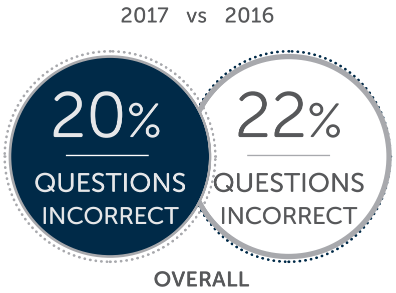
Wombat Security's 2017

BEYOND™ THE PHISH

Report

wombat® security technologies

#BeyondthePhish

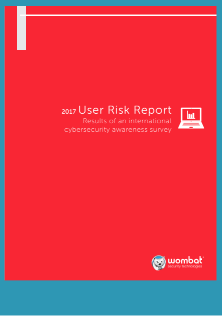


# Beyond the Phish

Check out our **User Risk Report** for results from an international cybersecurity awareness survey.

info.wombatsecurity.com/user-risk-report

TIP!


2017 User Risk Report
Results of an international cybersecurity awareness survey

wombat

It is standard knowledge for infosec professionals worldwide that cybercriminals are exploiting email-based attacks for their own gain. As pioneers in the development and use of simulated attacks, we recognize that anti-phishing training is as important now as it ever was. Spear phishing, business email compromise (BEC), and email-based ransomware are keeping response and remediation teams on their toes. But these are far from the only ways attackers can gain a foothold within an organization or compromise sensitive data and systems.

Our second annual *Beyond the Phish*™ *Report* features results from **more than 70 million questions answered** by our customers' end users from ten categories within our CyberStrength® Knowledge Assessments and our interactive training modules. We highlight strengths and weaknesses tied directly to phishing but also go **beyond the phish** to analyze knowledge of other business-critical best practices, including data protection measures, mobile device security, safe social sharing, and password hygiene.

Though we did see a modest overall improvement from the rate of questions answered incorrectly in 2016 — **20% vs. 22%** — gains in some areas were offset by losses in others. This year's report offers **year-over-year comparisons** at the category level, as well as analysis of **weaknesses by industry** and insights into some of the specific questions users were most likely to answer incorrectly. We also provide data about a new category — Protecting Yourself from Scams — which focuses on end users' understanding of common social engineering techniques that are used across a variety of attack vectors.

Also new this year are highlights from our *2017 User Risk Report*, which compiled results from an **international third-party survey of 2,000 working adults — 1,000 in the US and 1,000 in the UK** — and revealed common cybersecurity behaviors in areas similar to those assessed in our *Beyond the Phish* data.

While not a scientific study, this report offers an opportunity for organizations to contrast their end users' cybersecurity savvy to these two employee populations and evaluate how their knowledge levels fare in comparison to industry averages. As you examine the metrics presented here, it's important to consider how proactive you are being on the security awareness training front, and the implications of assuming that your employees have the fundamental skills necessary to safeguard personal and corporate data, devices, and systems.

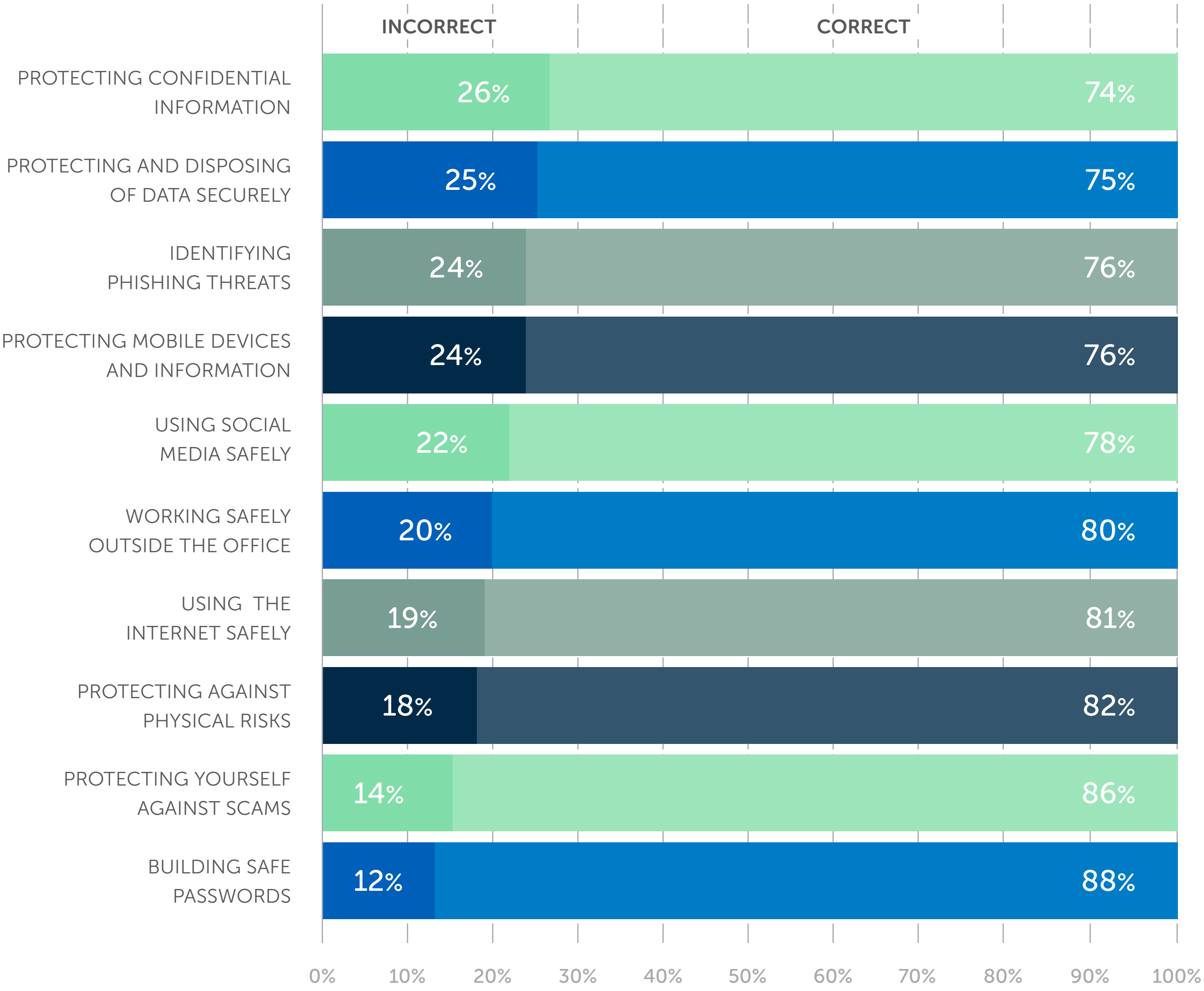
How Are End Users Doing?

70+ million

QUESTIONS ASKED AND ANSWERED

We took a look at more than **70 million** questions asked and answered in **10 categories**, from **June 2016** through **May 2017**. The year-over-year average improvement — from **22%** of questions incorrect to **20%** of questions incorrect — is certainly positive news, and users did well on average, answering more than 75% of questions correctly across most categories. However, given the business-critical nature of these topics, it's clear that there is still more room for improvement.

AVERAGE PERCENTAGE OF QUESTIONS ANSWERED CORRECTLY AND INCORRECTLY

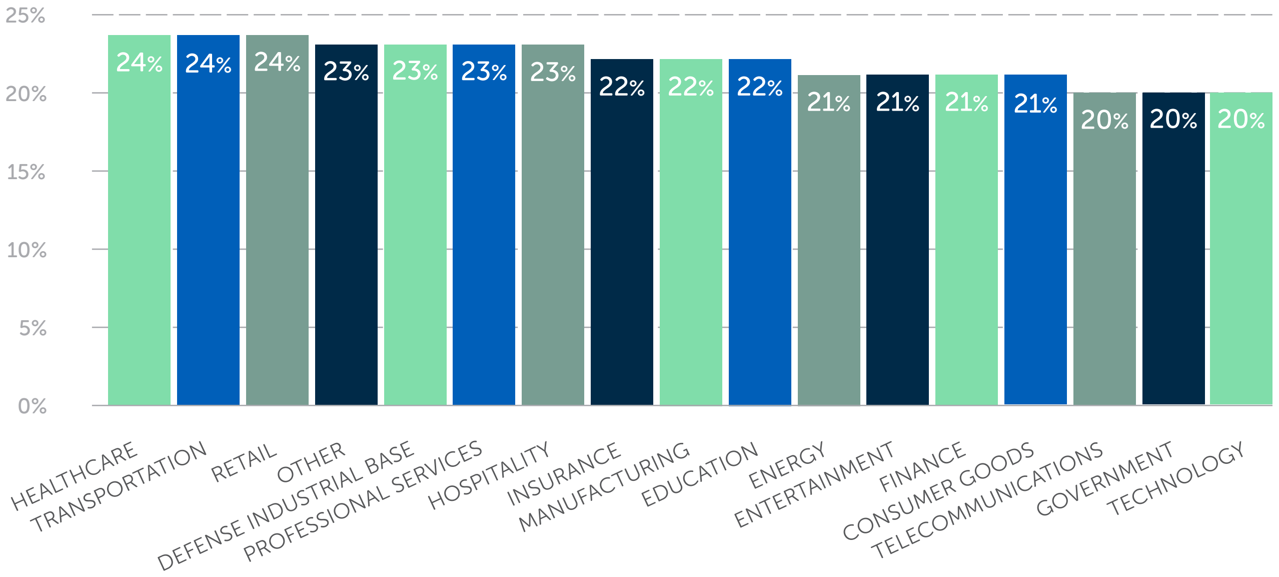


A Further Focus on Industry Data

In our **2016 report**, we included a fair amount of industry data, but we wanted to take a closer look at those metrics this year. As we noted in the introduction, there has been an overall reduction (modest though it may be) in the average percentage of questions incorrect, year over year. But as we drill into each of our cybersecurity categories, and examine the improvements as well as the negative progress, you will likely find it as interesting as we did to see how certain industries struggle with specific topics, and what those implications are for day-to-day business (to say nothing of national security).

Below, you will see a breakdown, by industry, of the average knowledge deficiencies across all categories. Though products and services vary significantly across these sectors, it is interesting to note that the level of end-user cybersecurity knowledge is very similar across the board. As we progress through the report, we will present more granular metrics, showing the industries that struggled the most with each topic.

AVERAGE PERCENTAGE OF QUESTIONS INCORRECT ACROSS ALL CATEGORIES



Protecting Confidential Information

2017 vs 2016

26% QUESTIONS INCORRECT

27% QUESTIONS INCORRECT

Like last year, this category — which focuses on end-user cybersecurity best practices related to PCI DSS and HIPAA compliance — was the one that employees struggled with the most.

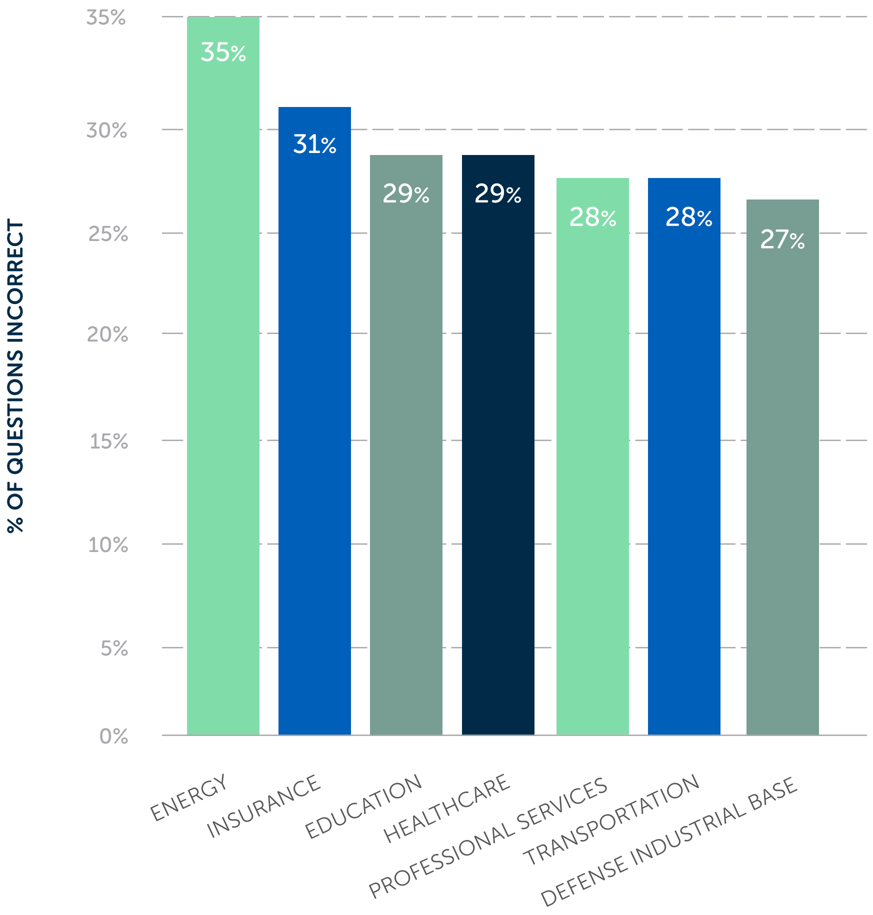
The modest year-over-year improvements seen in industries like Healthcare (the worst-performing sector in **2016**), Entertainment, and Manufacturing were offset by opposite moves for end users in the Energy, Insurance, and Education sectors. In fact, the industries that struggled the most this year were all among the worst performers in **2016** as well.

FACT!

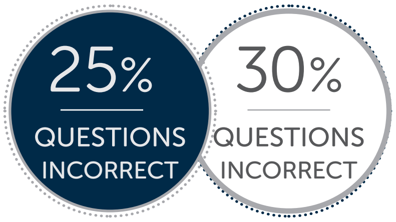
One of the questions users struggled with the most was around the use of shared login credentials.

To minimize this practice, employees should be made aware of the personal implications of allowing coworkers to access sensitive retail and healthcare systems using their credentials.

INDUSTRIES THAT STRUGGLE THE MOST



2017 vs 2016

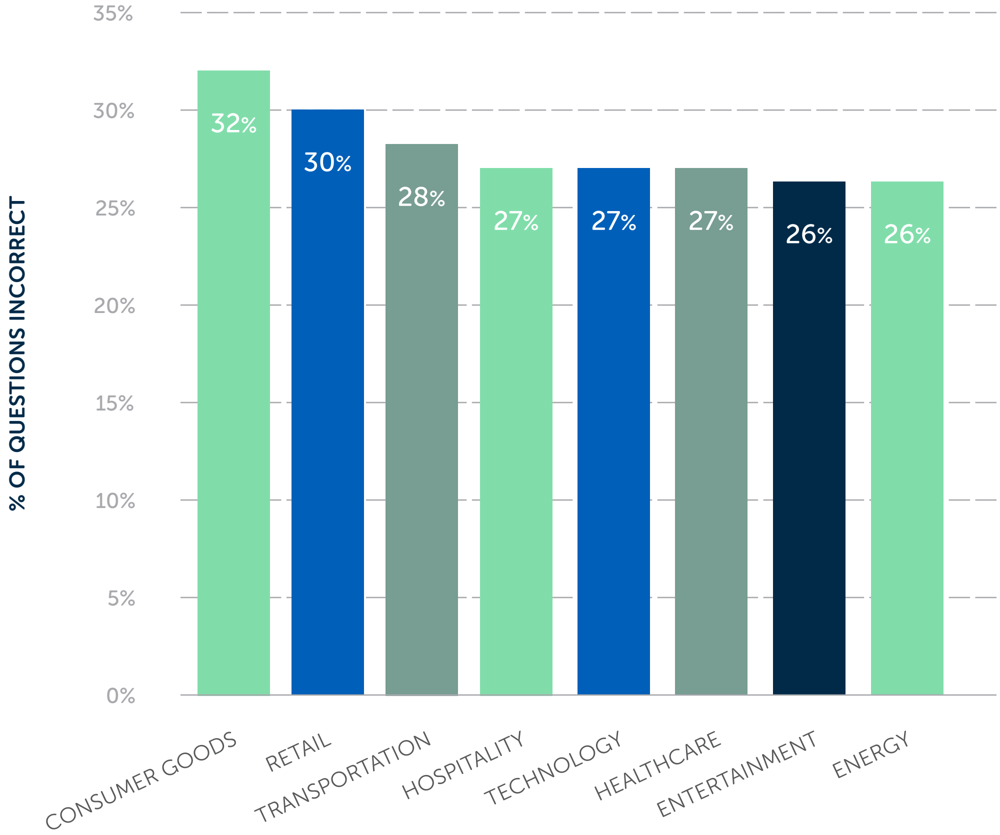


Protecting and Disposing of Data Securely

This category includes assessment and training questions that focus on the lifecycle of data, from creation to disposal, as well as techniques for handling personally identifiable information (PII) in general. Topics addressed include destruction of electronic and paper documents, use of USB devices, and classification of sensitive data.

We did see an overall improvement in this category this year, with two industries —Telecommunications and Manufacturing — making double-digit strides from **2016** to **2017**. However, end users across all industries still incorrectly answered a quarter of questions in this category. And the industry data remains discouraging overall. Though there were some shifts in the top-to-bottom rankings of worst performers, those industries that struggled the most in **2017** were also among the worst performers in **2016**.

INDUSTRIES THAT STRUGGLE THE MOST



Identifying Phishing Threats

2017 vs 2016

24% QUESTIONS INCORRECT

28% QUESTIONS INCORRECT

This category, which focuses on the different indicators and ramifications of phishing attacks, delivered the most consistent results this year. The rates of incorrectly answered questions across industries ranged from **21%** to **27%**, with all industries performing better than last year's **28%** average.

While it's logical for organizations to focus on simulated attacks to evaluate their end users' susceptibility to phishing attacks, question-based knowledge assessments give a more thorough gauge of employees' understanding of the phishing threat. Needless to say, we encourage our customers to deliver phishing tests; in fact, our founders' pioneering research spawned the use of these types of assessments. But even in those early days, we recognized that click/no-click exercises were just one component of an effective security awareness training program.

When we look at these two types of evaluations side by side — simulated attacks vs. question-based assessments — the results show the value of having a more complete picture:

HEALTHCARE

18% CLICK RATE* ON SIMULATED PHISHING ATTACKS

VS

26% QUESTIONS INCORRECT IN KNOWLEDGE ASSESSMENTS

GOVERNMENT

14% CLICK RATE* ON SIMULATED PHISHING ATTACKS

VS

24% QUESTIONS INCORRECT IN KNOWLEDGE ASSESSMENTS

*Click rate data is from our 2017 *State of the Phish Report*.

FACT!

This topic was the most popular with our customers. More than half of the assessment and training questions delivered to end users during our reporting period were related to phishing threats, and there was an even bigger emphasis on this topic than last year.

TIP!

Check out our **State of the Phish™ Report** for more data about phishing attacks.

info.wombatsecurity.com/state-of-the-phish

STATE OF THE PHISH 2017

Protecting Mobile Devices and Information

2017 vs 2016

24% QUESTIONS INCORRECT

15% QUESTIONS INCORRECT

This category saw the most significant downgrade in performance year over year, with only one industry (Telecommunications, with **14%** of questions incorrect) besting the average set in **2016**. As you'll see below, there was a marked increase in the number of questions that users answered incorrectly, with two industries posting a **2x uptick** over **2016's** average.

ACCORDING TO PEW RESEARCH, AS OF JANUARY 2017

92%

OF AMERICANS AGED 18-29 HAVE A SMARTPHONE

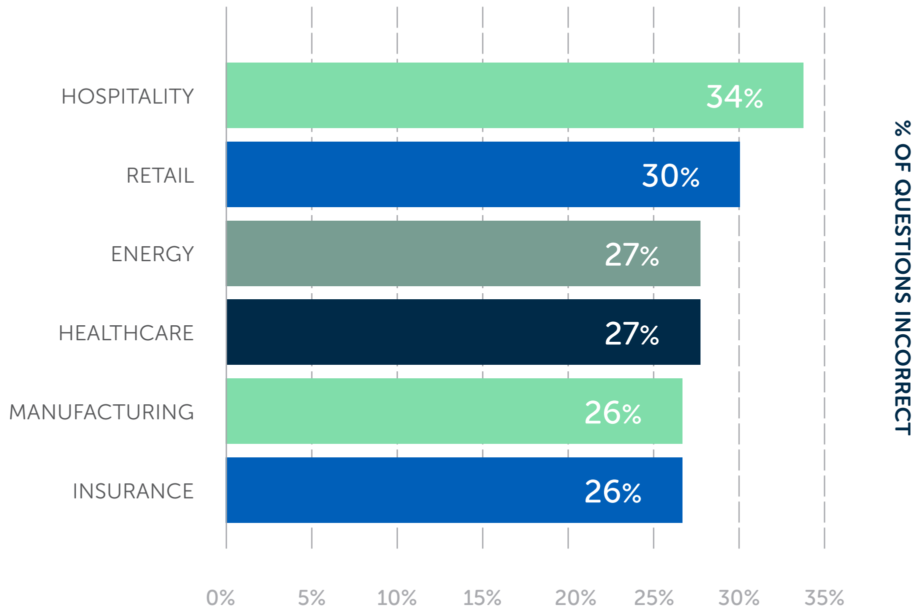
88%

OF AMERICANS AGED 30-49 HAVE A SMARTPHONE

Our data shows that users are struggling to understand the implications and ramifications of unsafe mobile applications and invasive permissions.

FACT!

INDUSTRIES THAT STRUGGLE THE MOST



Though we saw a slight uptick in our customers' tendency to assess and train on this topic in 2017, their prior reluctance to address mobile device security seems to have put users behind the knowledge curve. In the industry survey conducted for our **2016 report**, just **52%** of organizations said they evaluate their end users' knowledge of this topic.

As the Pew Research numbers show, we are rapidly approaching a **100% smartphone adoption** rate with **adults aged 18 to 49**. These devices are becoming increasingly complex and interconnected, and — as you'll note on the next page of this report — users frequently blur the lines between corporate and personal computing. A continued lack of awareness and knowledge among mobile device users will negatively impact the security of business data and systems.

Using Social Media Safely

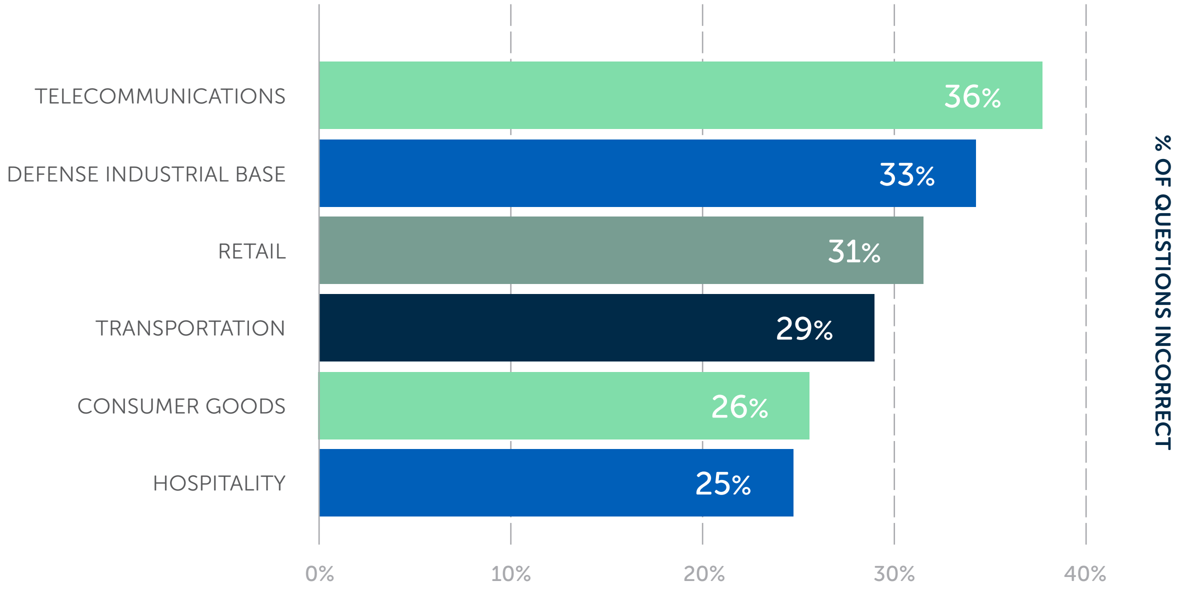
2017 vs 2016

22% QUESTIONS INCORRECT

31% QUESTIONS INCORRECT

This category saw the largest year-over-year improvement — a positive trend given the continued increase in use of social media platforms around the globe. In the past year, several high-profile public initiatives to improve safety and cut back on imposter accounts on social platforms have likely helped to boost our customers' continued efforts to raise end-user awareness and understanding of best practices. Even within those industries that struggled the most with this topic, only two fared worse than last year's average:

INDUSTRIES THAT STRUGGLE THE MOST



With that said, we too often see organizations classifying social media as an "outside" activity for their employees. This is simply short-sighted, particularly when you consider that our **2016 report** revealed that **more than 75%** of organizations allow access to social networking sites and apps on business devices. Even those who lock down access within the confines of corporate systems are exposed during users' off hours. It's important to acknowledge (and attempt to mitigate) the risks associated with poor social media habits, which can be done by raising awareness and educating end users.

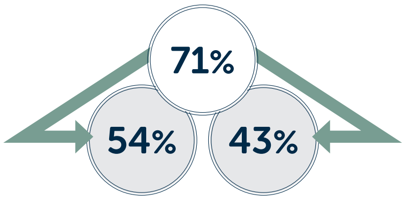
Keep These End-User Risks in Mind

Our *2017 User Risk Report* revealed the following points of concern with regard to social media best practices among US survey participants:

71% regularly use corporate devices outside the office

54% view or post to social media on those devices

43% allow friends or family members to view or post to social media on those devices



2017 vs 2016

20% QUESTIONS INCORRECT

26% QUESTIONS INCORRECT

Working Safely Outside the Office

We saw a significant improvement year over year in this category — a good sign given that more and more employees are regularly working outside the office, whether in a telecommuting capacity, while traveling, or otherwise. As you'll see from the top and bottom two performers, all industries fared better than the average percentage tallied in **2016**, though there is a wide spread between the highest and lowest marks.

ACCORDING TO GALLUP

43%

FACT!

OF EMPLOYEES WORK REMOTELY AT LEAST PART OF THE TIME

SOURCE: STATE OF THE AMERICAN WORKPLACE REPORT

WORST PERFORMERS

- 25% PROFESSIONAL SERVICES
- 25% TELECOMMUNICATIONS

BEST PERFORMERS

- 14% HOSPITALITY
- 15% INSURANCE

Those organizations that are not assessing and training end users about the best practices to employ when working outside the confines of corporate locations and networks may want to rethink that approach.

Our *2017 User Risk Report* revealed that the average employee is not well-versed in applying even simple safeguards:

54% of US workers believe that they can trust open WiFi networks in trusted locations.

Nearly 40% of UK workers who have installed a VPN said they rarely or never use it.

14% of UK workers have no locking mechanism on their mobile devices.

More than 50% of US and UK workers would leave a corporate laptop in their car rather than take it into a restaurant with them.

Using the Internet Safely

2017 vs 2016

19% QUESTIONS INCORRECT

16% QUESTIONS INCORRECT

Unfortunately, this category saw a lot of backward movement in comparison to **2016**. In fact, only one industry — Defense Industrial Base, whose users answered **14%** of questions incorrectly — performed better this year than last year.

WORST PERFORMERS

23% TELECOMMUNICATIONS

22% CONSUMER GOODS

22% ENTERTAINMENT

21% EDUCATION

BEST PERFORMERS

18% TECHNOLOGY

17% GOVERNMENT

14% DEFENSE INDUSTRIAL BASE

It's difficult to say why there would be slide in this area, particularly since last year's study found that this topic is included in the vast majority of cybersecurity education programs. Perhaps organizations took a step back following **2016's positive numbers**, moving away from internet safety to focus on topics like phishing and ransomware prevention.

Regardless of the reason, it's clear that organizations cannot make assumptions about levels of risk from one year to the next. Key topics — like best practices for browsing the web and examining unknown and potentially dangerous URLs — must be regularly covered and reinforced in order to create a culture of security within any organization.

?

MOST INCORRECT QUESTIONS

Here are some of the topics users struggled with the most:

- The risks associated with shortened URLs
- Identifying safe sites vs. risky sites
- The implications of using social logins for applications outside of social media

2017 vs 2016

18% QUESTIONS INCORRECT

15% QUESTIONS INCORRECT

Protecting Against Physical Risks

As in **2016**, this was one of the best understood topics among end users, though we did see a bit of a slide this year. Our data shows one likely reason for this: Organizations put less emphasis on this topic this year than they did last year.

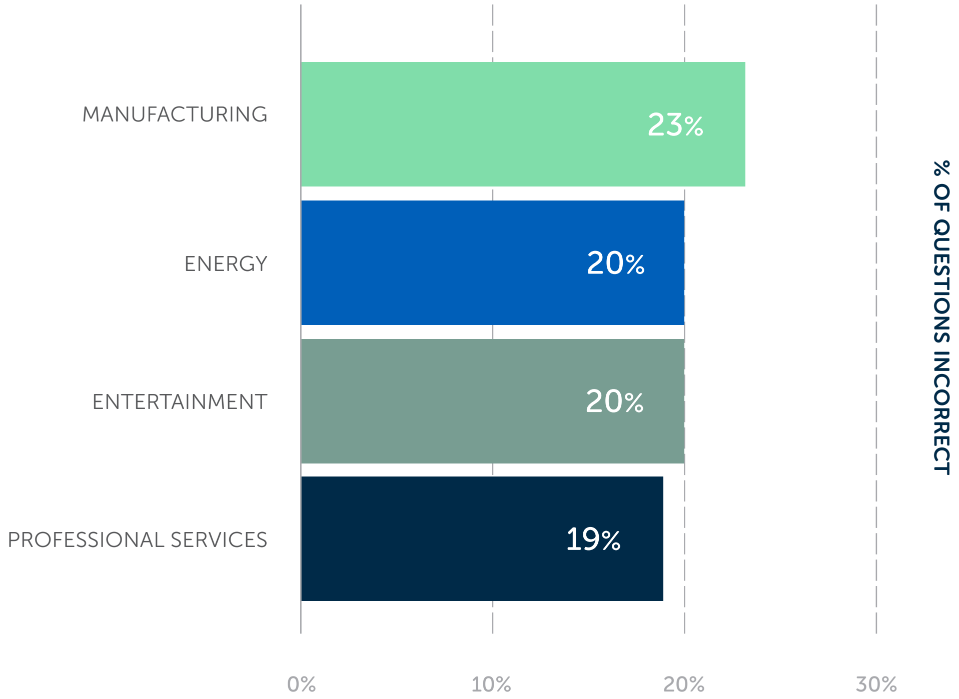
Among the sectors that struggled the most (noted below), we again saw representatives from critical infrastructure industries. This is particularly concerning because a physical breach within these types of organizations can have far-reaching consequences that impact public safety and even national security.

TIP!

Our data indicates that end users often fail to see the importance of physically protecting items like ID badges, printed phone directories, and files that provide details about service providers (like HVAC technicians and legal firms).

Employees should be reminded that physical security and cybersecurity are linked. People, assets, and areas should be protected offline as well as online.

INDUSTRIES THAT STRUGGLE THE MOST



The bottom line with physical security lies in continued vigilance. Though it can be tempting to regard these types of safeguards as “common sense” behaviors, organizations should not dismiss the idea of raising awareness and teaching their employees the importance of best practices related to physical security. Good clean desk habits and relatively simple actions — like locking doors and checking credentials — present low-cost opportunities to improve security postures overall.

Protecting Yourself Against Scams

2017

14%

QUESTIONS INCORRECT

We carved out this category within our **2017 data** in order to better examine how well end users understand the fundamental principles of social engineering. Though most regularly associated with phishing emails, cybercriminals and con artists apply social engineering techniques across a range of attack vectors, including vishing (voice phishing) calls, smishing (SMS/text phishing) messages, social media pretexting, and in-person encounters.

It was encouraging to see that end users performed well, on average. (Only our Building Safe Passwords category registered better scores.) Only two industries fared significantly worse than the mean, and three industries bested their counterparts by a fair margin:

FACT!

Data mining for online attacks often happens in areas outside of cyberspace.

IND

WORST PERFORMERS

22% TRANSPORTATION

19% RETAIL

BEST PERFORMERS

10% EDUCATION

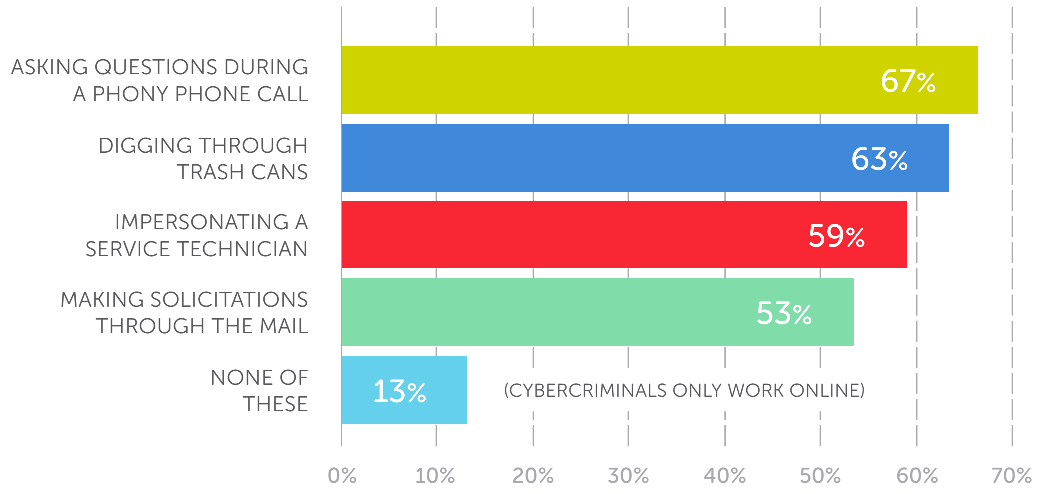
11% TELECOMMUNICATIONS

11% DEFENSE INDUSTRIAL BASE

PROF

We caution organizations not to take awareness of social engineering threats for granted, however. Many end users do not recognize that cybercrime extends beyond online activities, as indicated by the survey responses from our *2017 User Risk Report* (see below). It's important to educate employees about the different techniques that social engineers employ to gather information and gain access.

HOW DO CYBERCRIMINALS OBTAIN INFORMATION? (MULTIPLE RESPONSES PERMITTED)



2017 vs. 2016

12% QUESTIONS INCORRECT

10% QUESTIONS INCORRECT

Building Safe Passwords

Like last year, end users performed best in answering questions about password safety. Given that passwords are long-standing safeguards and many organizations have established policies, it is reasonable to think that employees are well-versed in the need to apply these protections to sensitive accounts and systems.

However, there is still work to be done. As noted below, end users in several industries continue to struggle with best practices related to password creation and application, with some sectors performing much worse than the average:

WORST PERFORMERS

22% TRANSPORTATION

20% DEFENSE INDUSTRIAL BASE

18% HOSPITALITY

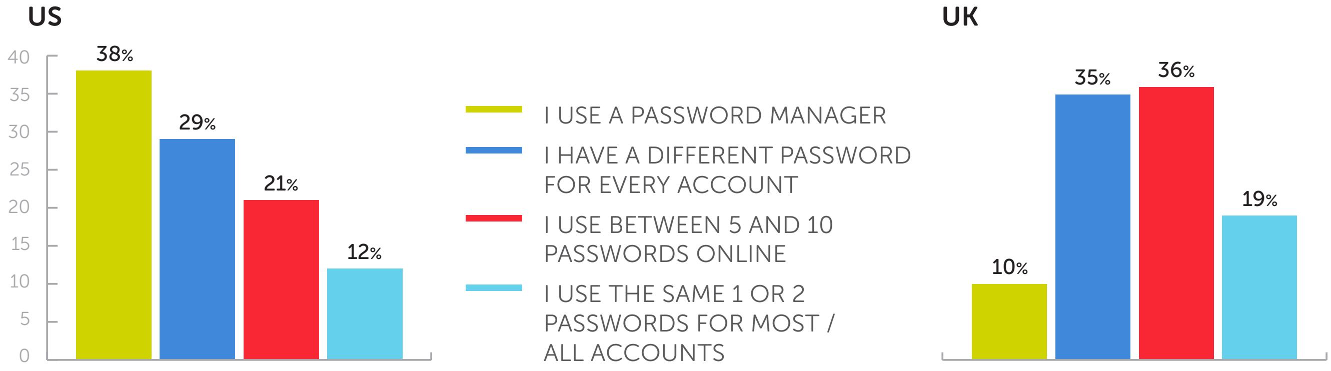
17% RETAIL

16% PROFESSIONAL SERVICES

15% TELECOMMUNICATIONS

Our *2017 User Risk Report* again offers a cautionary tale for organizations that are making assumptions about what end users do and do not know about creating strong, unique passwords. In particular, our survey revealed that employees are regularly reusing passwords across multiple systems and sites, an increasing risk given that lists of compromised credentials are readily available to cybercriminals. It is critical to educate your employees about how to effectively manage their logins and give them the tools they need to improve the security of their corporate and personal accounts.

HOW DO YOU MANAGE ONLINE ACCOUNT PASSWORDS?



Continuity Is Key to Success

As cybercriminals have shown over the past several years, the threat landscape is capable of both consistency and change. Phishing attacks have been on our collective radar for years, but some of the earliest tricks — like the Nigerian Prince and his merry band of copycats — still hit their mark. At the same time, methods have morphed; as technical safeguards have advanced, so have attackers' sophistication levels. And fighting phishing is but one element of managing end-user risk. With the proliferation in electronic communications, social media platforms, and connected devices and systems — to say nothing of the vast magnitude of data output, which IBM recently estimated to be about **2.5 quintillion bytes per day** — the personal and business lives of the average employee are very different than they were just a few years ago.

Every day, there is a lot to think about from a cybersecurity perspective. And every year, things change. The graphic below, which highlights statistics from Domo's 2017 *Data Never Sleeps 5.0* infographic (and offers some comparisons to 2016), clearly shows why users and organizations alike need to stay on their toes when it comes to managing and protecting data and devices.

As is evidenced in the year-over-year comparisons we've presented throughout this report, **organizations cannot count on awareness and knowledge to remain at constant levels.** Even within successful security awareness training programs — those that focus on building a culture of security, in which employees are valued and empowered to be part of the solution rather than relegated to being an unchangeable part of the problem — there are peaks and valleys. But organizations that deemphasize end users' role in cybersecurity and address it only occasionally (or, worse yet, that abandon the pursuit altogether) are destined to fall further and further behind the curve.

2017 DATA BY THE MINUTE

Source: Domo.com

103.4M
Spam Emails Sent

3.6M
Google Searches

Social Sharing

4.1M
Videos Viewed on YouTube

528K
Photos Shared on Snapchat

456K
Tweets on Twitter

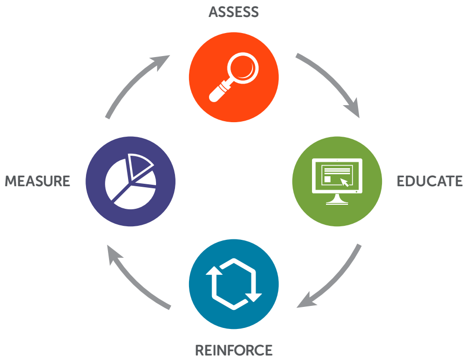
47K
Photos Posted on Instagram

2017	vs	2016
	Amazon Sales	
$259K		$222K
	Forecast Requests Received by The Weather Channel	
694K		569K
	Text Messages Sent	
15.2M		3.6M

About Wombat Security

Wombat Security Technologies, headquartered in Pittsburgh, PA, provides information security awareness and training software to help organizations teach their employees secure behavior. Our Security Education Platform includes integrated knowledge assessments, simulated attacks, and libraries of interactive training modules and reinforcement materials.

Wombat was born from research at the world-renowned Carnegie Mellon University, where its co-founders are faculty members at the CMU School of Computer Science, and in 2008 they led the largest national research project on combating phishing attacks, with a goal to address the human element of cybersecurity and develop novel, more effective anti-phishing solutions. These technologies and research provided the foundation for Wombat's Security Education Platform and it's unique Continuous Training Methodology. The methodology, comprised of a continuous cycle of assessment, education, reinforcement, and measurement, has been show to deliver up to a 90% reduction in successful phishing attacks and malware infections.



wombat security technologies
Change Behavior. Reduce Risk.

#BeyondthePhish

wombatsecurity.com
info@wombatsecurity.com | 412.621.1484
UK +44 (20) 3807 3472