2017 User Risk Report

Results of an international cybersecurity awareness survey

wombat security technologies

2017 User Risk Report

It is no secret that cybersecurity and its role in data protection is front-page news on a regular basis. But is the average employee reading these headlines and recognizing that their behaviors play a major role in securing their information, devices, and systems at work and at home? **That's what we wanted to find out.**

Fun Fact:
Our survey concluded less than 24 hours prior to the start of the public warnings about the WannaCry ransomware attack.

In May 2017, we surveyed more than 2,000 working adults — 1,000 in the US and 1,000 in the UK — about cybersecurity topics and best practices that are fundamental to data and network security. What we found out about the personal habits of these individuals was sometimes heartening, occasionally perplexing, and frequently terrifying — but always enlightening.

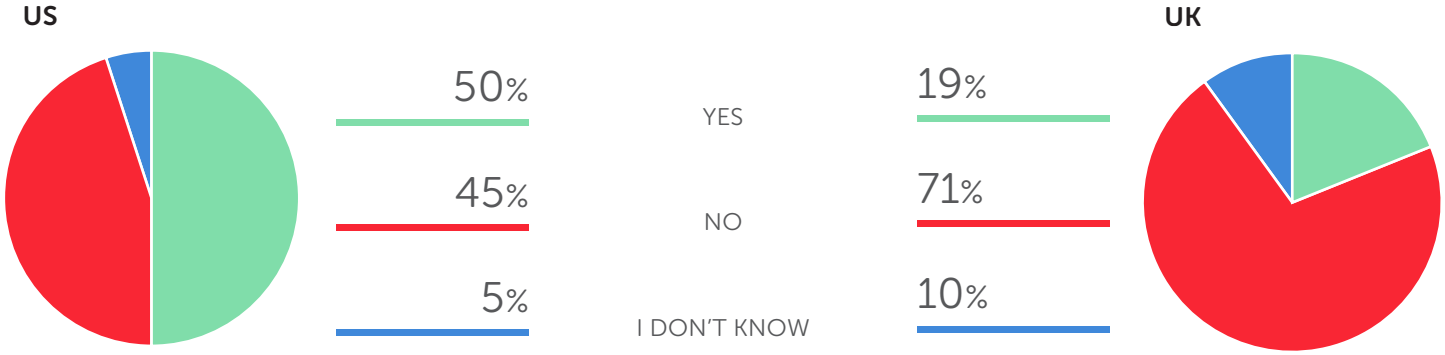
You will see some sections in which responses are presented as global averages (where responses were similar across both survey groups) while others show a breakdown by region. Though both audiences showed a clear need for improvement, there were some surprising differences in key areas, and we wanted to show these distinctions when warranted (though, for the most part, we let you draw your own conclusions about why the variances exist).

To Wet Your Whistle...

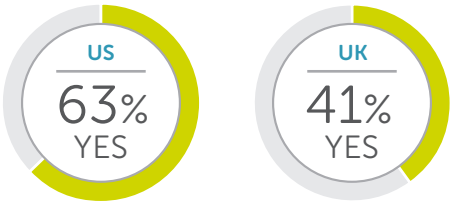
Here are a few general questions and responses we asked to set the stage for our more in-depth queries. You will no doubt find it interesting to compare these results to those presented later in this report.

Have You Ever Been the Victim of Identity Theft?

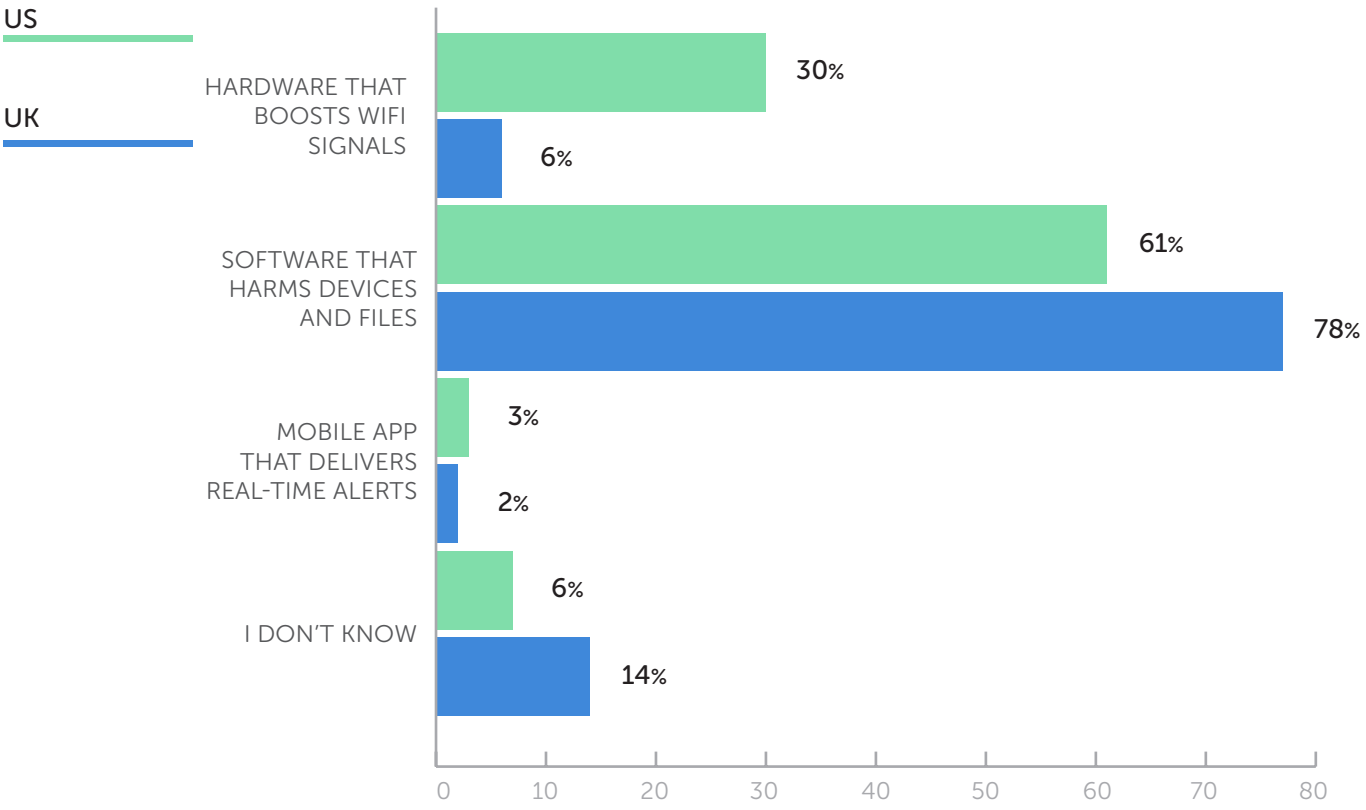
Here, we saw a major difference between US and UK respondents:



Have You or Someone You Know Had a Social Media Account Hacked or Duplicated?



What Is Malware?



You might think these results bode well for understanding of what ransomware is…**but read on**.

Phishing and Ransomware: Two Sides of the Same Coin

A Jedi master once said, "Your eyes can deceive you; don't trust them."[1] This is sage advice for all employees (regardless of midi-chlorian count) as cybercriminals rely on the art of deception. After all, phishing scams and email-based ransomware attacks are nothing without end-user interaction.

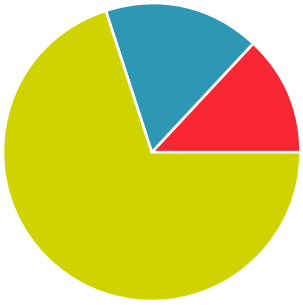
It's because phishing emails are so frequently the delivery mechanism for ransomware that we decided to report on these survey results together. Though the *2017 Data Breach Investigation Report* indicated that email supplanted web drive-by downloads as the top malware infection vector, Verizon does not tally ransomware attacks with phishing-related data breaches. Similarly, the Anti-Phishing Working Group does not include ransomware emails in its *Phishing Activity Trends Report*.[2]

Because there is so much crossover between phishing and ransomware, we feel it's critical that organizations get a good sense of employees' awareness of both of these threats and address them as two sides of the same coin.

What Is 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

These results are very similar to those noted in our *2017 State of the Phish Report*; now, as then, we are heartened to see that well more than half of employees can define phishing on basic terms. However, we remain concerned that **30%** still do not know about this threat (and that more than **10%** of respondents wouldn't even hazard a guess).

[1] Obi-Wan Kenobe, *Star Wars: Episode IV – A New Hope*

[2] "Q4 Phishing Report Shows Mixed Bag of Trends, a Need for Diverse Training," Wombat Security Blog, April 7, 2017

What Is Ransomware?

As we noted in the intro, our survey of US and UK employees concluded less than 24 hours before the WannaCry ransomware attack started its global spread. As such, the results indicated were not influenced by the significant bump in media coverage that happened following the attack.

Globally, we again saw similar levels of awareness (or lack thereof, as the case may be). However, there were far more UK employees who were not willing to even guess at the answer to the question, which is why we've broken out these responses regionally:

US

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

UK

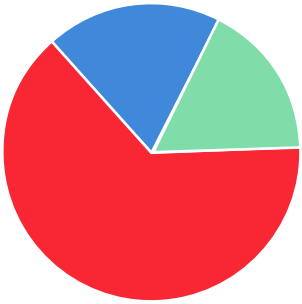
Have You Ever Fallen for a Phishing Attack?

Here, we saw a major difference between US and UK respondents:

US

	US	UK
YES	46%	17%
NO	43%	64%
I DON'T KNOW	11%	19%

UK



Of those who did admit to having fallen victim to a phishing scam, their experiences were similar in both regions, with the vast majority (**80%**) saying they had fallen for the attack on a personal device. Only **17%** indicated they had experienced an attack at work, and just **3%** fell for an attack on both a work device and a personal device.

Do You Back Up Your Important Personal Files?

It was refreshing to see that many employees are backing up their personal files, using either external hard drives, cloud storage, or a mix of the two. Our results did indicate, however, that US users are more likely to perform these tasks.

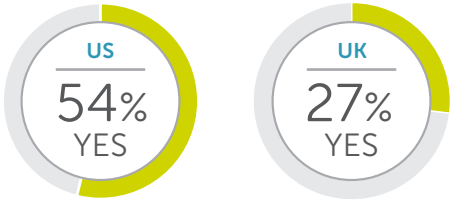
Popular Misconceptions

"Fool me once, shame on you. Fool me twice, shame on me." Or so the saying goes.

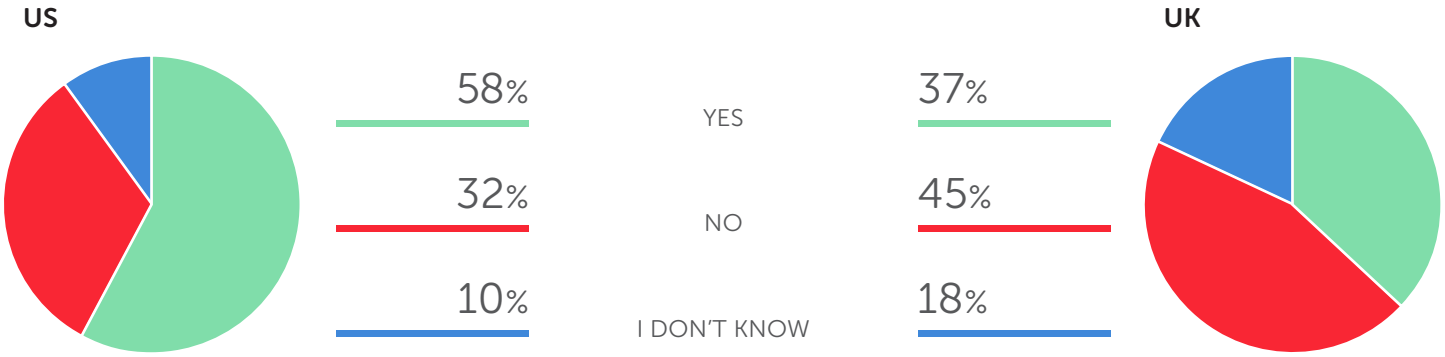
Unfortunately, it appears that some employees out there are being fooled on a regular basis.

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.



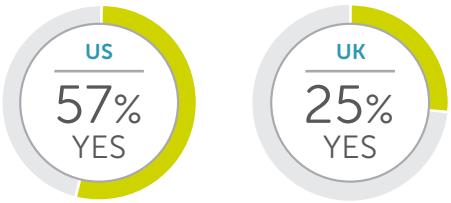
Can Your Anti-Virus Software Stop a Cyberattack?



Here again we saw a lot of false trust, with more US respondents believing anti-virus software could save them from an attack (but more UK employees failing to offer a definitive answer).

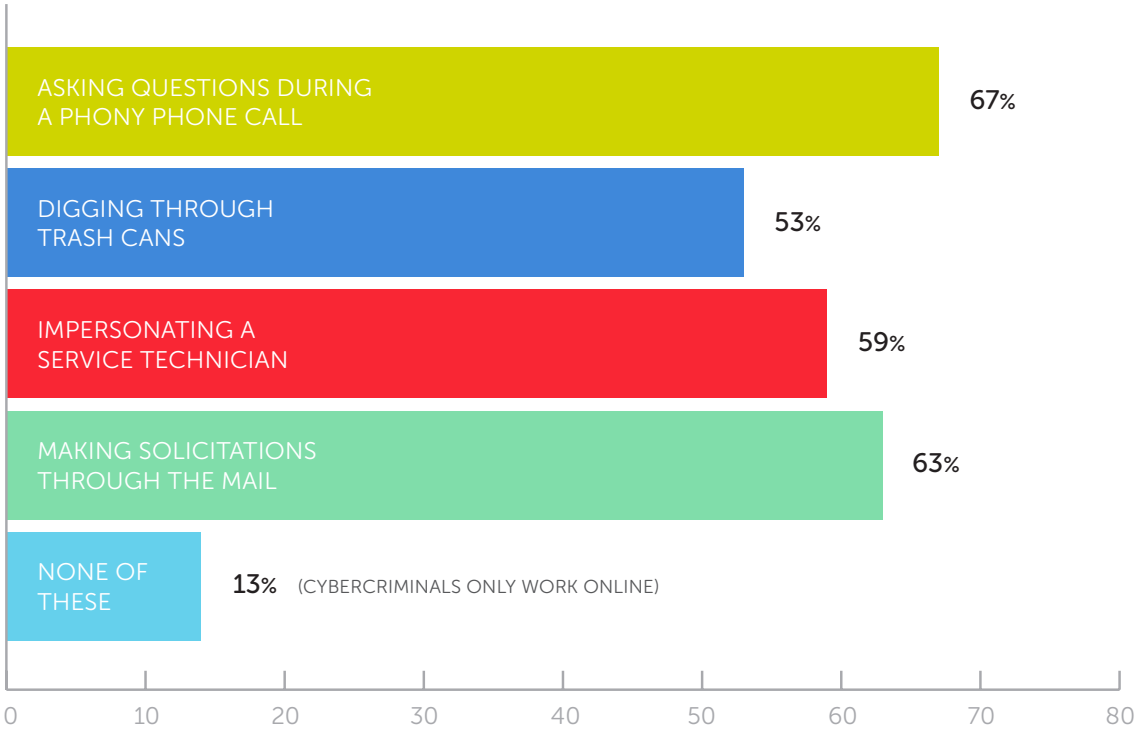
Are Business Pages Approved by Social Platforms Before Being Posted?

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).



How Do Cybercriminals Obtain Information? *(Multiple responses permitted)*

GLOBAL AVERAGES



Globally, there was a fair amount of recognition that cybercriminals utilize multiple attack vectors (though there are clearly still those who are not aware that cybercriminals employ social engineering tactics offline).

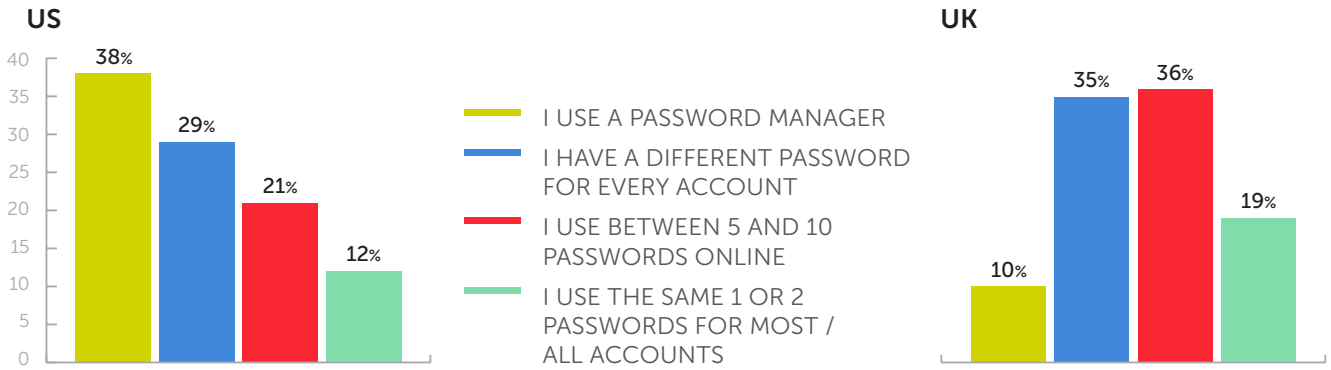
Lock, Stock, and Few Smoking Passwords

American web developer and social media entrepreneur Matt Mullenweg once said, “Love is great, but not as a password.” How right he was.

We asked our survey participants their habits with online passwords and mobile locks. Though there were some bright spots (more people than we expected said they are using a password manager, for example), there are still too many people using basic protections (or none at all).

How Many Passwords Do You Use for Your Online Accounts?

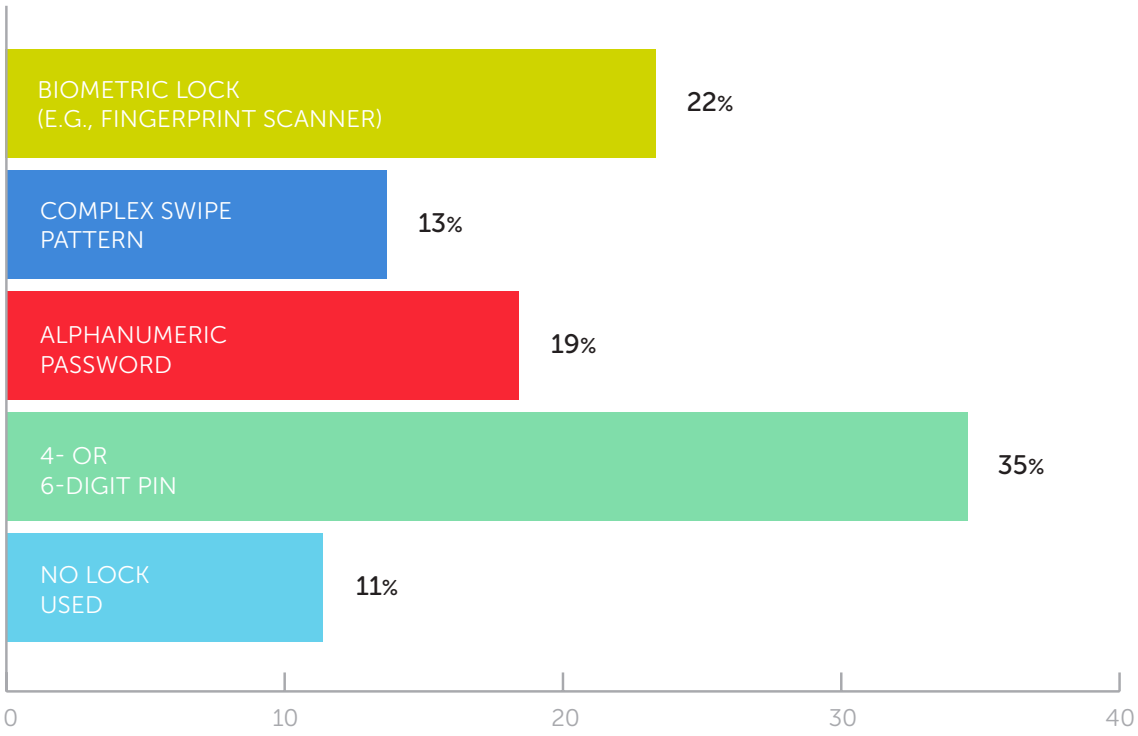
Here, we saw US employees edging out their UK counterparts on password security, with nearly four times as many US participants saying they use a password manager. In contrast, UK employees are much more likely to use fewer passwords and fall into the trap of password reuse. (Note: We asked respondents to choose the answer that best matched their approach.)



What Primary Security Lock Do You Use on Your Mobile Devices?

There was a fair amount of consistency globally with regard to use of mobile device protections — though UK employees were more likely to leave their smartphones and tablets totally unprotected.

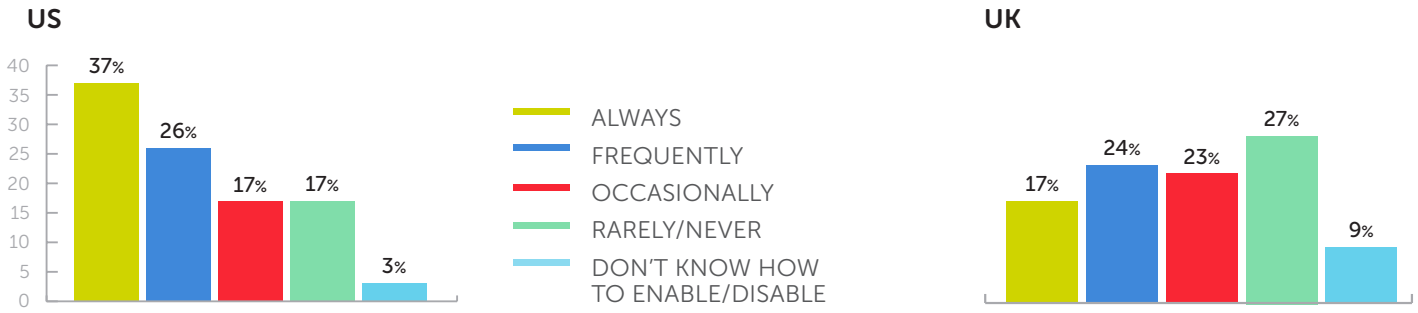
GLOBAL AVERAGES



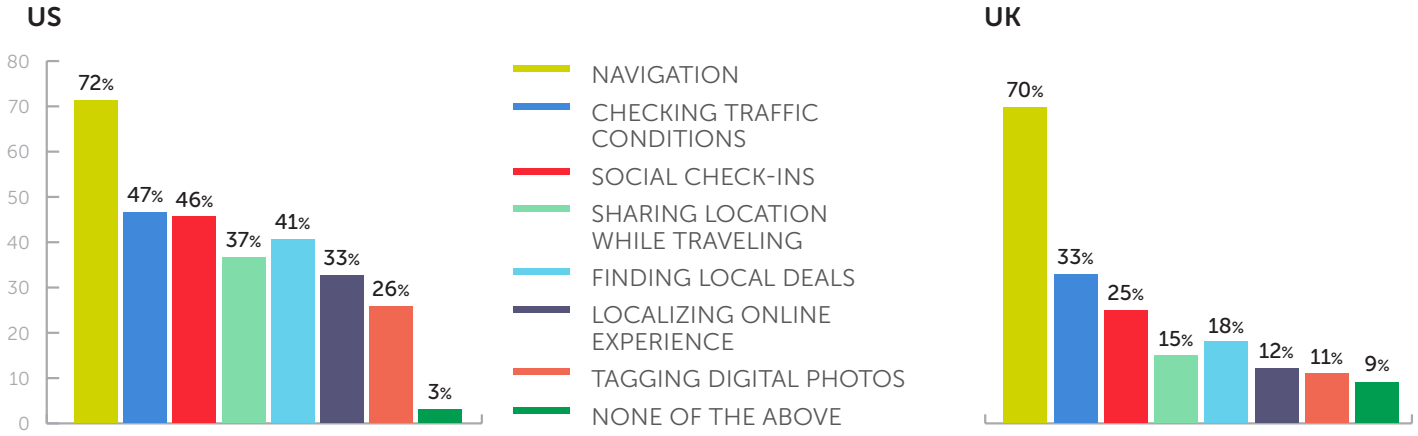
Author and educator Newton Lee said, “As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace.” Here’s how employees are doing with some of these responsibilities.

Location Tracking and Sharing

How Often Do You Enable Location Tracking on Your Mobile Device?



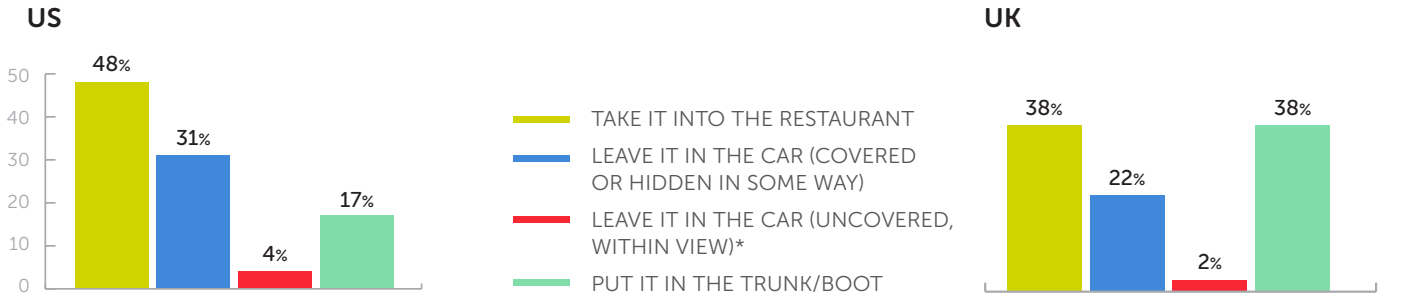
How Do You Use Location Tracking? *(Multiple responses permitted)*



Riding in Cars With Electronics

We were curious to know how employees physically manage their devices while on the road. We asked what they would be most likely to do with a laptop if they drove to meet a friend or colleague for dinner. There was again a significant difference in behaviors between US and UK respondents.

What Would You Do With Your Laptop?



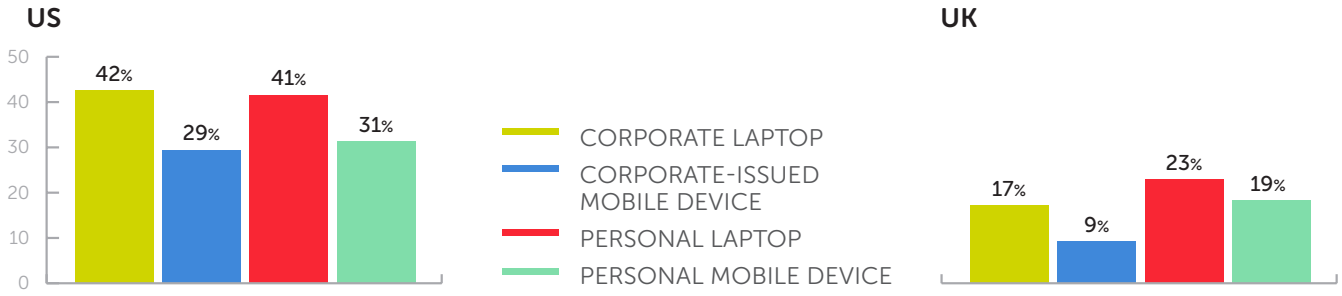
** Yes, respondents actually admitted to this*

Use (and Non-Use) of VPNs

Given that virtual private networks (VPNs) have gained a lot of traction in both the corporate and consumer sectors, we were surprised to see the significant differences between US and UK adoption rates. But we were even more surprised by the number of employees who either do not know about this technology or are actively choosing not to use it.

Have You Installed a VPN?

Where Have You Installed a VPN? *(Multiple responses permitted)*

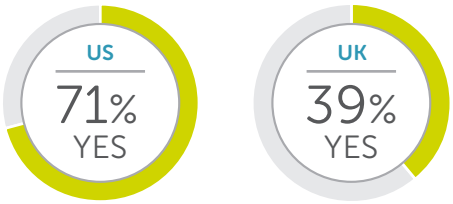


How Often Do You Use Your VPN?

Misuse of Corporate Devices

Ernest Hemingway famously said, “The best way to find out if you can trust somebody is to trust them.” Clearly, organizations show a measure of trust when they provide devices like laptops and smartphones for their employees to use inside and outside the office. **Is that trust misplaced?**

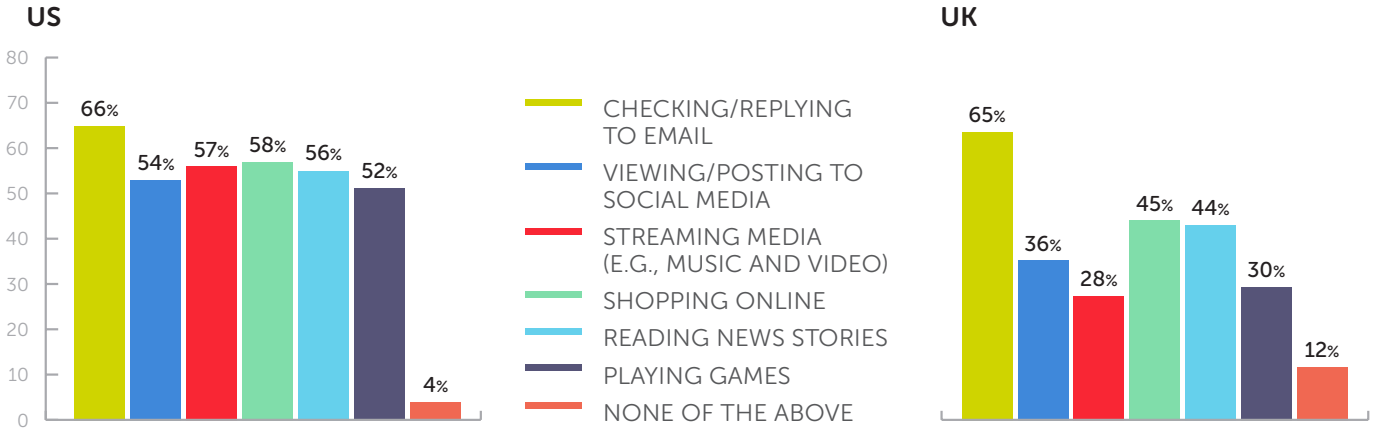
Do You Have a Corporate Laptop or Smartphone That You Regularly Use at Home?



The fact that the US outpaced the UK nearly 2-to-1 is interesting, though not surprising to us given that a survey completed for our *2017 State of the Phish* report showed that UK employees were far less likely that their US counterparts to blur the lines between work and personal activities.

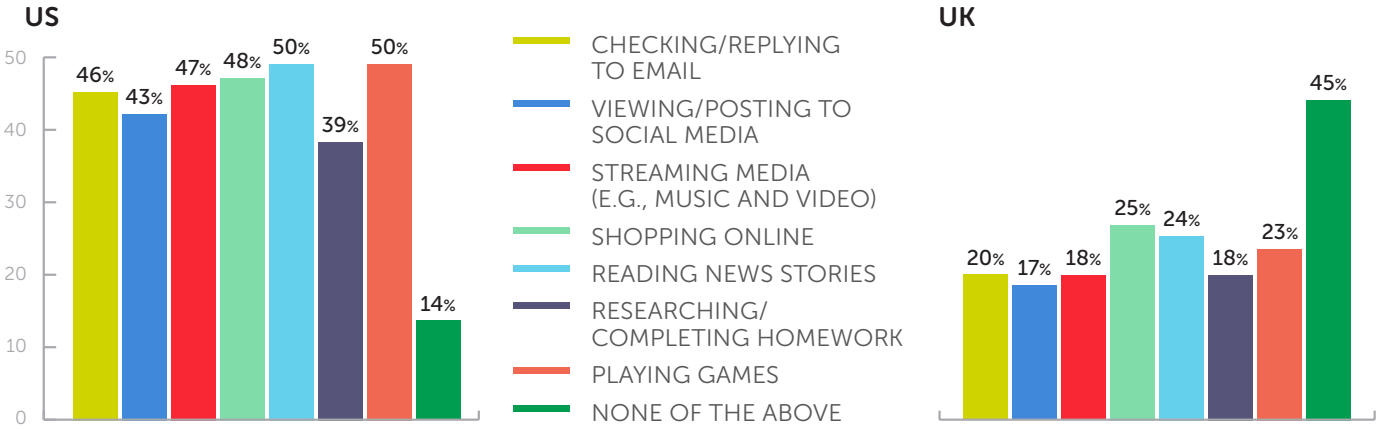
What Personal Activities Do You Perform on Your Corporate Device? *(Multiple responses permitted)*

We asked those who do regularly use corporate-issued devices outside the office to identify the types of personal activities they do on those devices. Though there are some similarities, UK employees are again less likely to mix business and pleasure.



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.



IN CONCLUSION

Author James Nathan Miller said, “The only exercise I excel at is jumping to conclusions.” We certainly didn’t break a sweat drawing this very clear conclusion based on the results of our User Risk Survey: **there is still much work to be done on the security awareness training front.**

Sure…it’s probable that, in the wake of the WannaCry attack, employees’ recognition of what ransomware is has increased. But it took a major global event to create that probability. Regardless, greater awareness of ransomware — or any cybersecurity threat — is not the same as knowing how to avoid that threat.

To drive true and lasting behavior change, employee education programs must include regular delivery of both awareness *and* training activities. When organizations consider the implications of end-user-driven risks, they should also consider the opportunities to mitigate these risks and create a workforce that has the knowledge to make informed choices and has the ability to be part of the solution rather than part of the problem.

READ OUR OTHER RESEARCH

Visit our website at **wombatsecurity.com/research** to download our other studies and reports, including the following:

The ***2017 State of the Phish Report*** compiles data from tens of millions of simulated phishing attacks sent through our Security Education platform over a 12-month period, as well as multiple surveys. It includes direct feedback from infosec professionals on the latest phishing exploits and vulnerabilities in their organizations; information about the most devastating types of phishing emails; and insights into different industries and how they are performing on different types of simulated phishing attacks.

The ***2016 Beyond the Phish Report*** compiles data from nearly 20 million questions asked and answered inside our Security Education Platform over a two-year span, as well results of an extensive survey of our database of information security professionals. It reveals how real end users are performing on security topics beyond the phish and the importance of a complete and measurable security and awareness training program that assesses end users beyond the phish.

The ***State of Security Education: Healthcare*** takes a deeper look at the healthcare-specific data we collected for our *State of the Phish* and *Beyond the Phish* reports and examines how end users in the healthcare space are performing on cybersecurity knowledge assessments about a variety of topics, including: protecting confidential information (PHI, PII); identifying phishing threats; physical risks; and data protection and disposal.

Change Behavior. Reduce Risk.

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