quarters of respondents were given either a "Risk" or "Novice" profile—indicating that they exhibited behaviors that put their organization at risk of a security or privacy incident. This is a 5% increase from the year before.

25% of employees achieved the "Hero" profile. These individuals know their stuff when it comes to security and privacy and exhibited less risky behaviors relating to avoiding malware, steering clear of phishing emails, and keeping sensitive data secure.

Employees in the finance sector performed the worst of the seven industry segments analyzed, with 85% of finance workers showing some lack of cybersecurity and data privacy knowledge.

Employees in management roles or above showed riskier behaviors than entry- or mid-level employees. 77% of respondents in management showed a general lack of awareness, while 74% of those in subordinate positions scored the same.

14% of employees lacked the ability to correctly identify phishing emails. This is a notable increase in respondents who showed risky behaviors when it came to phishing attempts from our 2017 survey, in which 8% of employees struggled in this area.

Only 58% of respondents overall could define business email compromise (BEC), suggesting a concerning lack of awareness surrounding this common social-engineering tactic.

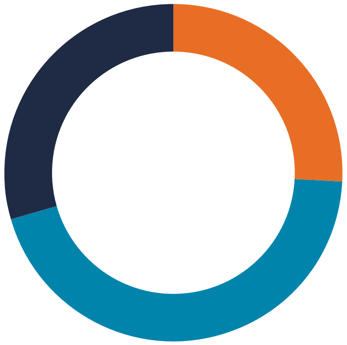
20% of employees did not report a variety of theoretical risks to security and privacy, such as unsecured sensitive data and malware-infected computers.

26% of employees made poor decisions involving the secure use of social-media, such as sharing as-yet-unreleased product information from their organization.

EXECUTIVE SUMMARY (CONTINUED)

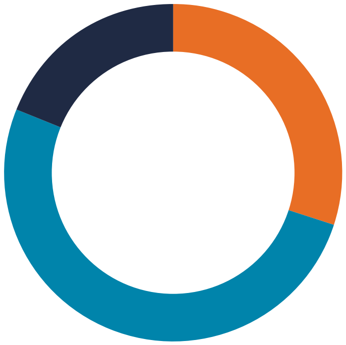
Year-Over-Year Comparison

Percentage of respondents who scored into each segment:



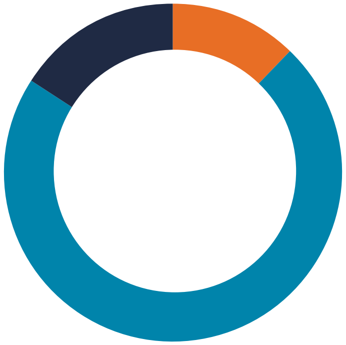
2018

● Risk	30%
● Novice	45%
● Hero	25%



2017

● Risk	19%
● Novice	51%
● Hero	30%



2016

● Risk	16%
● Novice	72%
● Hero	12%

STATE OF AWARENESS IN DETAIL

Get the details on what employees did and didn’t know in each threat vector, plus comparisons of this year’s results to our last two reports.

INCIDENT REPORTING

Will Employees Say Something When They See Something?

The InfoSec news is filled with countless stories of malware sitting on servers unnoticed and data breaches going unreported for weeks, sometimes months. With the average cost of a data breach topping out at $3.9 million in 2017, organizations cannot risk increasing this already staggering cost with a workforce uninformed about responsibly reporting cybersecurity and data-privacy incidents.

Our Findings

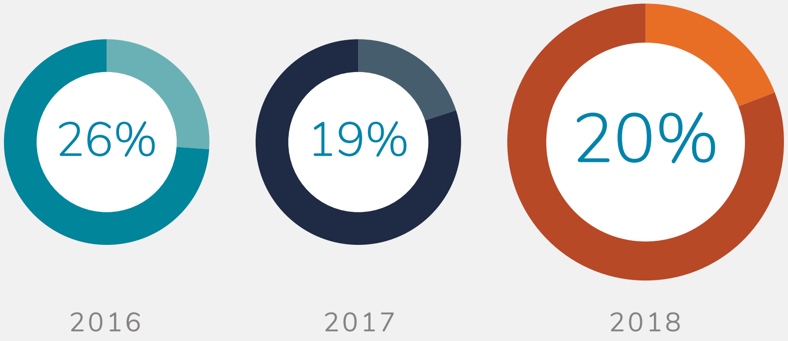
In our findings, one-fifth of employees did not report a variety of theoretical risks to security and private data, as they should have. These include unsecured personnel files, unsecured confidential product information, and potentially infected computers. Though performing worse than last year, respondents in this year's survey fared significantly better than those in 2016 (20% vs. 26%).

Financial-sector employees proved the least knowledgeable in this threat vector, with a quarter of respondents showing risky behaviors overall. Specifically, one out of five finance employees failed to report finding an unlocked file cabinet filled with sensitive files.

Why You Should Care

Employees at organizations of all sizes should should feel comfortable with and understand the proper guidelines for reporting any incidents they feel might pose a threat to their company's security or data-privacy posture. A reported event that turns out to be nothing will likely do little harm, while a true cyberthreat discovered too late could have disastrous consequences. An organization that fosters a culture of incident reporting is a more secure one.

Year-Over-Year Risk Score Comparison:



Do Employees Know to Let the Right One In?

Though the connection between physical and logical security has grown in recent years, the on-the-ground aspect of cybersecurity and data privacy should not be overlooked. According to Verizon Enterprises' 2018 Data Breach Investigations Report (DBIR), one out of 10 breaches still involved physical actions, such as stealing hardware or other equipment.

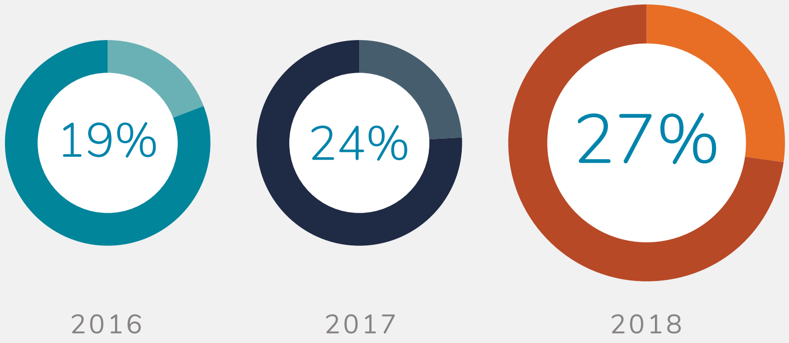
Our Findings

When asked questions about controlling access to their organization's building (i.e. holding the door for someone unrecognized, also called "tailgating,") **almost a third of survey respondents indicated they'd take risky actions**. Specifically, 23% of respondents said they would hold their office door open for someone who asked to enter, even though they didn't have the proper identification. Based on the previous years' findings, employees have gotten worse at recognizing potential physical security threats finding their way in through the office front door.

Why You Should Care

The modern work environment has become a sea of plastic access cards hanging from beltloops and slung from lanyards. These security measures can seem like overkill, but threats against an organization's data are not limited to just those coming from hackers and cybercriminals. An unexpected delivery or a friendly looking stranger trying to access your office should be addressed with caution and allowed entry only through approved methods, such as being accompanied by authorized personnel.

Year-Over-Year Risk Score Comparison:



Can Employees Spot an Infected Computer?

As many as 350,000 new types of malware are discovered *each day*, according to industry researchers. Other data from the Ponemon Institute shows that it can take, on average, 170 days for malware to be detected once it gets in. That's close to half a year of potential damage done before the organization even notices.

Our Findings

Unfortunately, our research points to the need for improvements in the average employee's ability to detect a malware infection during their workday. **Overall, close to one-fifth of employees failed to recognize at least one of four possible signs of a malware-infected computer**.

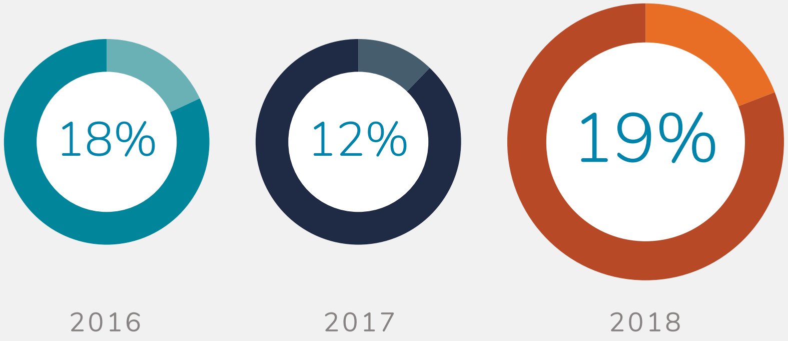
The malware sign most misidentified was a slow computer, which nearly a third of respondents (31%) overlooked as a potential indication that the computer had been infected. Multiple web searches ending at the same address was the sign correctly identified most often—87% of employees said this was a clue malware had infected their computer. Though 2016 to 2017 saw improvements in recognizing potential malware signs, this year's respondents did worse than both previous years.

When broken out by job level, managers and executives performed worse, coming in at 25% compared to 18% of lower-level employees. The finance sector proved the worst of the seven industries, with almost a third of financial employees missing signs of possible malware infection.

Why You Should Care

Though ransomware, with its screen-locking, brightly colored warnings that a computer has been infected, is becoming more rampant, not all signs of malware infection are this obvious. Signs such as a sluggish computer, anti-virus software mysteriously turning off, and misbehaving browsers should not be overlooked. One of the best early warning systems is a sharp-eyed employee population keeping an eye out for signs like this.

Year-Over-Year Risk Score Comparison:



Where Are Your Employees Stashing Sensitive Data?

"In the cloud" has become a way of life. One cloud storage firm found that employees use, on average, 28 different cloud sharing or collaboration apps. However, they also found that 16% of files uploaded to file sharing services contain sensitive information.

Our Findings

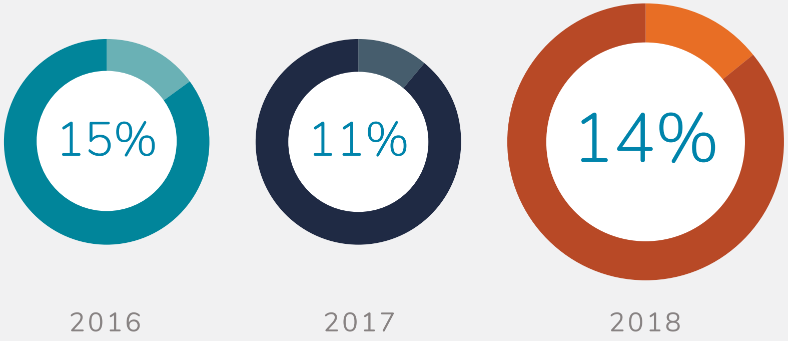
We based this section of the survey on a common occurrence most employees have likely encountered involving personal cloud storage and the potential dangers associated with it. In a scenario in which respondents were working in a public space with a laptop about to run out of battery power, **14% of employees incorrectly chose to either store a confidential work document on their personal cloud storage account or transfer it to their mobile device to work on later.** Seventy-one percent of respondents chose the safest action in this scenario, which was to delay work involving the document until back at the office.

Management-level employees were almost twice as likely as their mid- and -entry-level colleagues to choose the risker option in this scenario (21% vs. 12%), perhaps speaking to the increased demands on time and nontraditional work schedules higher-level employees can have. One in four finance industry workers who took the survey also took risky actions, the highest percentage of all seven industries surveyed.

Why You Should Care

Despite the ease of "putting it in the cloud," the risks of storing anything that could even be considered confidential on personal cloud storage are too great. Not only does such behavior leave an organization open to loss of IP and other valuable data, but lawsuits and reputational damage are other very real possibilities. Employees need a strong understanding of both these dangers overall and their individual organizations' cloud storage policies.

Year-Over-Year Risk Score Comparison:



Do Your People Know Personal Data When They See It?

Personal information can take many forms. Social Security numbers and tax information are the most obvious, but even something as innocuous as a password hint left for all to see in a work space can have serious consequences. Such a hint could be used to access not just work networks but provide a gateway into the personal data of the employee in question.

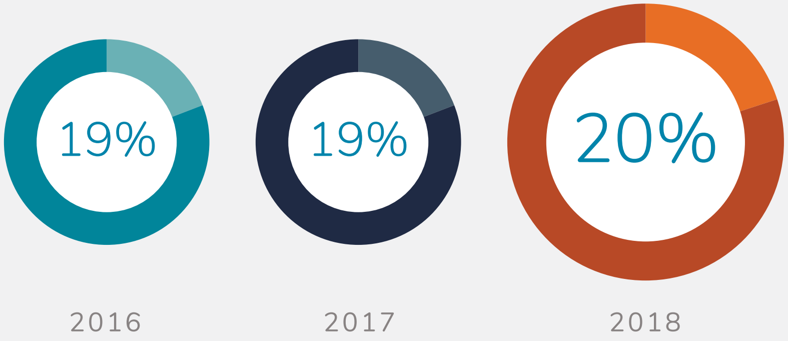
Our Findings

When asked how best to dispose of a variety of different types of sensitive information, 20% of employees chose the riskier of the two options (either disposing of unneeded personal information in a shredder or an unsecured trash bin). In one scenario, 59% of respondents chose to discard a password hint left in public view in the trash, rather than in a shredder. Fortunately, the vast majority of respondents correctly choose to discard unneeded documents containing employee Social Security numbers and driver's license information in a secure shredder.

Why You Should Care

Data has become the new oil in our digital world, but sensitive information should not be treated as solely a commodity to be bought and sold. Sensitive information, such as birthdates, addresses, and Social Security numbers, means the well-being of real people—your clients, employees, and coworkers. According to one industry report, identity thieves with access to sensitive data defrauded 15.4 million people of $16 billion in 2017. Separate from these personal tolls, sloppy handling of this information can lead to fines, revenue loss, and irreparable corporate reputational damage.

Year-Over-Year Risk Score Comparison:



A Deep Dive into a Persistent Threat

The dangers of phishing attacks are difficult to overstate. According to the 2018 DBIR, 92% of malware was still delivered by email. Researchers at Symantec have found that the average person gets 16 malicious emails per month. Industry report after industry report continues to show both the prevalence of this specific form of social engineering and its enduring success. After all, cybercriminals wouldn't keep hitting this attack vector if it wasn't getting them want they want: access to valuable sensitive data through malware intrusion or simply tricking people into sending this information directly.

Our Findings

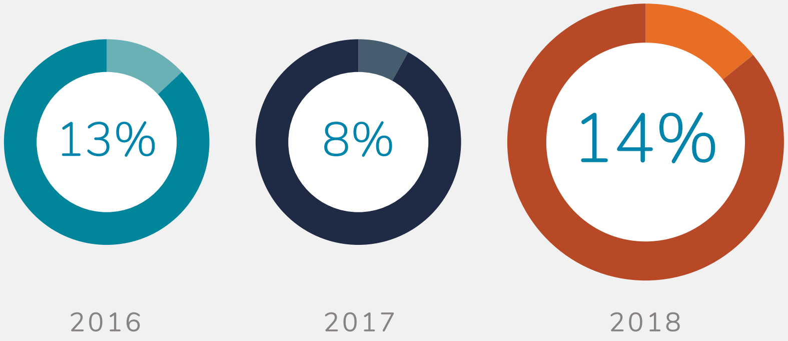
With phishing this much of a threat, we wanted to again explore the average employee's ability to identity phishing emails in an everyday, office-based scenario, as we have in our previous two annual reports. New to this year's report, we asked three multiple-choice, general-knowledge questions about phishing to dive deeper into the average employee's knowledge of this most widespread cyberthreat.

When asked to mark four example emails as either legitimate or phishing attempts, **14% of employees failed to identify true phishing emails**. For the second year in a row, an email purporting to be from a famous investor offering a hot stock tip proved to be the trickiest, with one out of five of respondents failing to report it as phishing.

Unfortunately, the data shows an overall breakdown in the ability to correctly identify email phishing attempts among respondents this year compared to those last year.

Nearly a quarter of respondents who described themselves as management-level or above (23%) showed a lack of awareness of the phishing examples presented, performing far worse than their entry- and mid-level counterparts (11%). Across the industry sectors we analyzed, finance employees again showed the riskiest behaviors, with a quarter of respondents in this segment lacking the ability to recognize at least one of the four phishing attempts presented. Interestingly, 38% of finance employees marked the sample phishing attempt describing a stock tip from a famous investor as legitimate.

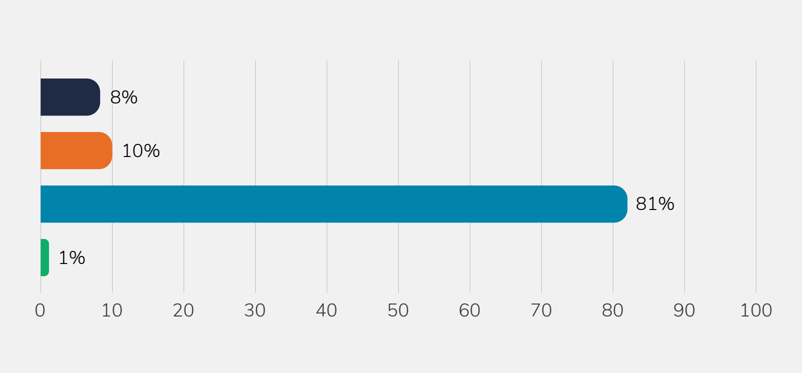
Year-Over-Year Risk Score Comparison:



Turning to the general-knowledge questions, the overall responses came in as follows:

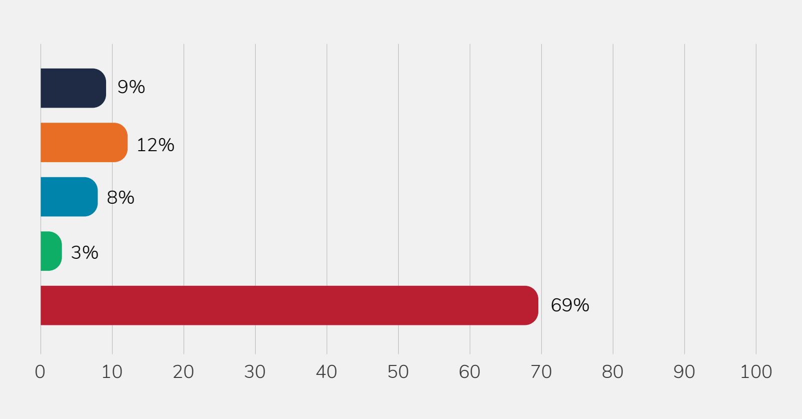
Which Action Below Is the Most Correct Response to a Suspected Phishing Email?

- Clicking a link in the email to investigate the legitimacy of the website it leads to
- Opening an unexpected attachment to verify its contents
- Reporting the email to your IT department *(correct response)*
- Replying to the message directly to see who it's from



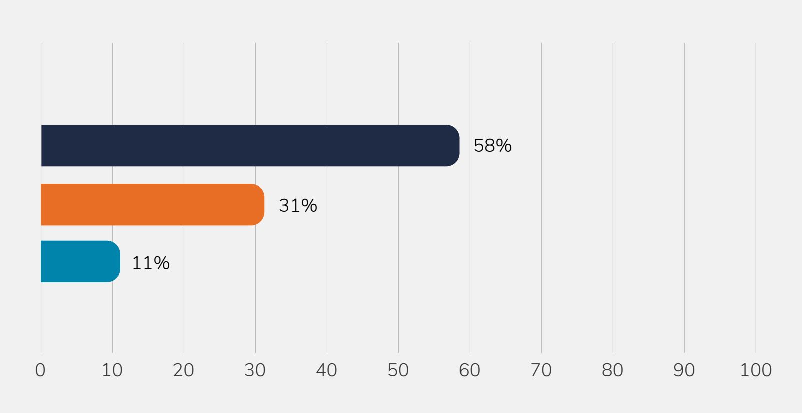
Which of the Following Is a Common Goal of Phishing Emails?

- Login credential theft
- Tricking user to open malware payload
- Revealing sensitive or financial information
- Wire transfers
- All of the above *(correct response)*



Which Description Below Best Defines Business Email Compromise?

- An attacker gaining access to a company's email system and sending emails masquerading as the company's CEO *(correct response)*
- A hacker using a fake company name and logo to craft a phishing email
- A CEO mistakenly sending sensitive information to the wrong person

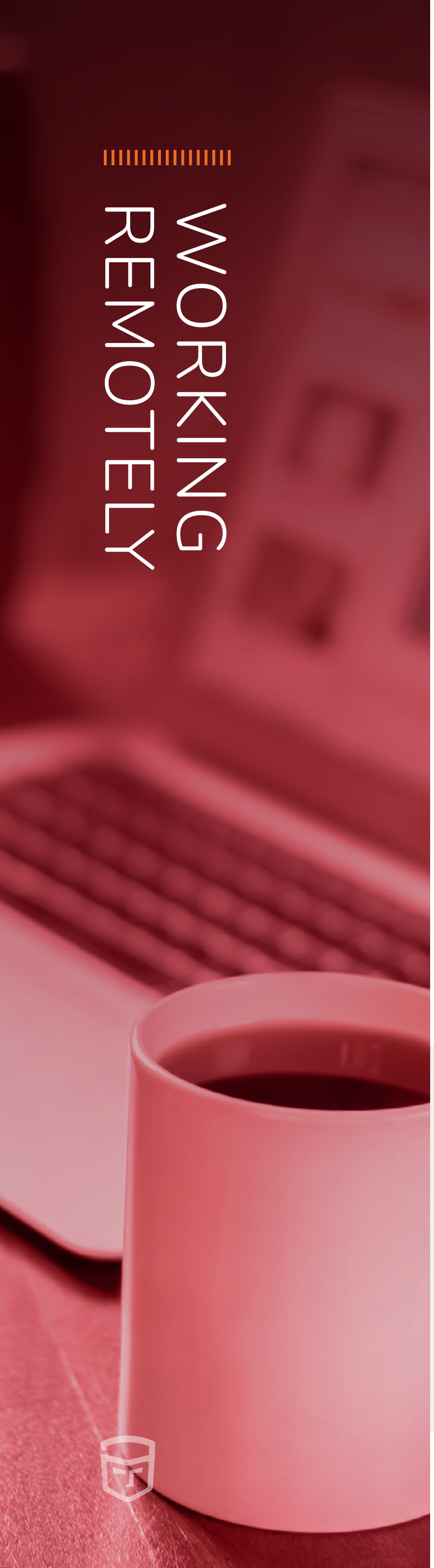


Overall, these questions revealed a reasonable level of knowledge amongst the average employee represented in the survey, but there were areas where improvements are needed. Some weak spots included:

- Only 58% of respondents overall could define business email compromise (BEC), suggesting a concerning lack of awareness surrounding this common social engineering tactic.
- Only 53% of respondents who self-described as management or above correctly identified BEC, faring worse than those in entry or mid-level positions (59%).
- Though the vast majority of respondents overall (81%) correctly chose to report a suspected phishing email to their IT teams, this still leaves 18% who elected to either open an unexpected attachment (10%) or click a link in a suspected phishing email to see where it goes (8%). Either of these actions could compromise a company's network, leading to leaked sensitive data or malware intrusion.
- Management and higher performed worse than their entry- and mid-level counterparts when asked what they should do with a suspected phishing email (69% vs. 86% choosing the correct answer). Specifically, nearly one in six management-level respondents (17%) chose to open an unexpected attachment connected to a suspected phishing email.
- Overall, finance employees fared the worst on these questions. Nineteen percent of finance sector employees thought opening an unexpected attachment was an appropriate response to a suspected phishing email, while 16% chose to click a link in such an email to investigate its legitimacy.

Why You Should Care

Given the ubiquity of phishing emails, any lack of awareness concerning this cyberthreat should be cause for worry. As the authors of the DBIR wrote in their 2018 report (in which 96% of breaches and other incidents were tied to phishing emails), "The vampire only needs one person to let them in." In particular, the scourge of BEC– relying on emails spoofing requests by higher ups to send tax information and other sensitive data– shows no signs of letting up. According to the FBI, BEC-related financial losses have reached $12.5 billion globally. Long story short: suspected phishing emails are nothing to take lightly.



Will Employees Stay Secure When Out of Office?

For better or for worse, working outside of the traditional office setting has become more common place. Workplace industry research has found that as many as 4.3 million employees work remotely or from home at least half the time, a 140% increase from 2005. Although the ability of employees to easily bring work with them to places like cafés or other public locations could lead to increased productivity, though such practices also introduce the risk of data breaches and other cyber incidents.

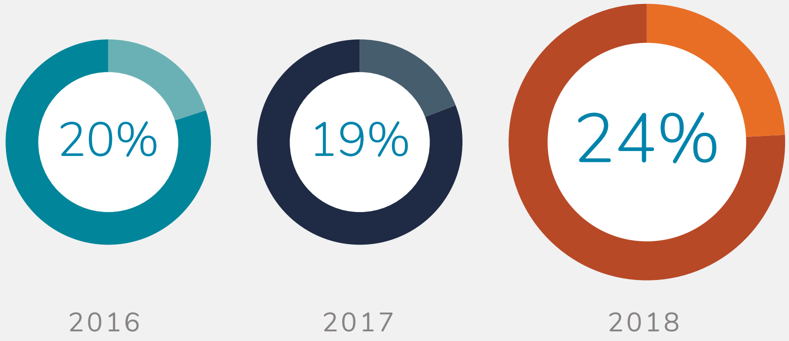
Our Findings

When asked about the most secure actions to take in scenarios involving working remotely on work-related tasks, almost a quarter of employees surveyed chose risky ones. In one scenario, 21% of respondents ignored the potential dangers of free, public Wi-Fi available in a café and chose to complete work tasks using this internet connection. In a separate scenario, 84% of respondents correctly identified connecting to their company's VPN while using public Wi-Fi as a security measure that should be taken.

Why You Should Care

The possibilities of bad actors using an unsecured, public Wi-Fi hotspot to intercept data being sent between connected computers and the router are all too real. Firm corporate policies should be put in place to ensure employees use your company's VPN, make sure any sites visited have HTTPS as part of the URL, and keep accessing any sensitive information to a minimum.

Year-Over-Year Risk Score Comparison:



Do Employees Know What Sharing Responsibly Looks Like?

The impact of social-media on our everyday lives is immense; something unimaginable even just 10 years ago. According to one report, [64% of internet users worldwide (3.6 billion people)] are active on social-media, with 77% of employees admitting to using social-media while on the clock. Separate from clicking malicious links spread socially, the pitfalls of irresponsible social-media use include damage to a company's organization due to an inappropriate post or re-share or the unintended release of proprietary information.

Our Findings

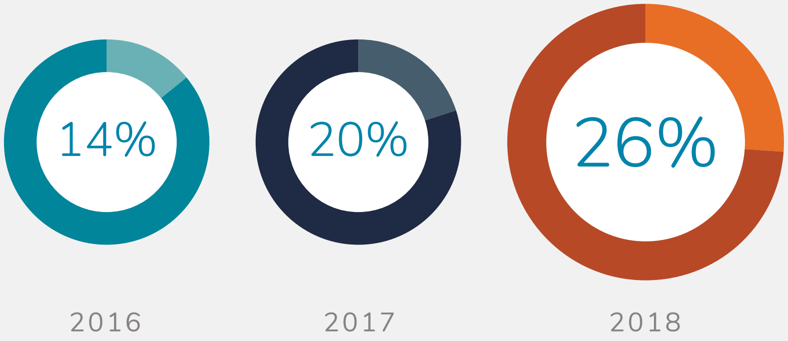
Across four scenarios presented involving safe and secure use of social-media in our survey, just more than one in five employees made poor decisions. These included actions that could harm an organization's reputation, such as re-tweeting a coworker's sarcastic tweet about a competitor (23% thought this appropriate) and boasting on Facebook about an as-yet-unreleased new product offering (16% thought this appropriate).

Of all eight threat vectors analyzed, responsible social-media use produced the broadest difference in knowledge between management and above and mid-to-entry-level employees. **Just more than a third (36%) of managers executives chose risky actions related to social-media, while 23% of lower-level employees made the same choices.** Finance employees once again proved the worse at identifying responsible practices related to social-media, with 39% taking actions that could harm their organization's reputation.

Why You Should Care

The benefits of near-instantaneous communication and the potential for positive social change inherent to social-media come with a dark side. Being too quick to share can have lasting negative impacts not just on your company, but the personal lives of employees, too. The ubiquity of social tools demands clear policies laying out rules for accessing social-media at work and what should be shared and posted on behalf of the company.

Year-Over-Year Risk Score Comparison:



CONCLUSION

The overall results of this report revealed a trend we weren't happy to see: employees performing worse across the board compared to the previous year. The lack of awareness when it came to phishing emails was particularly troubling. We put more of a focus on phishing this year because of the massive thorn in the sides of IT managers and CISOs it represents. The added focus given to phishing in our survey unfortunately revealed additional weaknesses.

This lack of phishing awareness is troubling for two reasons. One, phishing as a threat is not going away any time soon. Two, susceptibility to phishing can represent a fundamental misunderstanding of security best practices at an organization-wide level. Technical safeguards against phishing attempts are important, but they cannot take up the slack left by a fundamental lack of security awareness in an employee base. If an employee falls for a phishy email, chances are security best practices are not top of mind.

An additional surprise was the overall struggles with security and privacy awareness exhibited by the financial sector employees who took our survey. This is worrisome because industry research continues to show that the financial sector is hit disproportionately hard by cybercriminals. Though industry analysts report billions of dollars in cybersecurity spend for the finance industry, much of this money is poured into strictly technological solutions. But millions (or billions) of dollars to beef up merely the technical side of an organization's information security strategy could be ill-spent if investments are not made in security and privacy awareness training programs that increase knowledge retention and minimize risky behavior.

But it's not all doom and gloom. Rather than litany of woes on how much the average employee still has learn when it comes to cybersecurity and data privacy best practices, this report should be taken as a roadmap for a robust security and/or privacy awareness initiative—one that will lead to real behavior change. Such changes are not achieved overnight, nor are they earned through one-off employee awareness training on security and privacy topics. Employee education is only achieved through varied training content and delivery methods, deployed on a repeating basis. When behavior change is achieved, it will be evident in employees combining policy know-how, common sense, and a keen eye for detail as they regularly align their actions with your organization's security and privacy principles.

TIPS FROM THE SECURITY AWARENESS EXPERTS AT MEDIAPRO

No matter the company size or industry sector, cybercrime and threats to sensitive data can impact anyone. The common thread among the threat vectors analyzed in this report, and others encountered in the real world, is the vital role humans play in thwarting attacks across these areas. Read on for tips meant to be shared with your workforce and advice for those responsible for security and privacy awareness.

Tips from the Security Awareness Experts at MediaPRO

	For Awareness Managers	For Employees
INCIDENT REPORTING	Include real-life examples of reportable incidents into employee training, in addition to information about company policies.	Report any potential security/privacy incidents to the right authority, be it your IT department, human resources manager, or your direct supervisor.
PHYSICAL SECURITY	Describe what's at stake in terms of both company and personnel well-being if an unauthorized person were given access to your work environment.	Be on guard for suspicious actions wherever you encounter them, even in the non-cyberworld. Always seek independent verification that attempts to get information—or get into your workplace—are legitimate.
IDENTIFYING MALWARE	Make clear that even seemingly minor unexpected computer behaviors could be signs of malware infection, include discrete steps to take if malware is suspected, and drive home the importance of regular software updates.	Take all necessary steps, such as regular software updates, to keep malware off your work and home computers. Keep an eye out for signs of malware, like pop-ups, blue screens, and system slowdowns.
CLOUD COMPUTING	Differentiate between storing personal information on cloud storage and using cloud tools for work information.	Take the time to understand how your organization uses cloud storage, and follow your employer's guidelines. Overall, carefully choose what kinds of information you place "in the cloud" and create secure passwords for your personal cloud sites.
IDENTIFYING PERSONAL INFORMATION	Connect the facts and figures found in the personal information your company may handle to the tangible, real-world consequences the compromise of such data would lead to.	Internalize your company's data privacy policies and report potentially exposed private data when you see it.
PHISHING AWARENESS	Consider engaging a simulated phishing tool that connects to lessons describing signs that an unexpected email should be considered suspicious.	Scrutinize every email you receive for signs of phishing (whether on mobile or desktop), and never click links or download files until you've taken the time to verify that they are safe.
WORKING REMOTELY	Explain the importance of using your company's VPN when working out of the office and describe the methods cybercriminals can use to intercept data shared across unsecured networks.	Always look at websites to be sure they are secure (look for https://), use only Wi-Fi networks that offer password protection, and use VPN connections to connect to work networks.
ACCEPTABLE USE OF SOCIAL MEDIA	Present both the good and bad of social-media use and employ real-life examples of the kinds of social posts that can put both individual employees and the company as a whole into hot water.	Follow your employer's guidelines on posting about company matters on social-media. Take full responsibility for what you share and whom you share it with.

ABOUT MEDIAPRO

MediaPRO, headquartered in Bothell, WA, is nationally recognized for working with Fortune 500 companies and mid-sized businesses to produce employee security and privacy awareness training programs that reduce human risk and improve employee behaviors. MediaPRO's suite of LearningLAB products are used by the most risk-aware companies in the world, have won more than 100 e-Learning awards, and have earned a place as a Leader in Gartner's Magic Quadrant for Security Awareness Computer-Based Training. For more information, please visit www.mediapro.com, or follow MediaPRO on LinkedIn, Facebook, Twitter, and Google+.