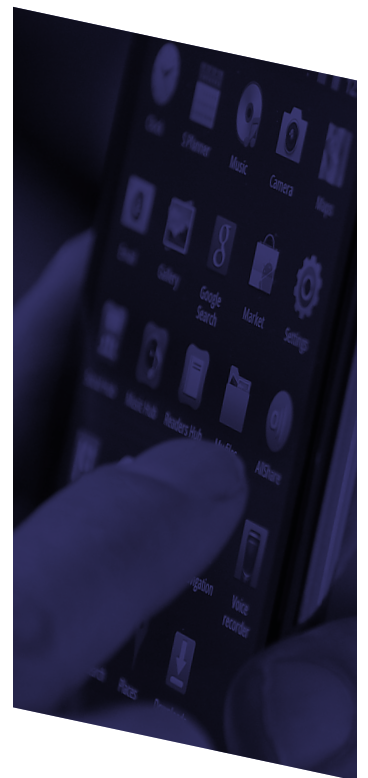
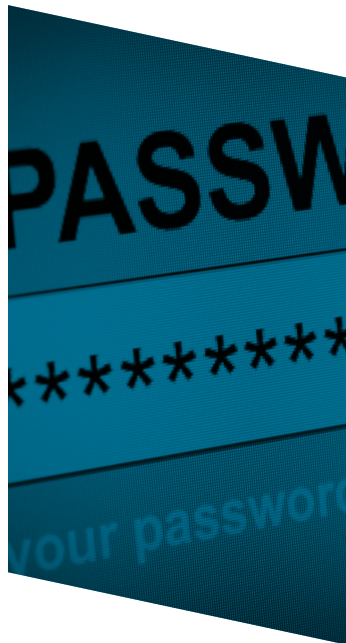
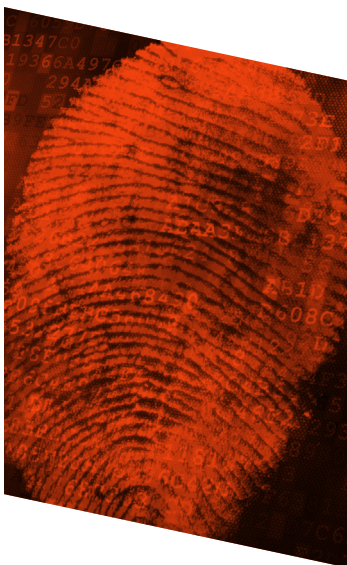


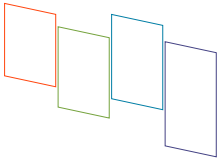
Wombat Security's 2016

Beyond the Phish

Report



#BeyondthePhish



Beyond the Phish

As our *State of the Phish Report* reinforced earlier this year – phishing is still a large and growing problem for organizations of all sizes. And as pioneers in the use of simulated phishing attacks, we strongly recommend organizations make anti-phishing education the foundation of their security awareness and training programs.

However, we also recommend that they think **beyond the phish** to assess and educate their end users about the many other cybersecurity threats that are prevalent (and emerging) in today’s marketplace. Risky behaviors like lax data protection, oversharing on social media, and improper use of WiFi are all dangers in their own right — and could be considered contributing factors to the ever-growing phishing problem.

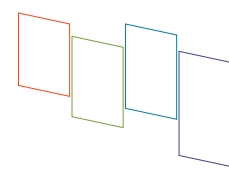
In this report we will take a look at the answers to nearly **20 million questions** asked and answered around nine different topics in our Security Education Platform over the past **two years** to understand what areas end users still struggle with and what areas they are doing better in.

We also surveyed hundreds of security professionals — customers and non-customers — about what security topics they assess on, and their confidence levels in their end users’ abilities to make good security decisions.

While not a scientific study, this report offers a look at these two sets of data and shows the importance of assessing and educating **beyond the phish**.

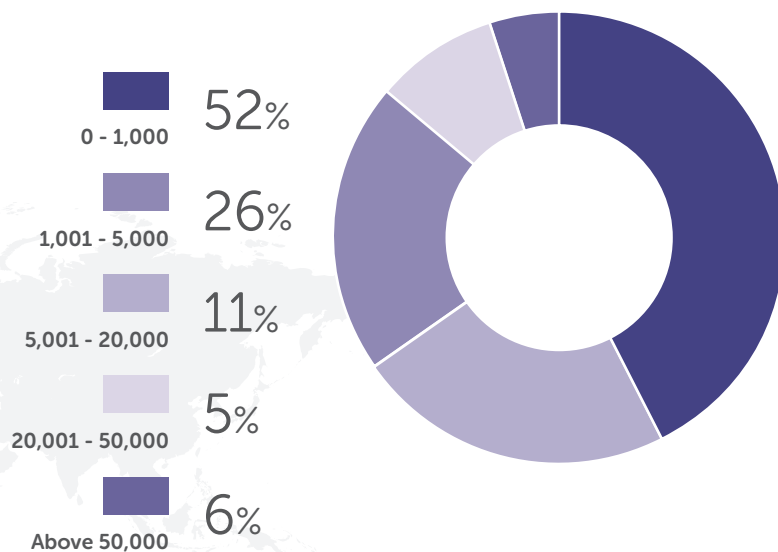
“We should all be thankful to Wombat Security for sharing empirical data from nearly 20M actual end-user assessments! The findings here are clear — organizations that measure user knowledge on a variety of security topics are gaining valuable insights into the most important factors of security risk, which can focus their efforts to address it. Depth of data, combined with a continuous, metrics-based approach to end-user security education, results in a solid knowledge improvement program. In my own analysis, successfully changing user behaviors have helped Wombat customers reduce security-related risks by about 60%.”

Derek Brink, CISSP,
Vice President and Research Fellow, Aberdeen Group

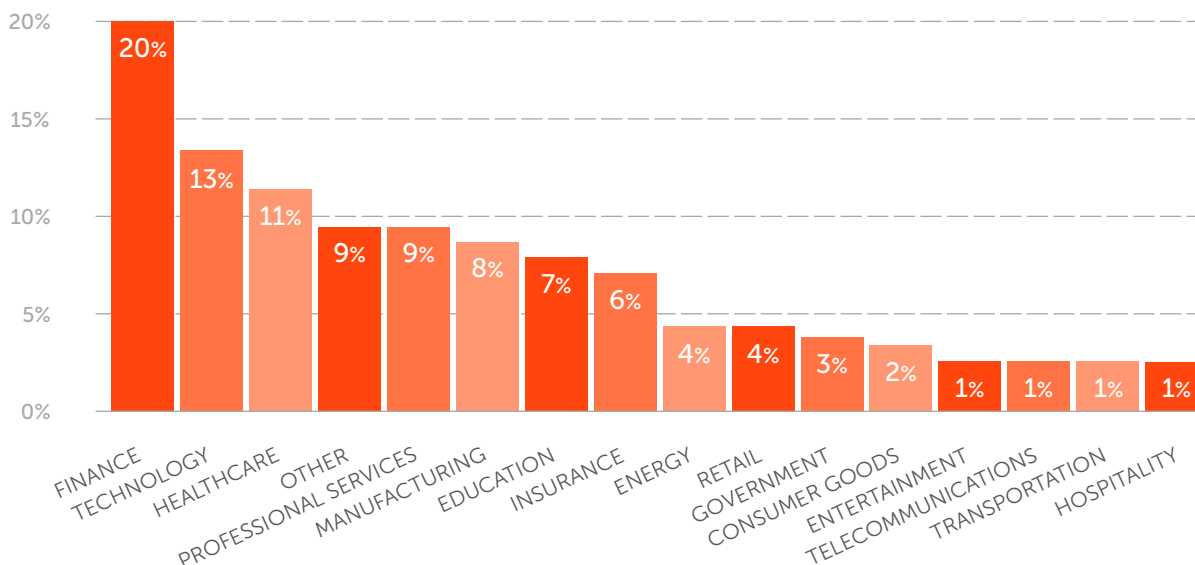


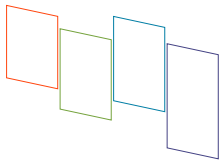
Who Participated in the Survey?

ABOUT HOW MANY EMPLOYEES WORK AT YOUR ORGANIZATION?



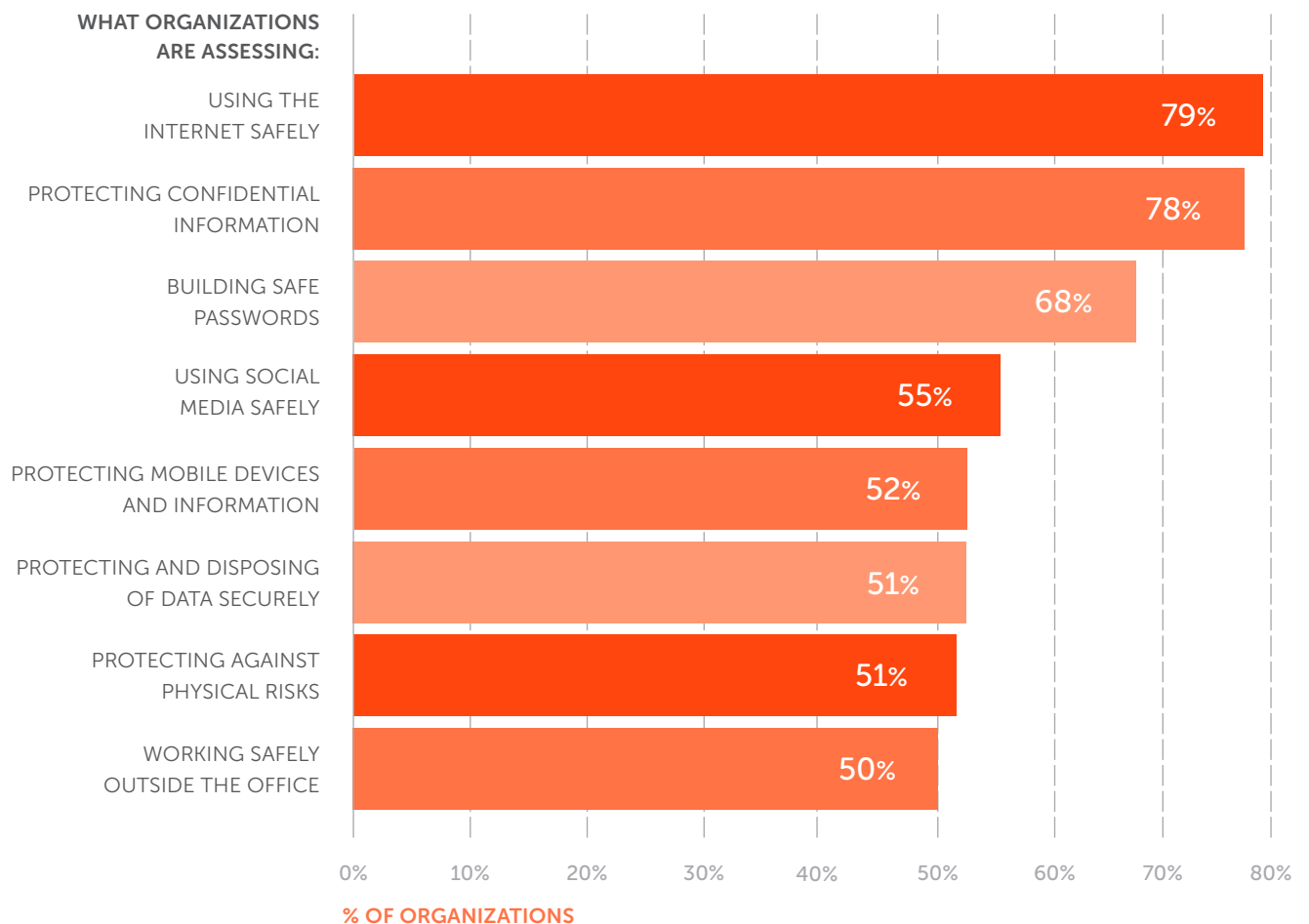
WHAT INDUSTRY DOES YOUR ORGANIZATION BELONG TO?



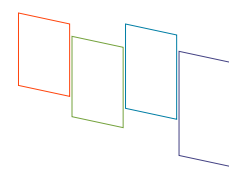


What Do Organizations Assess On?

We were curious what areas (other than phishing) organizations assess, and how they match up to the areas we see users struggle with (more than one answer allowed.)



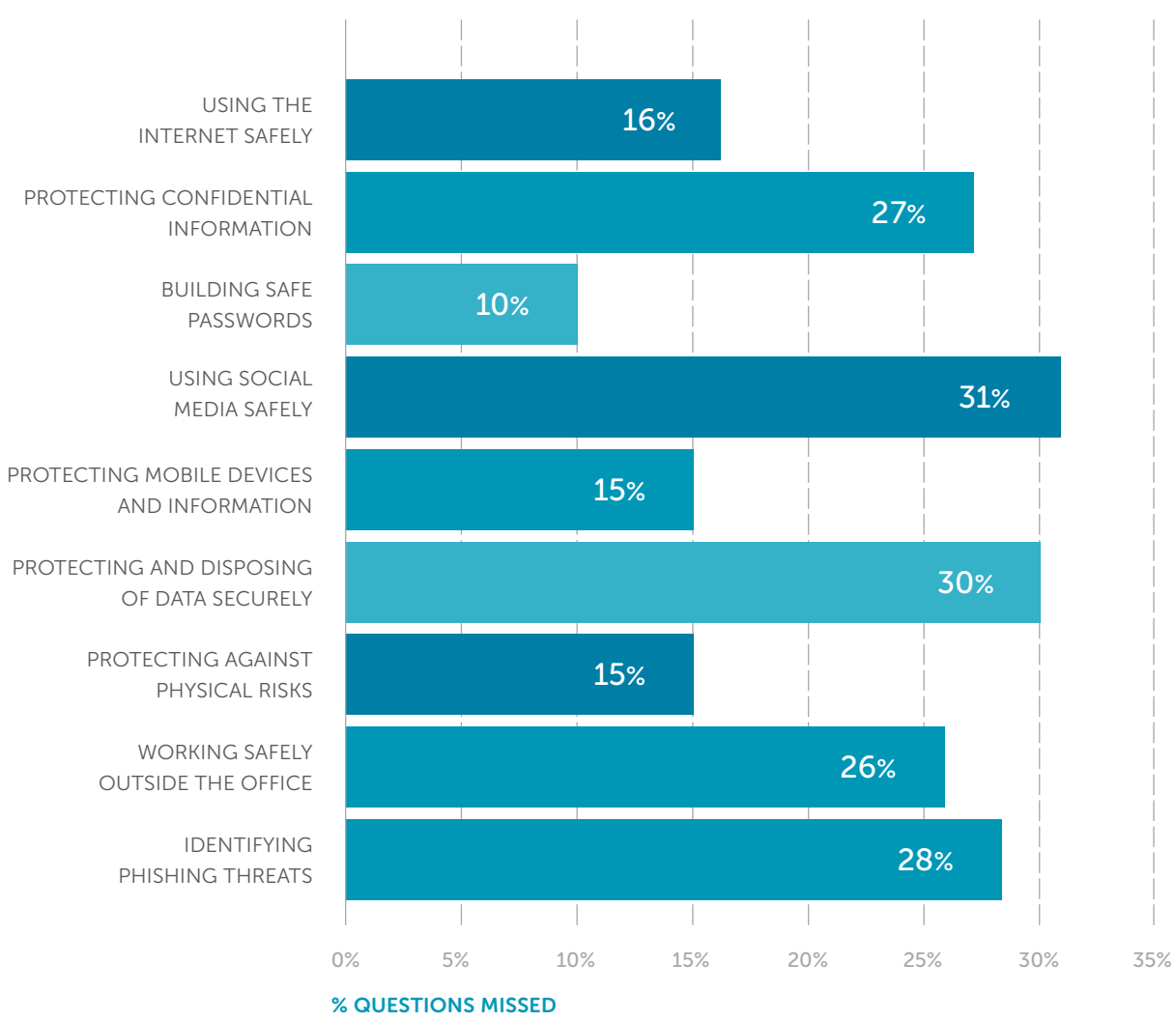
Progress is being made. **Using the Internet Safely** is the topic that most organizations reported that they assess, and it was one of the topics in which end users performed better.

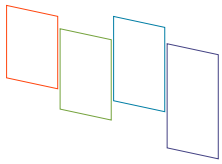


How Are End Users Doing?

≈ 20 million
QUESTIONS
ASKED AND ANSWERED

We took a look at approximately **20 million** questions asked and answered over the past **2 years**. There are some areas that end users continue to struggle in, and some where we are starting to see progress.



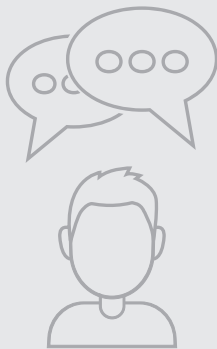


31%
QUESTIONS
MISSED

Using Social Media Safely

Social Media plays a big part in our lives but end users struggled here the most, missing **31%** of the questions we asked them around what they should and shouldn't do to keep themselves and their organizations safe.

What's more, in our survey of security professionals we found that only about half are assessing users around this topic. Most companies allow social media access on work devices while admitting they are not very confident that their employees know what to do to keep their organization safe.



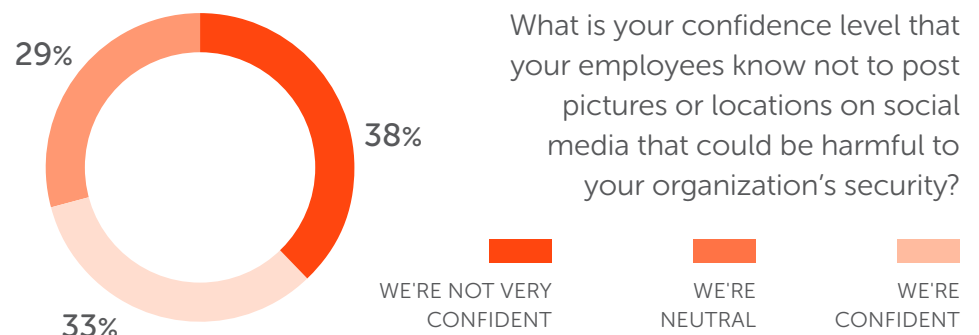
ONLY
55%

ASSESS ON USING
SOCIAL MEDIA
SAFELY

- YET -

76%

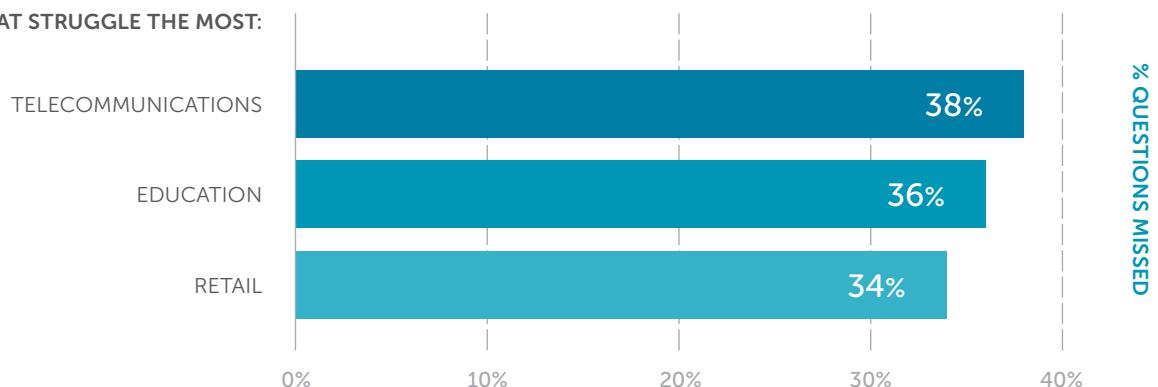
ALLOW ACCESS
ON WORK
DEVICES

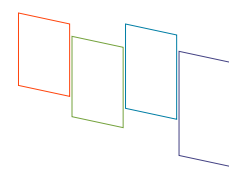


What is your confidence level that your employees know not to post pictures or locations on social media that could be harmful to your organization's security?

What does this mean? While more than **75%** of the working population is using social media, organizations are not regularly advising employees about best practices. Since many are not assessing on this topic and measuring knowledge, they do not know how large of a problem they have and are just hoping for the best. Hope is not a strategy. Continuous assessment and training is a systematic approach to address the problem.

INDUSTRIES THAT STRUGGLE THE MOST:





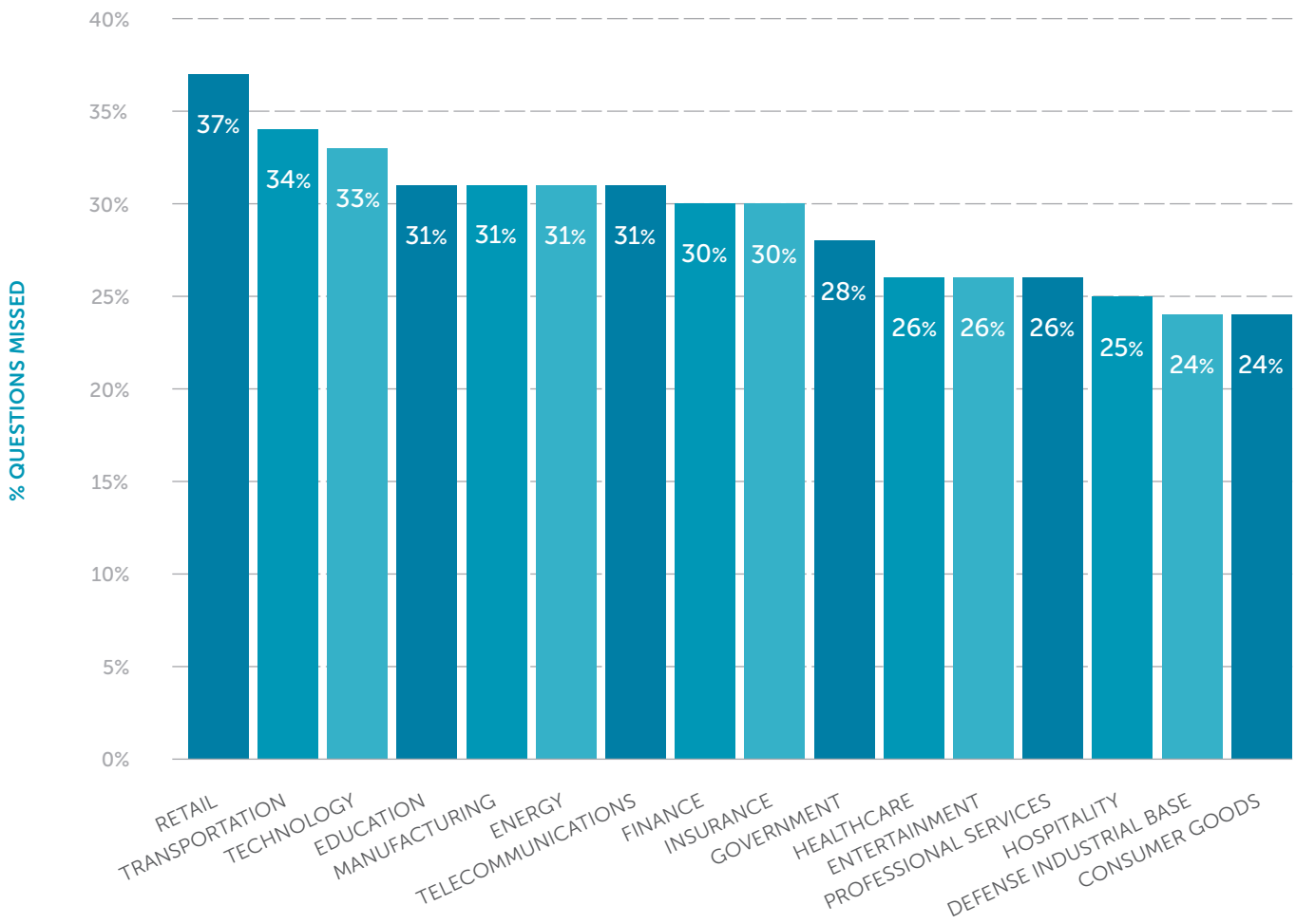
30%
QUESTIONS
MISSED

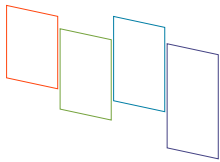
Protecting and Disposing of Data Securely

This category covers the lifecycle of data, from creation to disposal, and covers topics about handling PII (Personally Identifiable Information) on a more general level. Questions in this category covered topics such as using USBs, deleting files from hard drives, and securing work devices — and nearly **30%** of the questions we asked on this topic were missed.

This puts all of us in danger, and while some industries have done worse than others, none of them did very well considering their interaction with some of our most valuable information. According to our industry survey, only a little more than half are assessing around this topic at all.

INDUSTRIES THAT STRUGGLE THE MOST:





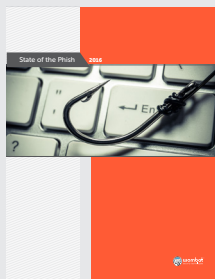
Identifying Phishing Threats

When organizations focus on reducing successful phishing attacks, they often think only about using phishing simulations. When our founders published the research that gave birth to the use of mock attacks, their vision extended beyond click/no-click assessments – their focus was on intervention and training that would change behavior and reduce end-user risk. But they knew simulated phishing emails and just-in-time training couldn't do that alone. From that, Wombat Security was born, along with a portfolio of products that allow organizations to not only **assess vulnerability** through simulated attacks, but also evaluate and **improve understanding** via knowledge assessments and interactive training.

When we look at these two types of phishing assessments side by side – simulated attacks vs. question-based evaluations – the results prove the need for both approaches:

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

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



HEALTHCARE

13%

CLICK RATE*
ON SIMULATED
PHISHING ATTACKS

VS.

31%

QUESTIONS MISSED
IN ASSESSMENTS



MANUFACTURING & ENERGY

9%

CLICK RATE*
ON SIMULATED
PHISHING ATTACKS

VS.

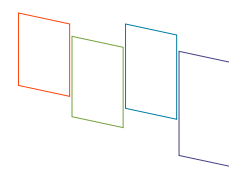
29%

QUESTIONS MISSED
IN ASSESSMENTS

*Click rate data is from our 2016 *State of the Phish Report*.

Simulated phishing is a great tool, but it only provides a click/no-click measurement – and you simply can't be sure why users didn't respond to a particular mock phish. Was it because they knew better? Or was it because the message wasn't relevant to them, or because they didn't see it in their inbox?


Reviewing data from simulated attacks and knowledge assessment results provides a clearer picture of employee competency with regard to recognizing and avoiding phishing attacks.



Protecting Confidential Information

27%
QUESTIONS
MISSED

Questions asked on this topic relate specifically to standards compliance in both PCI DSS and HIPAA. Just like the topic of Protecting and Disposing of Data Securely, many industries struggled with securing sensitive financial and medical information. Healthcare workers missed the most questions — **5 percentage points** worse than average. From our survey results, this is one of the top two topics that security teams are assessing on, and it should remain a top priority.

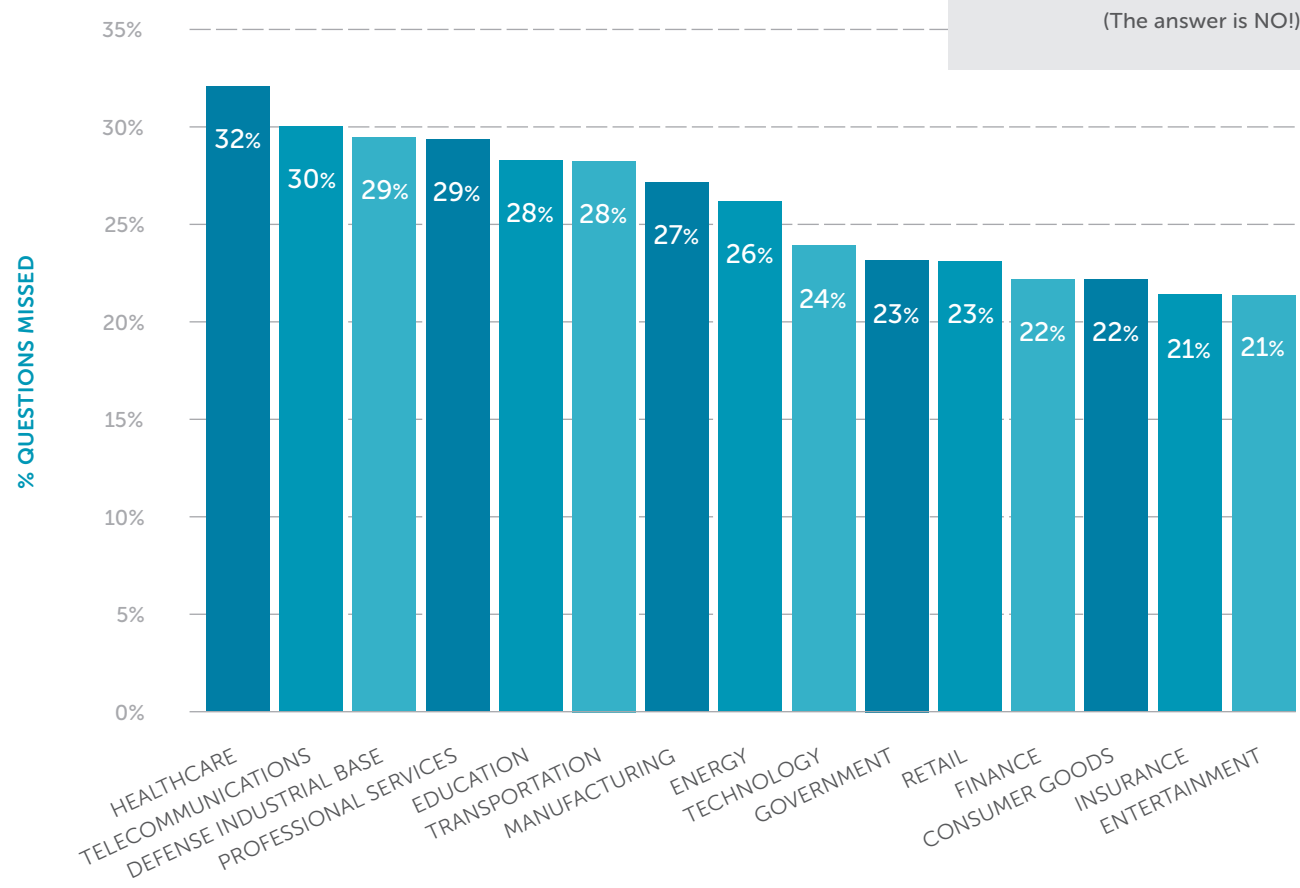
 What was one of the most missed questions asked around this topic?

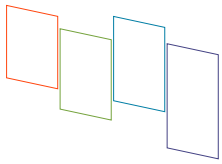
—

FACT! Is it safe for a call center employee to write a customer's credit card number down in a personal notebook for later processing?

(The answer is NO!)

INDUSTRIES THAT STRUGGLE THE MOST:





Working Safely Outside the Office

Today, working outside of the office is very common. Whether traveling for work or working from home or a local coffee shop -- there are a lot of things to consider to keep data, networks, and equipment safe.

The number of end users who want to connect to work anytime from anywhere is only going to increase. Organizations will need to keep educating their employees on how to stay safe on the road.

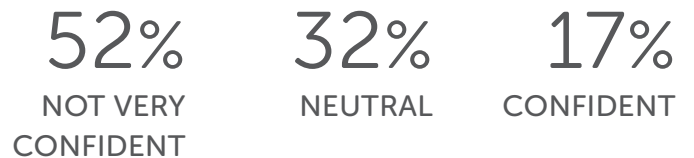


We were surprised that only **50%** of companies are assessing around this very important topic. Our data shows that **26%** of questions have been missed on topics ranged from safe use of WiFi to practical physical security. No industry did great, but there are three that did worse than others:

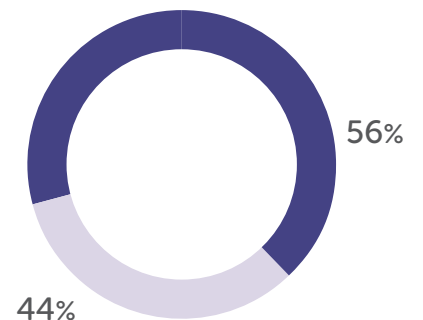


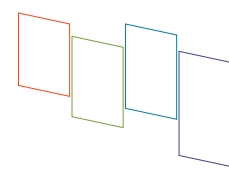
With so few organizations assessing employees about their telecommuting habits, we assumed confidence in end-user knowledge would run high. But that's not the case, even with something as basic as proper use of open-access WiFi networks. Still, it's not terribly surprising given that more than half of those surveyed do not provide guidelines for employees to follow while traveling.

How confident are you that employees don't connect to public WiFi networks without a protected connection such as a VPN?

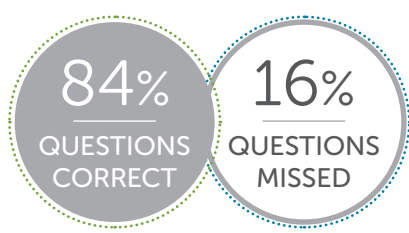


Do you have a security policy/guideline for employees to follow while traveling?





Using the Internet Safely



According to our survey, using the internet safely is the topic security professionals are assessing around the most with **79%** reporting it as part of their security education program. It seems to be paying off, with end users getting **84%** of the questions in this area correct. Malware and virus downloads are often done by end users who do not know how to spot dangerous URLs.

While most industries were doing well on this topic, a few still struggled more than others missed more than our average of **16%** questions missed:

TRANSPORTATION

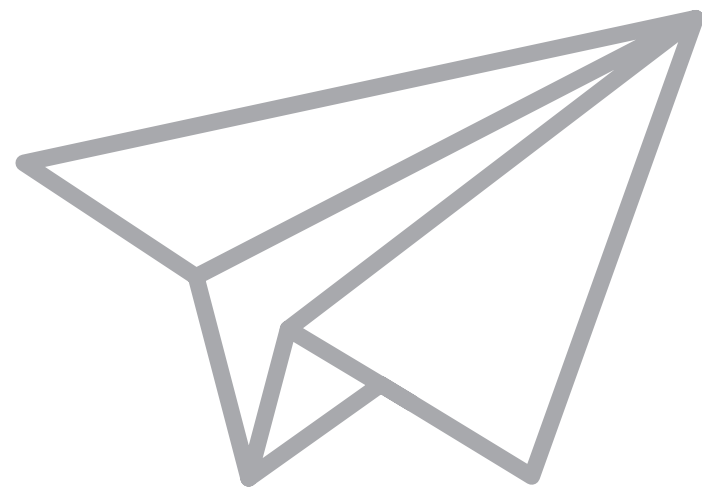
22%

RETAIL

20%

HEALTH CARE

18%



What is your confidence level that employees understand safe practices for browsing the internet (such as logging out of web apps before closing, etc)?

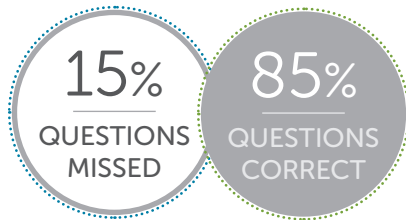
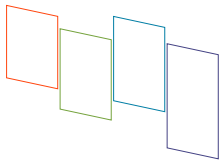


31%
NOT VERY
CONFIDENT

52%
NEUTRAL

17%
CONFIDENT

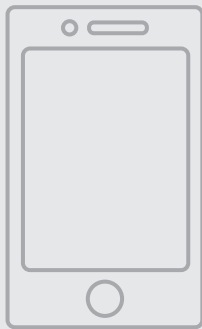
Just because there is progress, that doesn't mean that organizations should assess any less around the topic — continuous training keeps best practices top of mind for end users, especially on a topic that has become as second nature as browsing the internet.



Protecting Mobile Devices and Information

Recent data from Pew Research (see left) indicates how important mobile devices have become. The good news from our data is that this is one of the better understood topics, with **85%** of the questions being answered correctly (even though only **52%** of organizations are assessing around it). However, some industries did a bit worse than the average of **15%** questions missed:

ACCORDING TO PEW RESEARCH,
AS OF OCTOBER 2015



86%

OF THOSE AGED
18-29 HAVE A
SMARTPHONE

83%

OF THOSE AGED
30-49 HAVE
A SMARTPHONE

INDUSTRIES THAT
STRUGGLE THE MOST:

CONSUMER GOODS

26%

HEALTHCARE

25%

FINANCE

18%

0% 10% 20% 30%

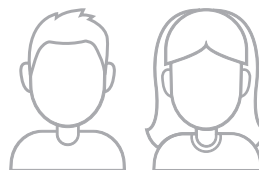
% OF QUESTIONS MISSED

Many of the most missed questions on this topic were around the area of Bluetooth connectivity. Most people did not realize that they can leave personal information behind on devices they have paired with, such as a rental car.



FACT!

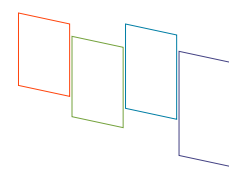
Does your organization provide mobile/BYOD device programs that allow network access?



67%
YES

33%
NO


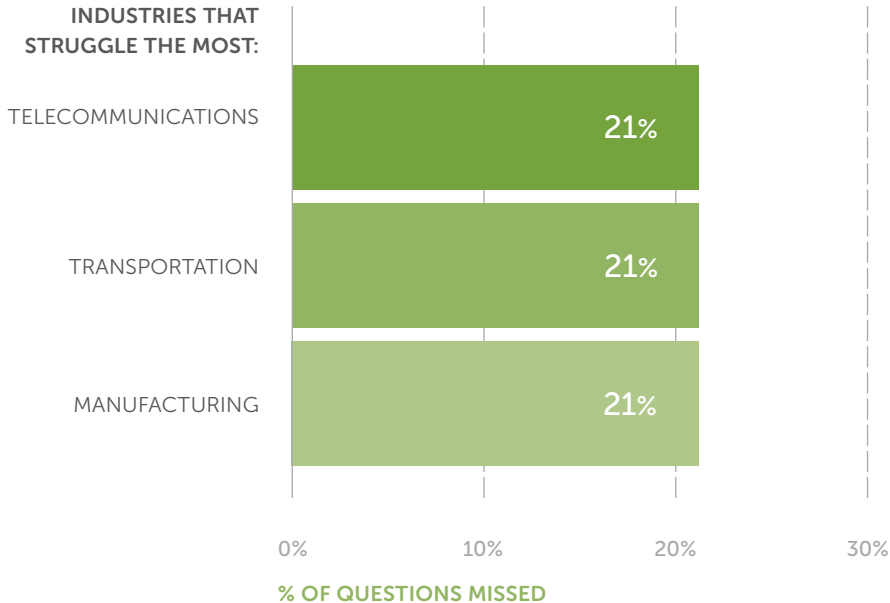
As technology changes and new threats develop, organizations and end users need to remain vigilant and up to date on how to stay safe.



Protecting Against Physical Risks

Physical security often seems like common sense — making sure no one follows you through a locked door into a secure area, not leaving sensitive files on your desk unattended — and it seems that most people are understanding the concepts presented, with **85%** of the questions asked being answered correctly. Still, only **51%** of organizations are assessing around this topic, so there is room for improvement there.

Of concern, we saw end users in critical infrastructure industries falling a bit above the average of **15%** questions missed, which is alarming given the potential impact of a physical breach in these types of organizations.

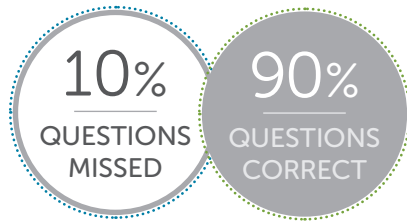
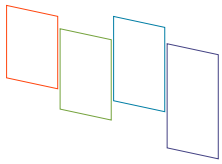


TIP!

Our data shows that end users often struggle with questions related to securing their devices while in the office.

We tend to take safety for granted within our own office environments, but insider threats are a real thing. Employees should be taught simple security practices such as locking their computer screens when leaving their work stations and locking laptops and other portable devices in a secure drawer or cabinet when leaving for the night.

» ONLY **51%** OF ORGANIZATIONS ASSESS THEIR END USERS ON THIS VERY IMPORTANT SECURITY TOPIC.



Building Safe Passwords

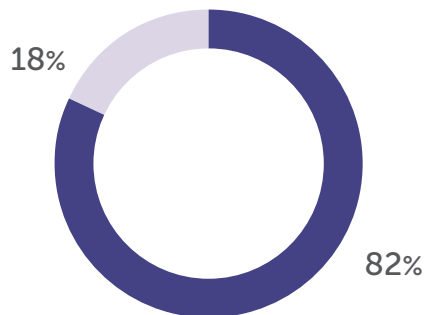
We often hear a lot about passwords, but from our data on nearly **1 million questions** asked around this topic, end users performed best with only **10%** of the questions being missed. It is also one of the **top three** areas with **68%** of security professionals assessing.



MOST MISSED QUESTIONS IN THIS AREA WERE RELATED TO USE OF PERSONAL INFORMATION LIKE BIRTH DATES OR WEDDING DATES WHEN CREATING PASSWORDS.

While most industries did very well on this topic area, two struggled far more than the average (see below). But in our survey, professionals from all industries indicated that they are proactive about password-related policies and technologies.

PROFESSIONAL SERVICES	HEALTHCARE
79%	83%



Do you enforce strong password policies (require a change at least every 60 days, special characters, a certain length, etc.)?

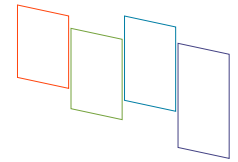
82%	18%
YES	NO

Do you use two-factor authentication?



60%	40%
YES	NO

No solution on its own is a silver bullet, a defense-in-depth strategy is best with both technical and end-user focused safeguards working together to keep your organization safe.



Measurement Is the Key to Success

It has been said before, and we will say it again — measurement is the key to success. The first step in a successful security awareness and training program is assessing employee knowledge... in other words, measurement. If you begin with measurement, then you know what topic areas to focus on and have a baseline to measure your success against going forward. Without measurement, you have no way to better understand your threats or the progress you are making with your program.

We asked two questions regarding measurement in our industry survey. Maybe not surprisingly, there was a difference between our customers and non-customers in the results, with Wombat customers significantly more likely to measure the effectiveness of their training and to follow initial assessments with training.

Do you measure the effectiveness of training?

Wombat Customers

70% **30%**
YES NO

Non-Customers

28% **72%**
YES NO

Do you follow initial assessments with training?

Wombat Customers

75% **25%**
YES NO

Non-Customers

54% **46%**
YES NO



"In Aberdeen's research — which includes 29 independent benchmark studies, involving more than 3,500 organizations, completed over a 5-year period — the leading performers were 70% more likely than the lagging performers to have invested in security awareness and training for their end-users. The 2016 *Beyond the Phish* report confirms not only that Wombat's customers are focused on measuring training effectiveness, but also that they are making progress in improving end-user knowledge across several key dimensions."

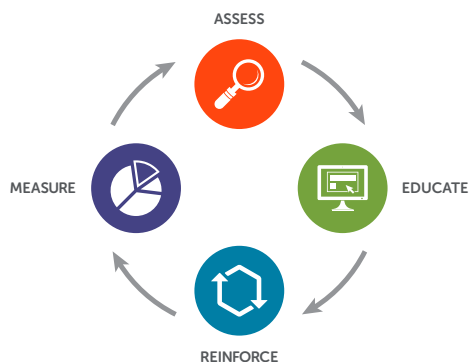
- Derek Brink, Aberdeen Research

Read the Aberdeen Group report, [The Last Mile in IT Security: Changing User Behavior](#).

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 cyber security and develop novel, more effective anti-phishing solutions. These technologies and research provided the foundation for Wombat's Security Education Platform and its unique Continuous Training Methodology. The methodology, comprised of a continuous cycle of assessment, education, reinforcement, and measurement, has been shown to deliver up to a 90% reduction in successful phishing attacks and malware infections.



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