# The State of Security Education: Phishing and Beyond
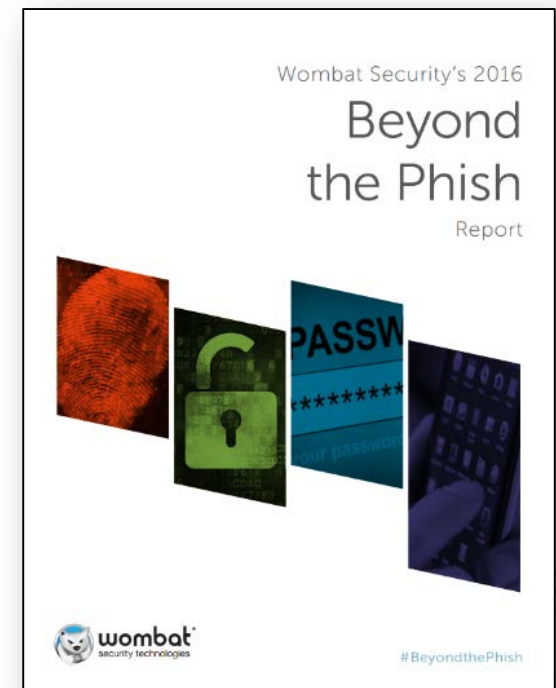
About Wombat Security

- Born from research at Carnegie Mellon University in 2008

- Achieved over 100% year over year growth in sales four years in a row

- Ranked 144 on Deloitte Technology Fast 500™

- A leader for 3 consecutive years in the Gartner Magic Quadrant

Deloitte.
Technology Fast500

Carnegie Mellon

GARTNER'S
MAGIC
QUADRANT

wombat
security technologies

Research
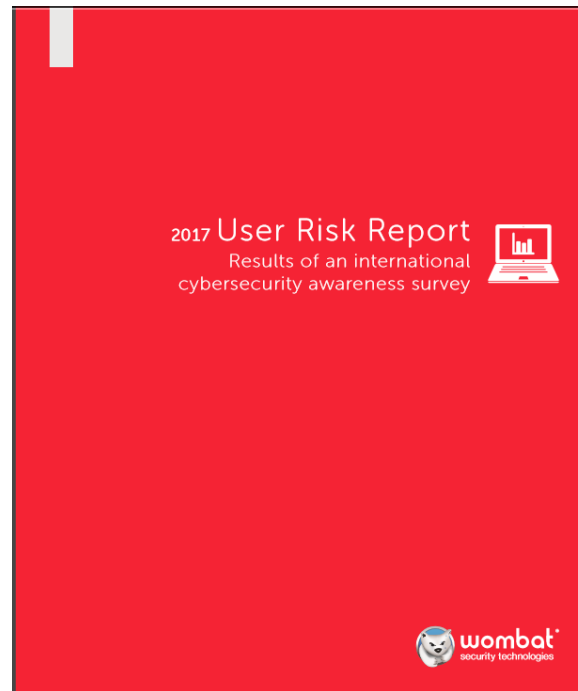
2017 report just released!

Phishing

Respondents in the US and the UK had similar levels of understanding of this topic:

GLOBAL AVERAGE

70%
CORRECT ANSWER

17%
INCORRECT ANSWER

13%
NO GUESS
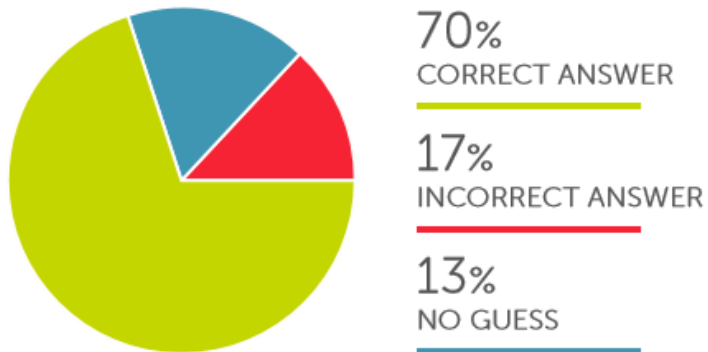
Ransomware

What Is Ransomware?

US			UK
	37%	CORRECT ANSWER	42%
	42%	INCORRECT ANSWER	19%
	21%	NO GUESS	39%

wombat
security technologies
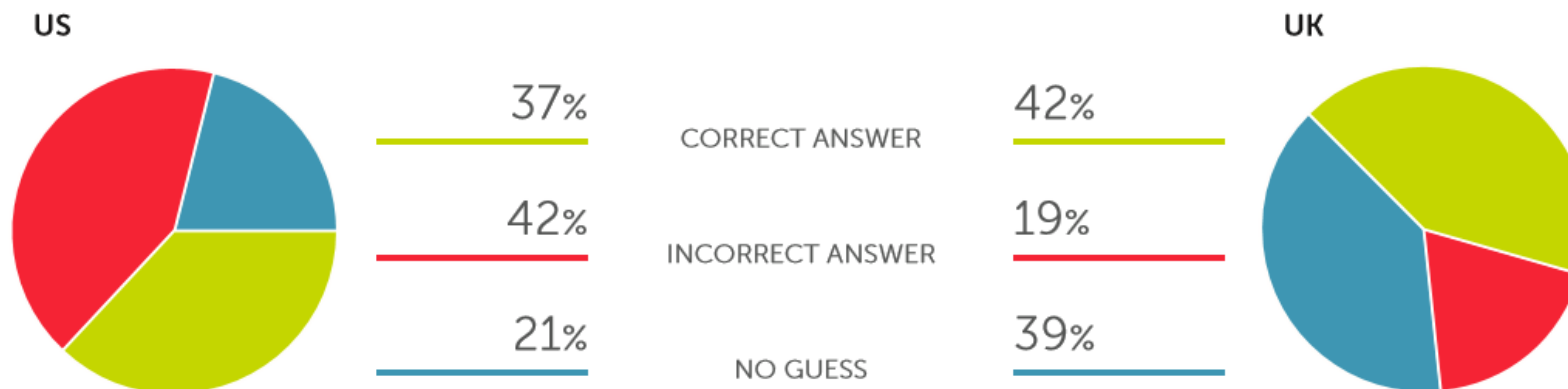
General Knowledge

Can Your Anti-Virus Software Stop a Cyberattack?

US

58% — YES — 37%

32% — NO — 45%

10% — I DON'T KNOW — 18%

UK

wombat
security technologies
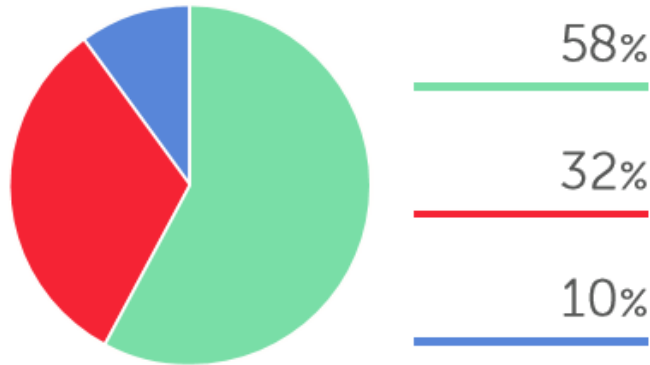
General Knowledge

Does a Trusted Location = Trusted WiFi?

We presented our survey participants with what we thought was a relatively straightforward question: *If you are in a place you trust — like a nice hotel, 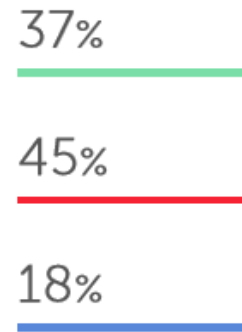local coffee shop, or international airport — can you trust that location's free WiFi service to keep your information secure?* We were surprised by the number of people (particularly those in the US) who have misplaced trust in these networks.

US 54% YES

UK 27% YES

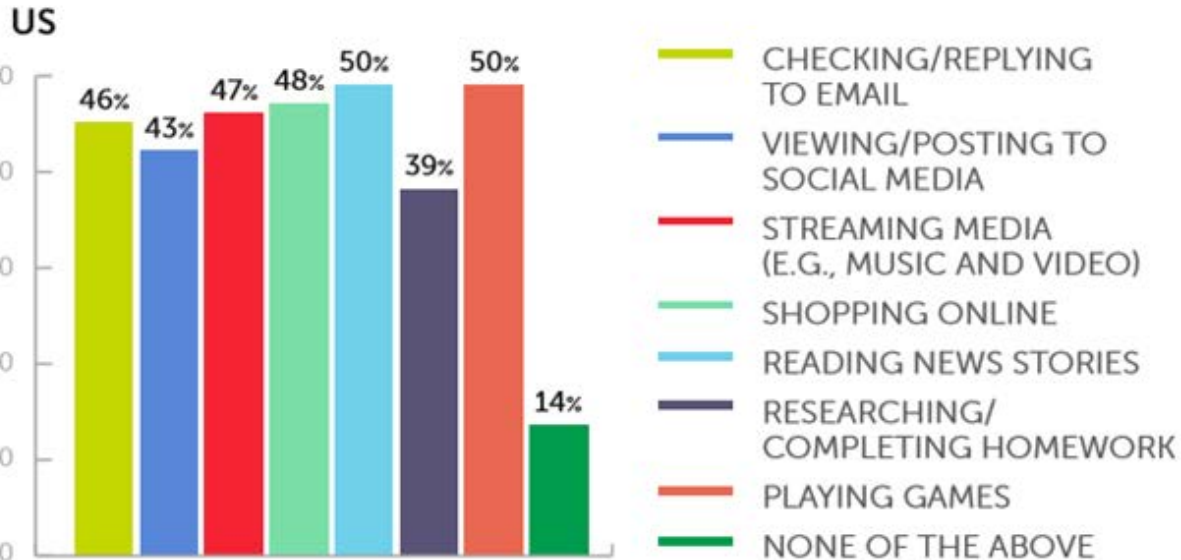## Are Business Pages Approved by Social Platforms Before Being Posted?

Unfortunately, too many employees believe that platforms like Facebook, Instagram, and Twitter approve business pages before allowing them to be posted (though US employees once again lag behind their UK counterparts).

US 57% YES

UK 25% YES

wombat
security technologies

Personal Use of Corporate Devices

What Personal Activities Do You Allow Family Members or Trusted Friends to Perform on Your Corporate Device? *(Multiple responses permitted)*

Well, we admit it: we were floored to see how many employees (particularly those in the US) give their friends and family members access to their corporate devices.

US

Activity	Percentage
CHECKING/REPLYING TO EMAIL	46%
VIEWING/POSTING TO SOCIAL MEDIA	43%
STREAMING MEDIA (E.G., MUSIC AND VIDEO)	47%
SHOPPING ONLINE	48%
READING NEWS STORIES	50%
RESEARCHING/ COMPLETING HOMEWORK	39%
PLAYING GAMES	50%
NONE OF THE ABOVE	14%

wombat
security technologies

State of the Phish 2017

Phishing Threats

What are Companies Experiencing?

76% reported being the victim of a phishing attack in 2016

Down **10%** from 2015

51% said the rate of phishing attacks is increasing

Down **15%** from 2015

45% said the rate of phishing attacks is decreasing

4% said the rate has stayed the same

44% experienced phishing through phone calls (vishing) and SMS messaging (smishing)

Decrease of **20%** from 2015

4% experienced phishing through USB attacks

Decrease of **33%** from 2015

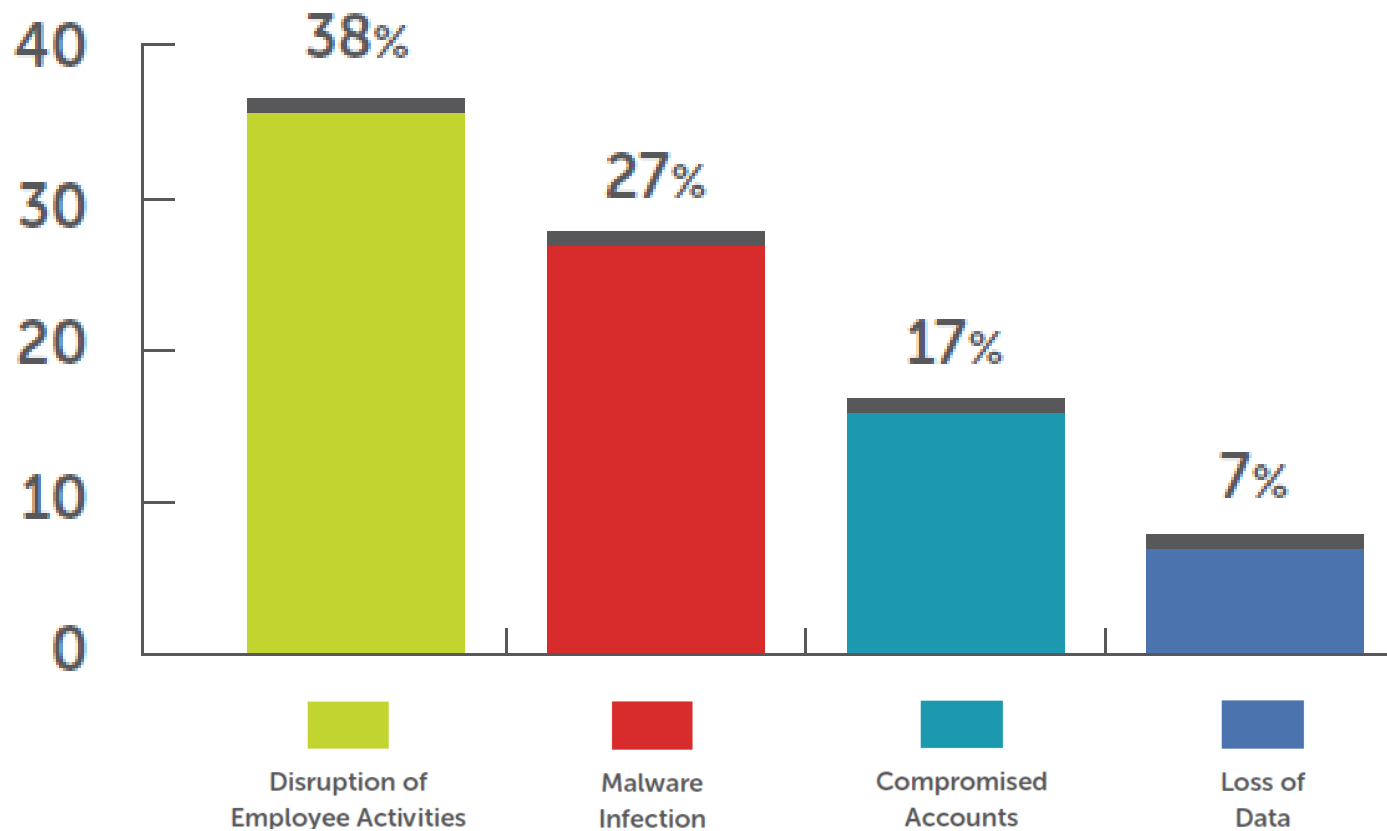**#StateofthePhish**

wombat
security technologies

Why Should You Care?

- Phishing attacks are increasing in complexity

- Attackers are targeting the end user

- Increasing reliance on end users to make responsible security decisions

- An increasingly connected and at-risk workforce

- Attacks cost your organization money and time

wombat
security technologies

The Impact of Phishing

What has the impact of phishing been on your organization? (choose all that apply)

38%	27%	17%	7%
Disruption of Employee Activities	Malware Infection	Compromised Accounts	Loss of Data

wombat
security technologies
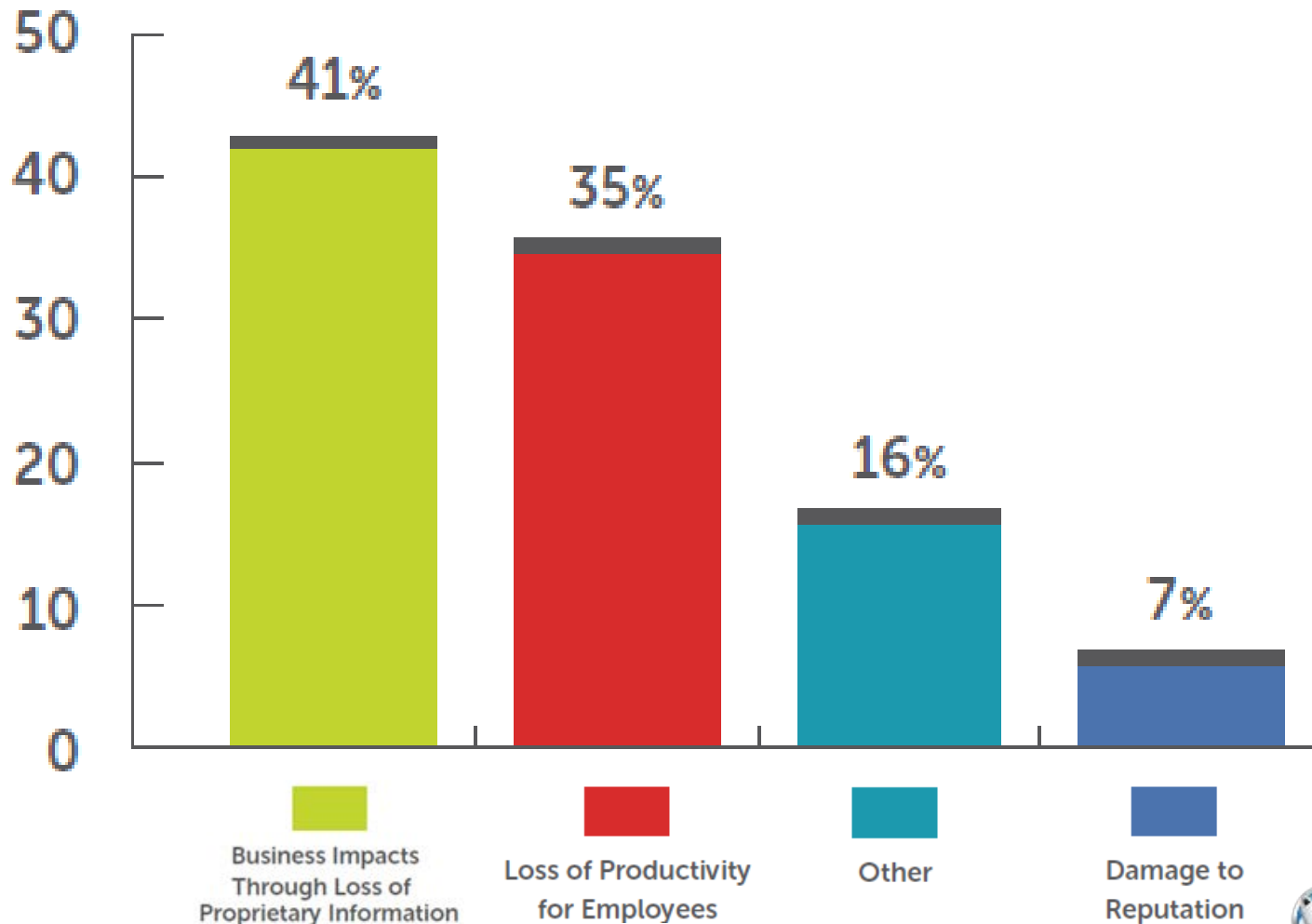
Breaches per Threat Action
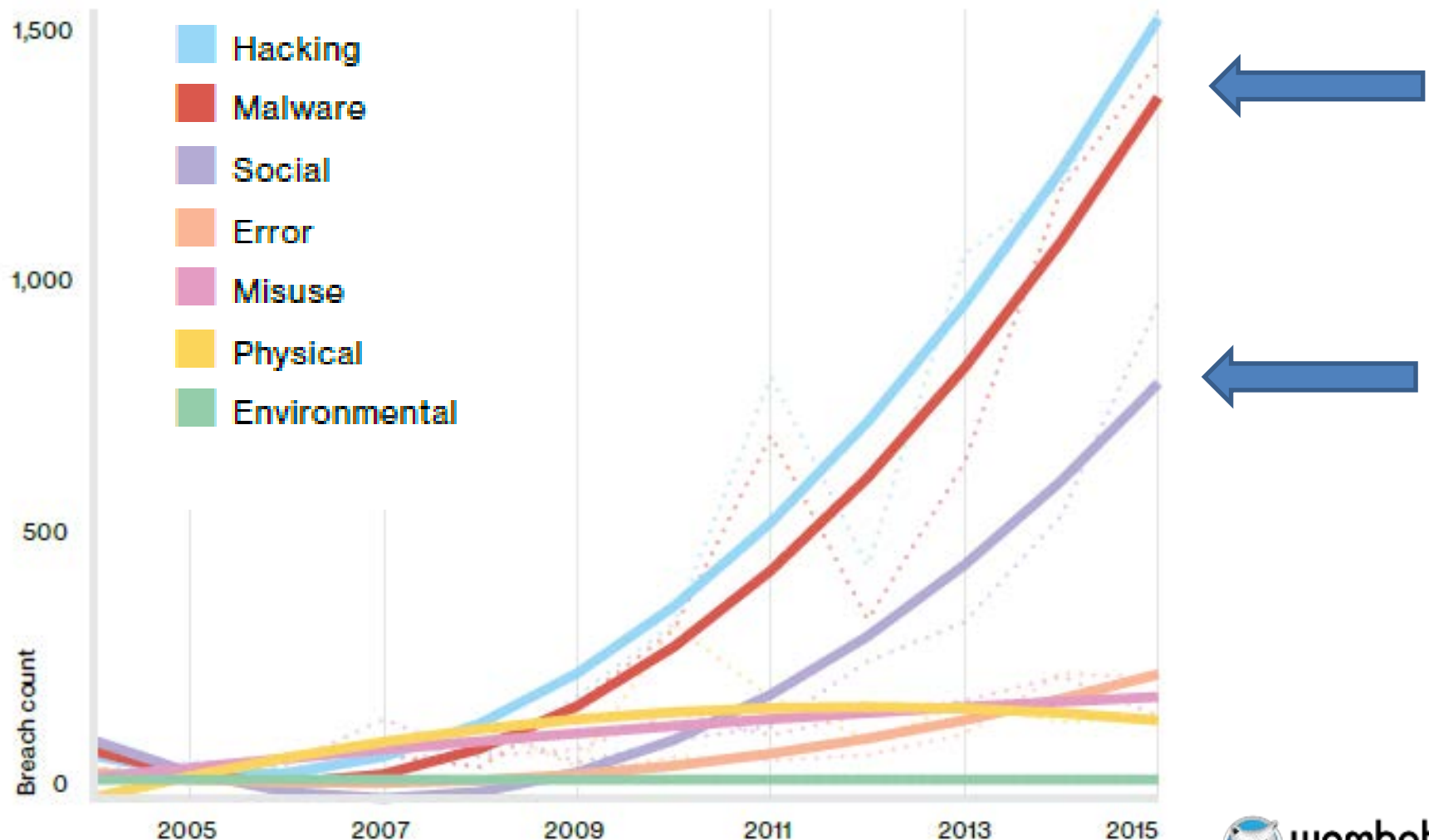
2016 Verizon Data Breach Investigations Report

Breaches Per Asset Category
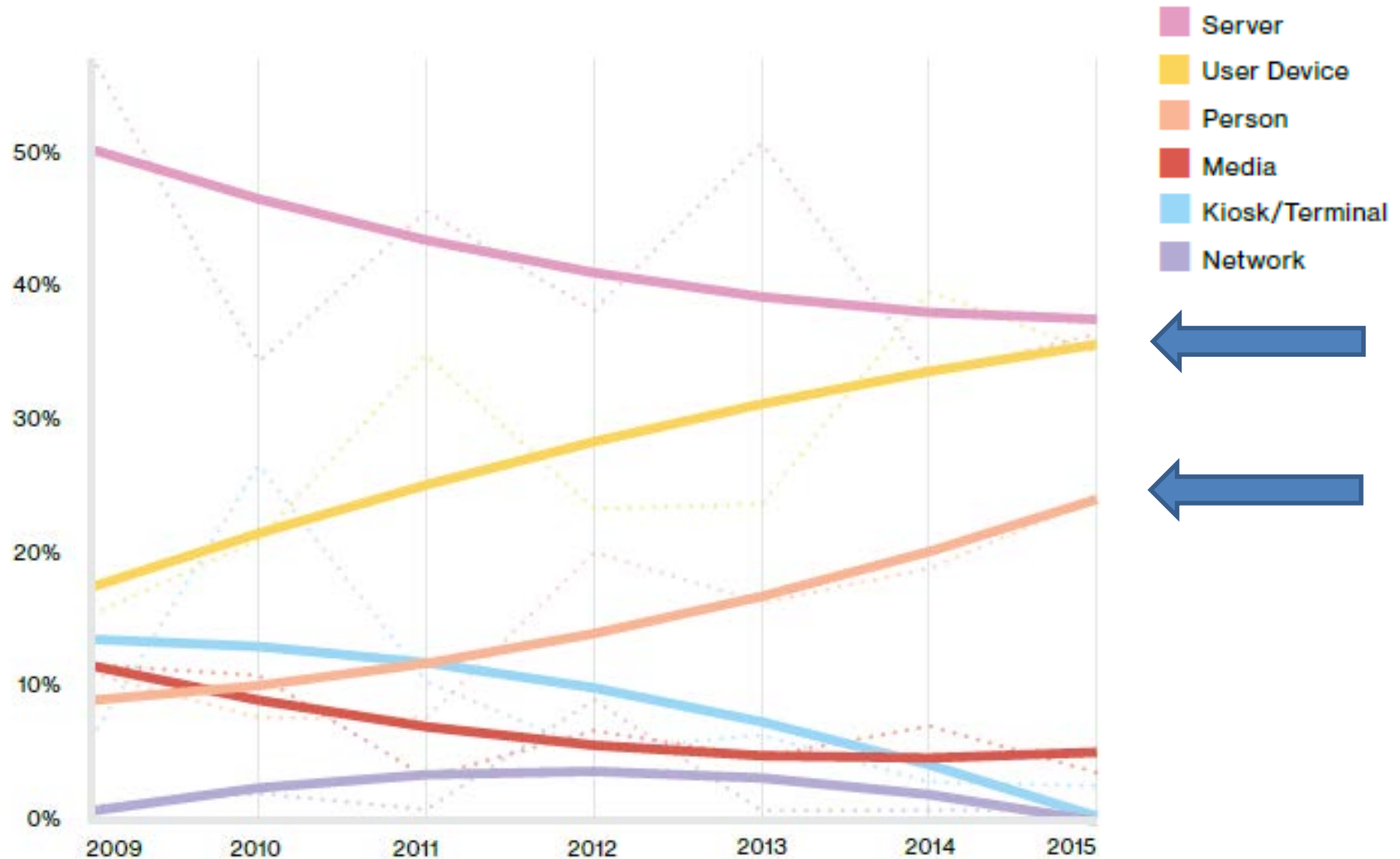
2016 Verizon Data Breach Investigations Report

Phishing Root Cause

Imposter Phone Calls

Unsafe Browsing

Oversharing on Social Networks

Roughly 156 million phishing emails are sent globally every day[1]

[1]Symantec Security Technology and Response Group

wombat
security technologies

Beyond the Phish

Beyond the Phish Data

Data compiled from Wombat Security and direct feedback from InfoSec professionals
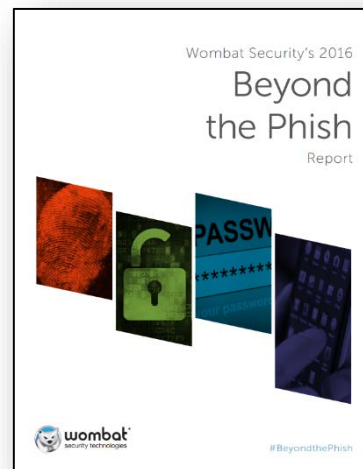
Wombat Assessment Data

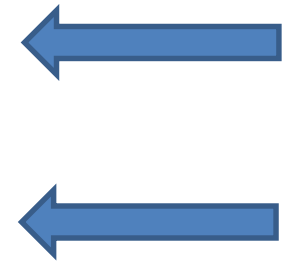- Analysis of data from nearly 20 million questions asked and answered inside the Wombat Security Education Platform

- Assessment data spans 2014 to 2016

InfoSec Professionals Survey

- Feedback from over 300 surveys
- Over 15 different industries

Topics Security Teams Assess On

WHAT ORGANIZATIONS ARE ASSESSING:

Topic	%
USING THE INTERNET SAFELY	79%
PROTECTING CONFIDENTIAL INFORMATION	78%
BUILDING SAFE PASSWORDS	68%
USING SOCIAL MEDIA SAFELY	55%
PROTECTING MOBILE DEVICES AND INFORMATION	52%
PROTECTING AND DISPOSING OF DATA SECURELY	51%
PROTECTING AGAINST PHYSICAL RISKS	51%
WORKING SAFELY OUTSIDE THE OFFICE	50%

% OF ORGANIZATIONS

#BeyondthePhish

wombat
security technologies

Where are Users Strong or Weak?
% incorrect answers

Chart: % QUESTIONS MISSED

- USING THE INTERNET SAFELY: 16%
- PROTECTING CONFIDENTIAL INFORMATION: 27%
- BUILDING SAFE PASSWORDS: 10%
- USING SOCIAL MEDIA SAFELY: 31%
- PROTECTING MOBILE DEVICES AND INFORMATION: 15%
- PROTECTING AND DISPOSING OF DATA SECURELY: 30%
- PROTECTING AGAINST PHYSICAL RISKS: 15%
- WORKING SAFELY OUTSIDE THE OFFICE: 26%
- IDENTIFYING PHISHING THREATS: 28%

#BeyondthePhish (2016)

wombat security technologies

Using Social Media Safely

31% ~~31%~~ **22%**

QUESTIONS MISSED

- Most missed questions were around being vigilant in recognizing if you are dealing with a friend's fake profile and posts
  - Look for posts that are out of the ordinary, spelling and grammar errors

- 70% of social media scams were shared manually (compared to only 2% in 2013)*

  * SYMANTEC CORPORATION Study: Internet Security Threat Report 2015

wombat
security technologies

Using Social Media Safely

31%
QUESTIONS MISSED

55% Assess on using Social Media safely

76% Allow access to Social Media on work devices

Using Social Media Safely

55% Assess on using Social Media safely

76% Allow access to Social Media on work devices

29%

38%

33%

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?

WE'RE NOT VERY CONFIDENT   WE'RE NEUTRAL   WE'RE CONFIDENT

#BeyondthePhish

wombat
security technologies

Protect and Dispose of Data Securely

30% ~~30%~~ **25%** QUESTIONS MISSED
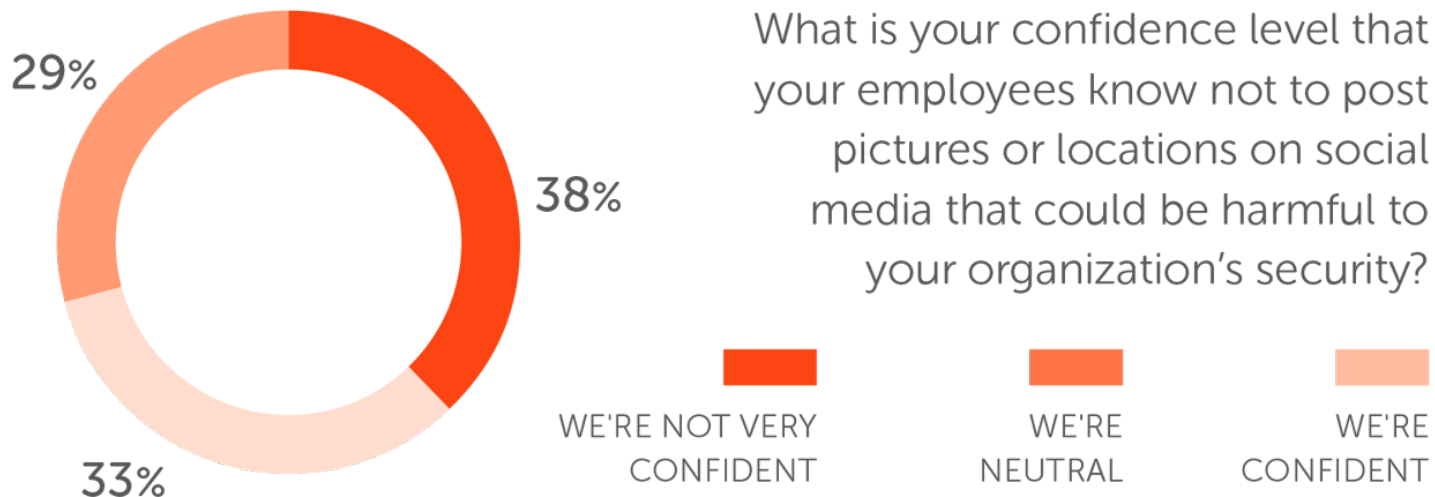
What Types of Questions were Asked?

- Lifecycle of data - from creation to deletion
- Handling PII
- Using USBs
- Deleting files from hard drives
- Securing work devices

One of the common misconceptions from end users is that there is technology in place that will protect them from being hacked so they did not need to be as vigilant
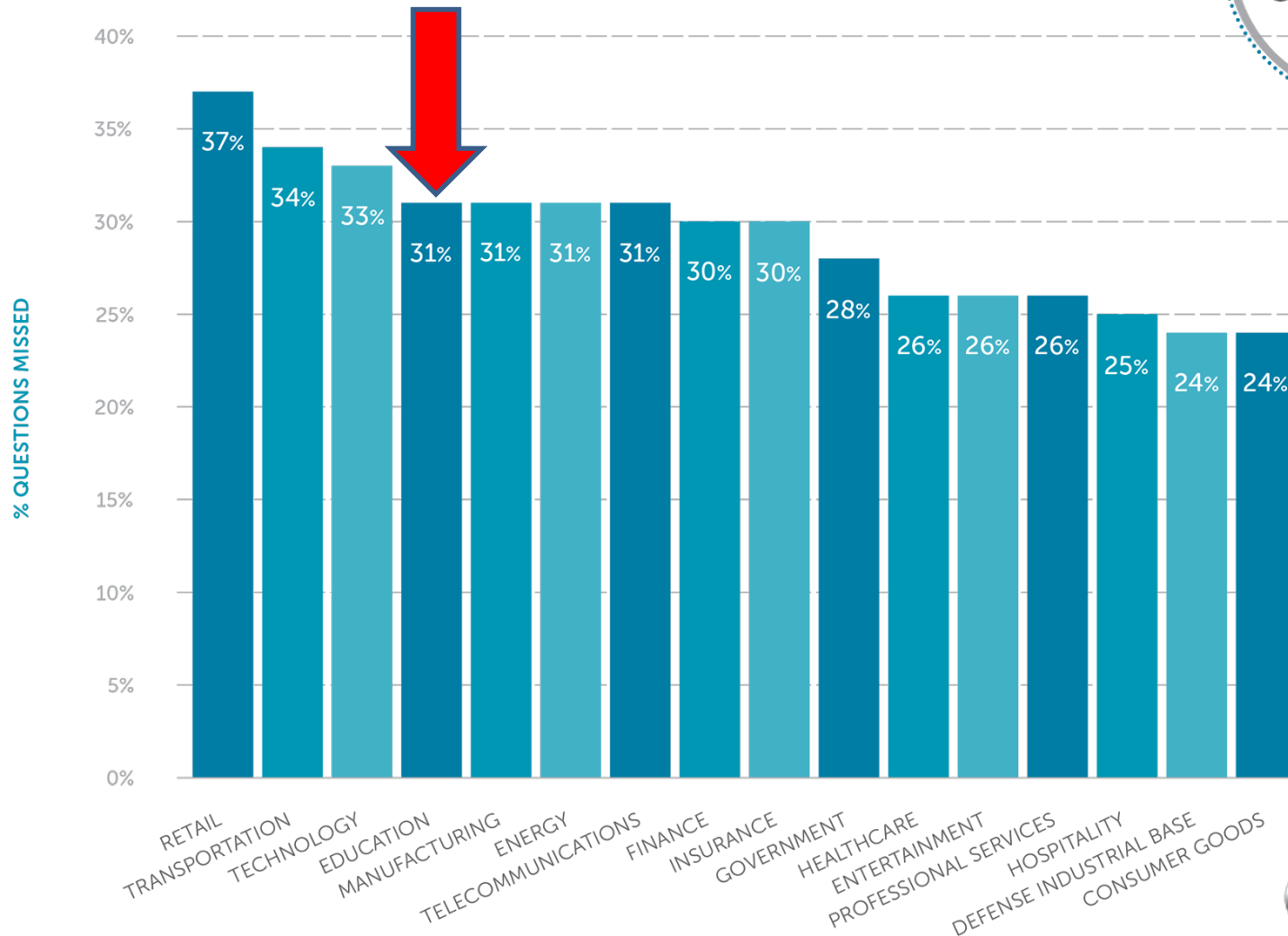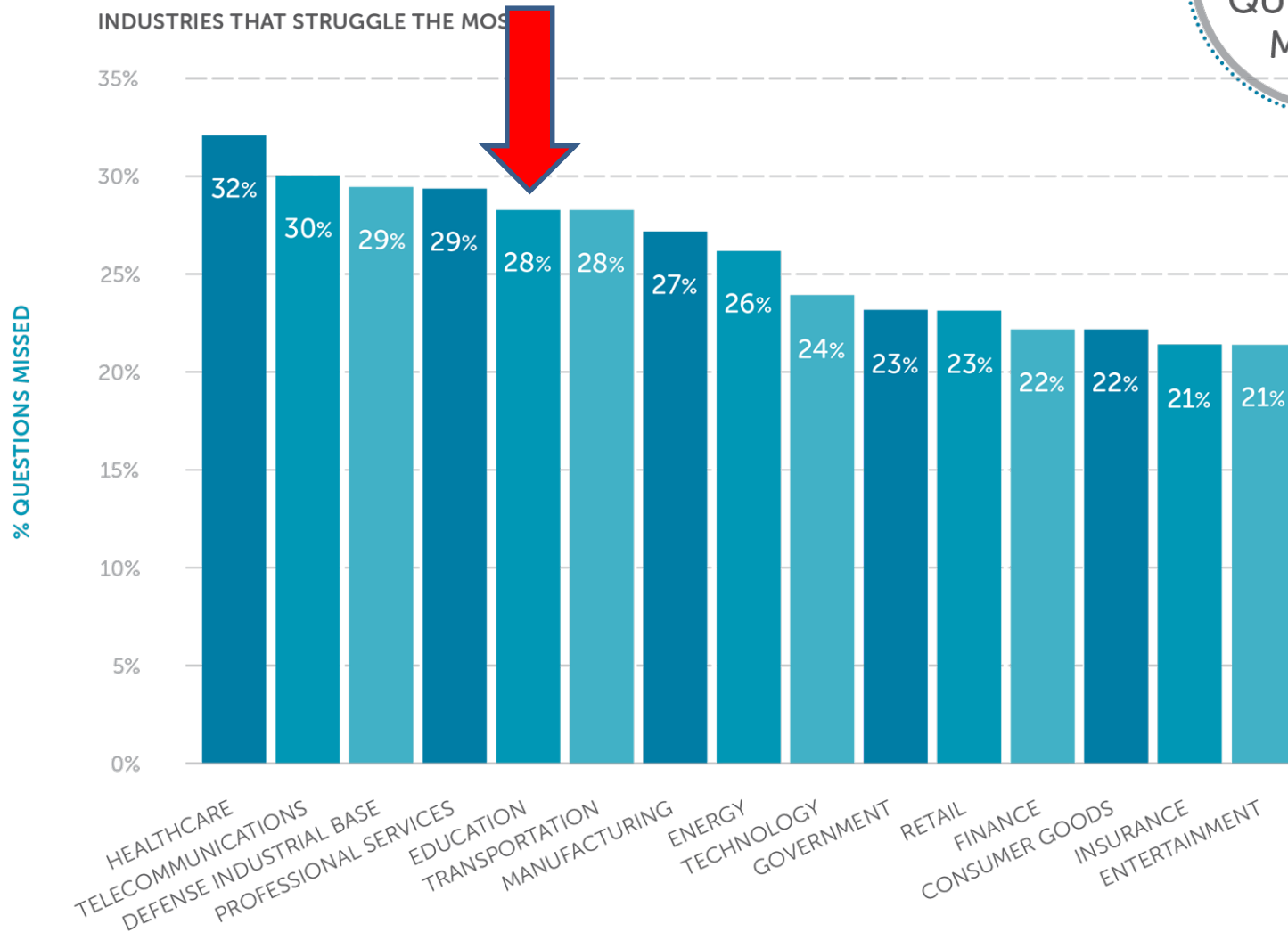
wombat
security technologies

Protect and Dispose of Data
A Big Problem

30%
QUESTIONS MISSED

INDUSTRIES THAT STRUGGLE THE MOST:

% QUESTIONS MISSED

Industry	%
RETAIL	37%
TRANSPORTATION	34%
TECHNOLOGY	33%
EDUCATION	31%
MANUFACTURING	31%
ENERGY	31%
TELECOMMUNICATIONS	31%
FINANCE	30%
INSURANCE	30%
GOVERNMENT	28%
HEALTHCARE	26%
ENTERTAINMENT	26%
PROFESSIONAL SERVICES	26%
HOSPITALITY	25%
DEFENSE INDUSTRIAL BASE	24%
CONSUMER GOODS	24%

wombat security technologies

Protect Confidential Information
Another Big Problem

27% 26%
QUESTIONS MISSED

INDUSTRIES THAT STRUGGLE THE MOST

% QUESTIONS MISSED

Industry	%
HEALTHCARE	32%
TELECOMMUNICATIONS	30%
DEFENSE INDUSTRIAL BASE	29%
PROFESSIONAL SERVICES	29%
EDUCATION	28%
TRANSPORTATION	28%
MANUFACTURING	27%
ENERGY	26%
TECHNOLOGY	24%
GOVERNMENT	23%
RETAIL	23%
FINANCE	22%
CONSUMER GOODS	22%
INSURANCE	21%
ENTERTAINMENT	21%

wombat
security technologies

Work Safely Outside the Office

20%

26% QUESTIONS MISSED

- Only 50% are assessing around this topic
- Most missed questions were around safely connecting to WiFi

wombat
security technologies

Work Safely Outside the Office

26%
QUESTIONS
MISSED

- Only 50% are assessing around this topic
- Most missed questions were around safely connecting to WiFi

How confident are you that employees don't connect to public WiFi networks without a protected connection such as a VPN?
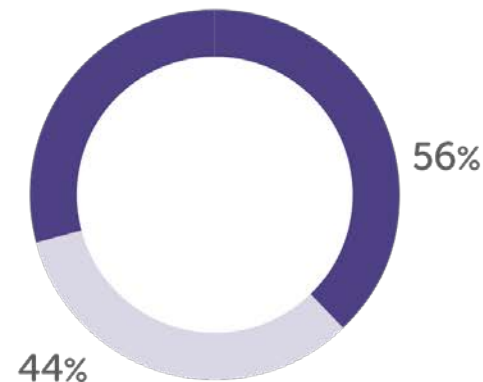
52% NOT VERY CONFIDENT   **32%** NEUTRAL   **17%** CONFIDENT

wombat
security technologies

Work Safely Outside the Office

26%
QUESTIONS
MISSED

- Only 50% are assessing around this topic
- Most missed questions were around safely connecting to WiFi

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

52%
NOT VERY
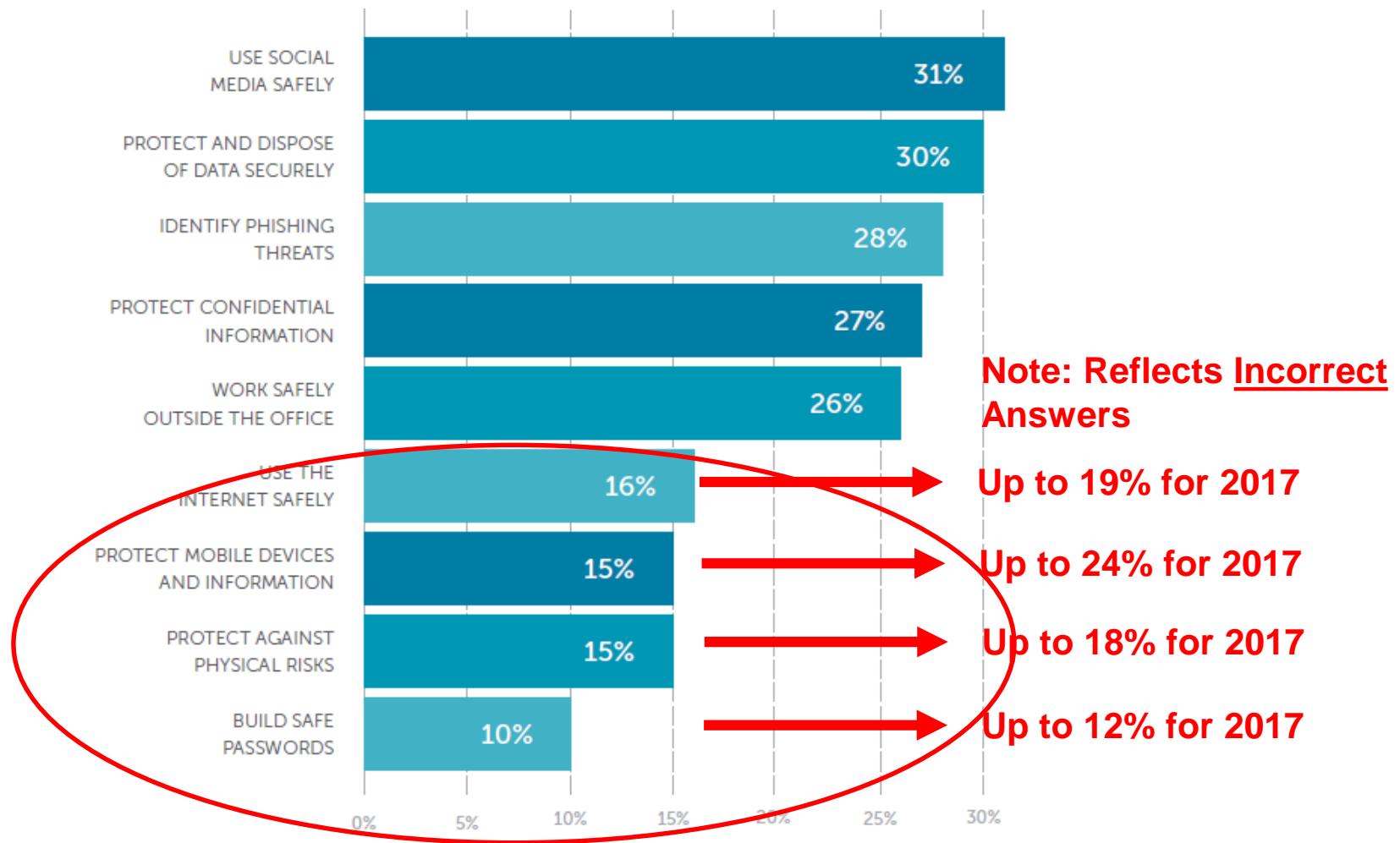CONFIDENT

32%
NEUTRAL

17%
CONFIDENT

Do you have a security policy/guideline for employees to follow while traveling?
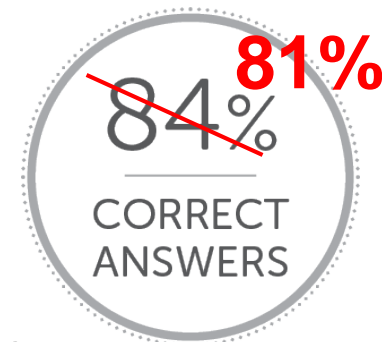
56%
YES

44%
NO

56%

44%

wombat
security technologies

Where do End Users Succeed?

USE SOCIAL MEDIA SAFELY — 31%
PROTECT AND DISPOSE OF DATA SECURELY — 30%
IDENTIFY PHISHING THREATS — 28%
PROTECT CONFIDENTIAL INFORMATION — 27%
WORK SAFELY OUTSIDE THE OFFICE — 26%
USE THE INTERNET SAFELY — 16%
PROTECT MOBILE DEVICES AND INFORMATION — 15%
PROTECT AGAINST PHYSICAL RISKS — 15%
BUILD SAFE PASSWORDS — 10%

Note: Reflects <u>Incorrect</u> Answers

Up to 19% for 2017

Up to 24% for 2017

Up to 18% for 2017

Up to 12% for 2017

wombat
security technologies

Use the Internet Safely

81% ~~84%~~ CORRECT ANSWERS

- 79% are assessing around this topic
- Defense Industrial Base did the best, getting 90% correct around this topic

What is your confidence level that employees understand safe practices for browsing the internet (such as logging out of web apps before closing, etc)?
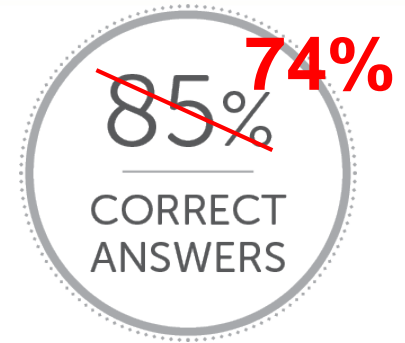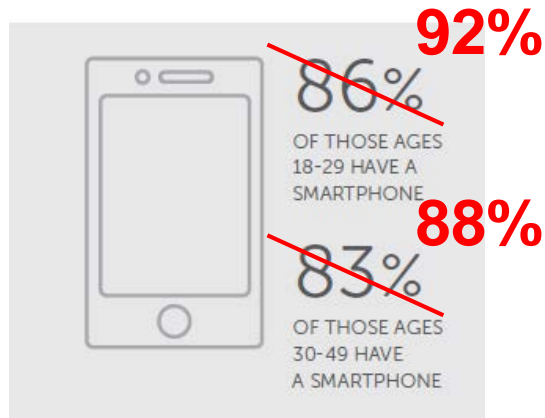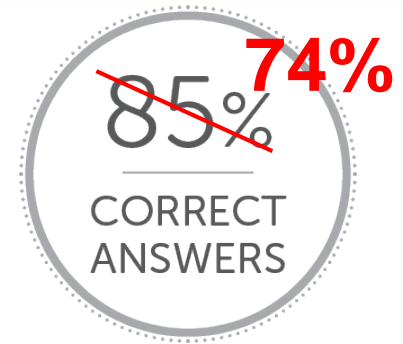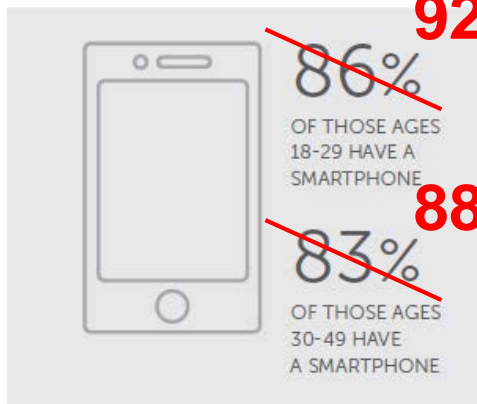
31% NOT VERY CONFIDENT

52% NEUTRAL

17% CONFIDENT

wombat security technologies

Protect Mobile Devices and Information

74%
~~85%~~
CORRECT ANSWERS

ACCORDING TO PEW RESEARCH, AS OF OCTOBER 2015

92%
~~86%~~
OF THOSE AGES 18-29 HAVE A SMARTPHONE

88%
~~83%~~
OF THOSE AGES 30-49 HAVE A SMARTPHONE

wombat
security technologies

Protect Mobile Devices and Information

74%
~~85%~~
CORRECT
ANSWERS

ACCORDING TO PEW RESEARCH,
AS OF OCTOBER 2015

92%
~~86%~~
OF THOSE AGES
18-29 HAVE A
SMARTPHONE

88%
~~83%~~
OF THOSE AGES
30-49 HAVE
A SMARTPHONE

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

67% YES   33% NO

wombat
security technologies

Protect Mobile Devices and Information

74%
~~85%~~
CORRECT ANSWERS

ACCORDING TO PEW RESEARCH,
AS OF OCTOBER 2015

92%
~~86%~~
OF THOSE AGES 18-29 HAVE A SMARTPHONE

88%
~~83%~~
OF THOSE AGES 30-49 HAVE A SMARTPHONE
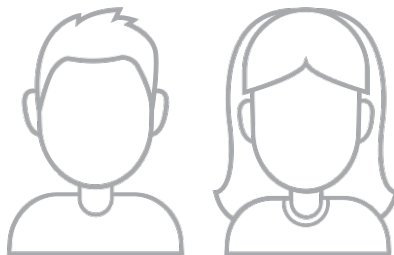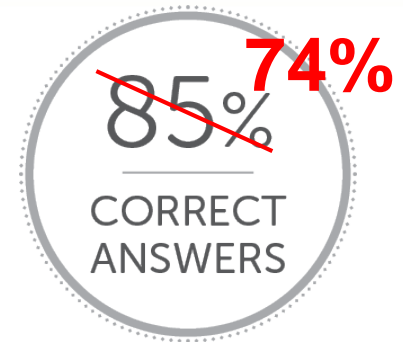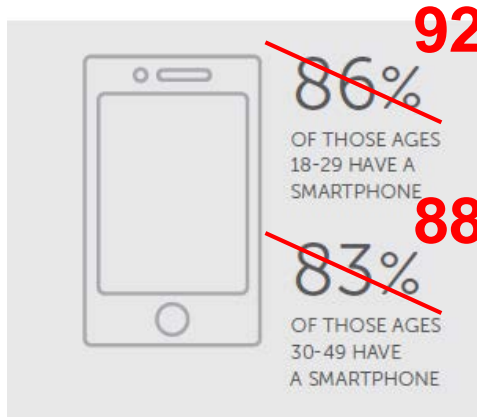
- Only 52% are assessing around this topic
- Most missed questions were around connecting to Bluetooth

Does your organization provide mobile/BYOD device programs that allow network access?
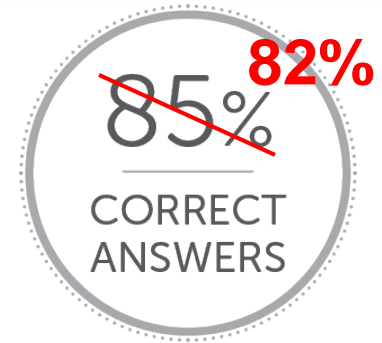
67% YES

33% NO

wombat
security technologies

Protect Against Physical Risk

82%

~~85%~~
CORRECT
ANSWERS
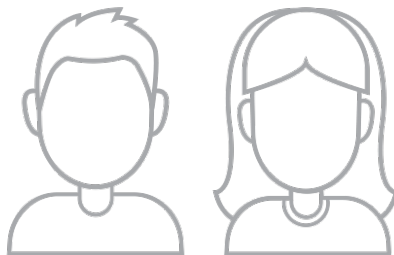
- 51% are assessing around this topic
- Top questions missed around computer safety in the office
  - locking your computer when you walk away
  - locking devices in your drawer overnight
- 55% of theft-related incidents occurred within the victim's work area*

*2015 Verizon Data Breach Investigations Report

wombat
security technologies

Build Better Passwords

88%

90%
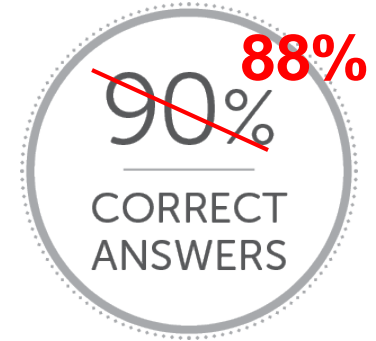
CORRECT
ANSWERS

- 68% assess on this topic

- Top questions missed around not using personal information to create passwords like birth dates or wedding dates

- Entertainment industry did the best in this topic, getting 93% of all questions correct.

wombat
security technologies

Build Better Passwords

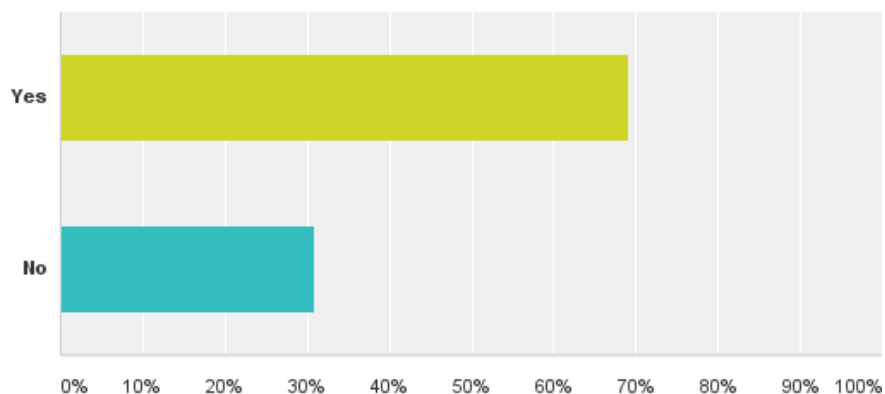**Do you enforce strong password policies?**
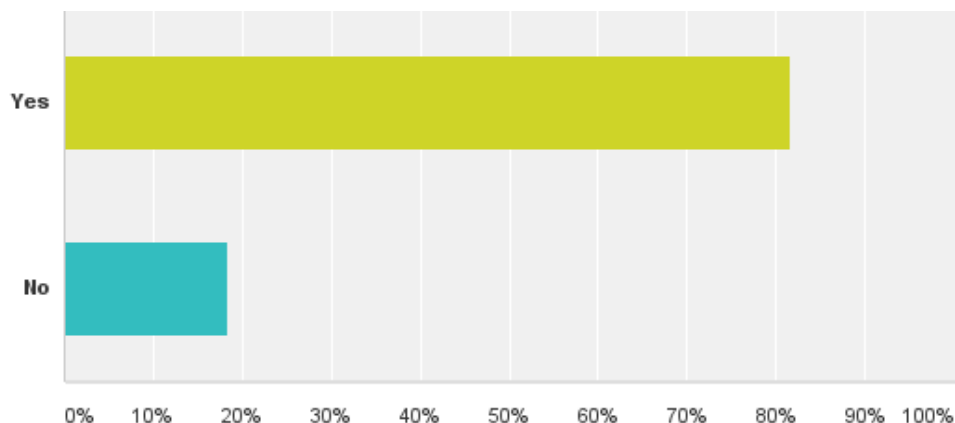
Do you use two-factor authorization?
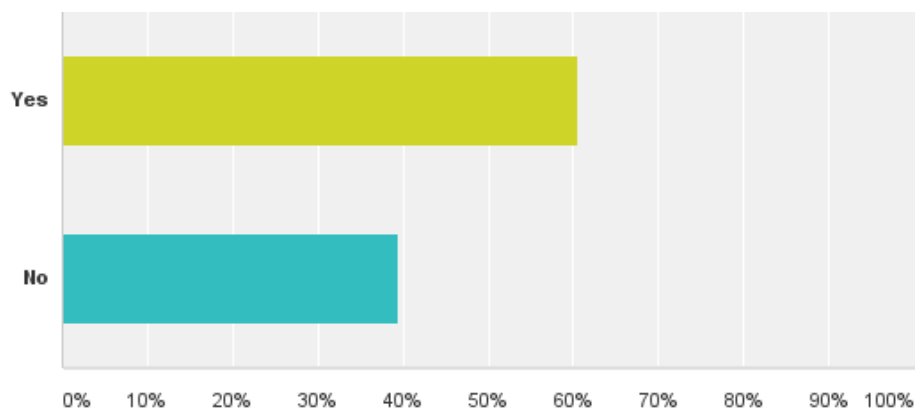
Measurement is Key

- Assessing allows you to:
  - Identify problem areas
  - Have something to measure progress against

Wombat Customers

Non-Customers

wombat
security technologies
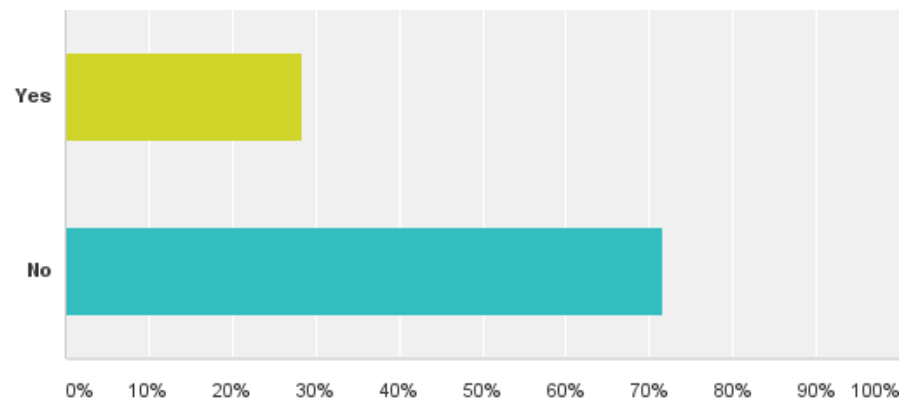
Simulated Attack vs. Assessments in 2017

Healthcare

18%

CLICK RATE IN
SIMULATED PHISHING ATTACKS

VS.

26%

QUESTIONS MISSED IN ASSESSMENTS

Government

14%

CLICK RATE IN
SIMULATED PHISHING ATTACKS

VS.

24%

QUESTIONS MISSED IN ASSESSMENTS

wombat
security technologies

Continuous Training Methodology

ASSESS

Knowledge assessments
Mock attacks

Detailed reports
show progress

MEASURE

Analyze
and
Repeat

EDUCATE

Interactive training
modules & games

Report phish, posters,
articles, newsletters, gifts

REINFORCE

wombat
security technologies
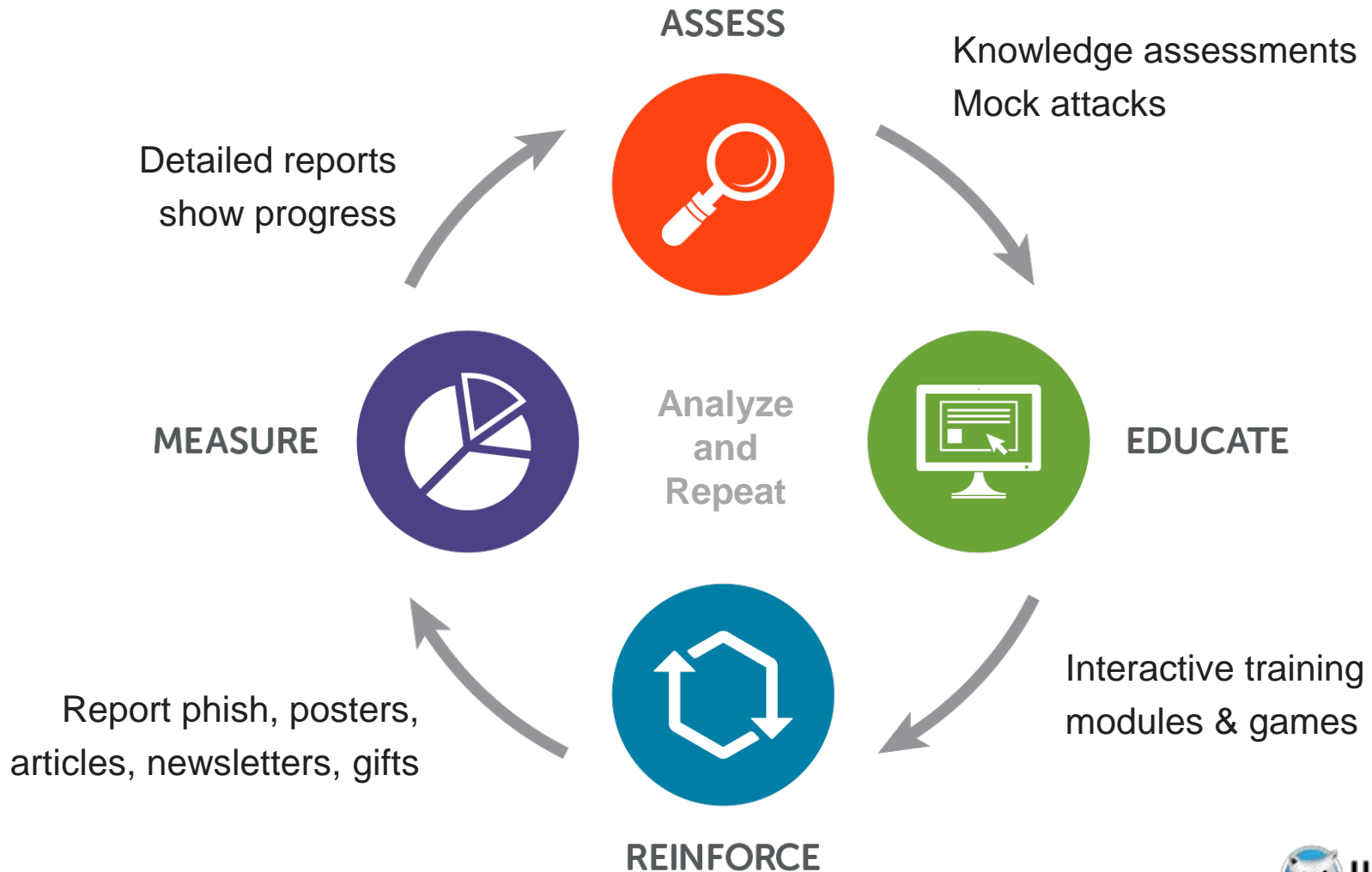
Application of Learning Science Principles

- Present concepts and procedures together

- Bite-sized lessons

- Learn by doing

- Story-based environment

- Provide immediate feedback

- Create teachable moments

- Use conversational tone

- Collect valuable data

Why You Should Pay Attention to Permissions

Some functions can expose you, your device, and your data to risks

Be very cautious of apps with unnecessary permissions (e.g., a flashlight app that accesses text messages)

Depending on your device, you may have little or no control over the permissions granted to an installed app

FREEtunes
7th Row Media
1,402,762 downloads
★★★★☆

Version 5.3 | Updated on Nov 18, 2013

Description: Search for and download the latest singles and albums by the top 100 artists for free.

Reviews | Permissions / Access Rights

4.4
★★★★☆
837 total

★ 5   382
★ 4   418
★ 3   27
★ 2   9
★ 1   1

★★★★☆ BakerAmy
Another winner from this developer!

★★★☆☆ jbrubaker23
I really like this app. It's easy to use.

★★★☆☆ Jamal L.
The search function is not the best, but

install
don't install

Web Search

Oops! This is a potentially risky app. Apps that provide access to illegal or pirated content are particularly dangerous. They often contain malware and other malicious content. They should be avoided.

wombat security technologies

Wombat Portfolio

ThreatSim® Simulated Attacks			Knowledge Assessments	User Behavioral Action and Response			Security Awareness Materials
Simulated Phishing Attacks	Simulated USB Attacks	Simulated Smishing Attacks	CyberStrength®	PhishAlarm®	PhishAlarm Analyzer	Education Triggers	Awareness Videos, Posters, Articles, Media

Security Education Platform
Fully integrated platform with assessments, training, reporting, and administrative features

Interactive Training Modules

Safer Web Browsing	Mobile Apps	Securing your Email Series	URL Training	Social Engineering	Safe Social Networking	Physical Security
Protecting Against Ransomware	Travel Security	Data Storage and Destruction	Mobile Device Security	Security Beyond the Office	Password Security	USB Device Safety
Email Security	Security Essentials for Executives	Security Essentials	PHI	PCI DSS	PII	GDPR

wombat
security technologies

Key Takeaways

- Phishing attacks are becoming more complex/targeted and incorporating other threat vectors

- Emerging/changing attacks (and varying user performance) requires a continuously evolving program. Set-it-and-forget-it won't suffice.

- Question-based assessments will expose user vulnerabilities 1.5 – 2x more than attack-based assessments… _AND_ provide visibility into users' specific vulnerabilities

- Informing users ≠ equipping users to **_behave_** differently

Questions?