STATE OF THE PHISH™ 2018

wombat®
security technologies

Introduction

Our fourth annual **State of the Phish™ Report** presents analysis of data from **tens of millions of simulated phishing attacks** sent through our Security Education Platform over a 12-month period. You will see data related to:

16+ industries

Our phishing campaign data is representative of **thousands of customers**, from mid-market to large enterprise, in more than 16 industries around the globe.

10,000+ responses from infosec professionals

The results from **quarterly surveys** of our database of infosec professionals reveal what organizations are experiencing, and how they are handling the phishing threat. Responses were received from customers and non-customers alike.

3,000+ computer user insights

We conducted a third-party survey of **more than 3,000 technology users** — 1,000+ adults each in the US, UK, and Germany — to gain a global perspective of end-user awareness levels.

A Study in Four Parts

We've structured this year's report a bit differently in an effort to better capture and deliver the types of data infosec professionals are seeking as they develop their own security awareness training programs. These insights can help CISOs, CSOs, and their teams identify opportunities to more effectively manage end-user risk within their organizations.

The 2018 State of the Phish Report is a study in four parts:

Business Intelligence

In this section, we explore the **simulated phishing data** generated within our learning management system between **October 1, 2016**, and **September 30, 2017**. We also highlight the results gathered from more than 10,000 responses submitted during the **quarterly surveys** sent to our database of infosec professionals. Key topics covered in this section include:

- Frequency of phishing attacks
- Vulnerabilities revealed by phishing assessments
- How phishing is impacting organizations
- What steps organizations are taking to mitigate risk

Influential Factors

In this section, we explore how factors like **program maturity, email personalization**, and **days of the week** influence click rates and end-user reporting frequency. We also examine **simulated phishing failure rates by industry**, and how different industries compare within our most-used template categories. As well, we present responses from our infosec survey about **consequence models for repeat offenders** (people who fall for a simulated attack more than once).

A Tale of Two Regions

Looming regulations in the UK and the rest of the European Union have made data privacy and protections a front-page story. But we wondered if this heightened consciousness is translating into a greater focus on cybersecurity education.
To find out, we parsed our quarterly survey data in order to compare **US and UK infosec professionals' perceptions** of the phishing threat and the **different approaches** to security awareness training in these regions.

End Users and Emerging Threats

Here, we reveal the results of our **third-party survey of 3,000 end users** — 1,000 each in the US, UK, and Germany — which reflect awareness and knowledge levels related to **phishing and ransomware**. We also highlight data related to **smishing (SMS/text message phishing)** and the potential ramifications of an uneducated workforce with regard to this emerging threat.

Business Intelligence

In addition to the data gathered from our Security Education Platform — which reveals end-user vulnerabilities — we surveyed our database of infosec professionals to determine the trends they are seeing in their organizations and the efforts they are undertaking to protect against the ever-dangerous phishing threat.

Compared to prior years, which highlighted responses from a one-time survey, this year's quarterly surveys gave us better insight into the ongoing nature of security teams' battles against social engineering attacks.

How Often Are Organizations Experiencing Phishing?

The Anti-Phishing Working Group's *Phishing Trends Report* for the first half of 2017 showed an uptick in overall volume in comparison to the second half of 2016, though levels remained far below the historic numbers seen in early 2016. Monthly volumes held relatively steady from January through June of 2017, with statistics indicating a tendency for cybercriminals to be more strategic about the brands and industries targeted.

(Source: http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf)

The results from our quarterly 2017 surveys echo the APWG's findings, with nearly all infosec professionals reporting a steady or higher volume of attacks than in 2016.

76% said they experienced phishing attacks in 2017, which held steady from 2016.

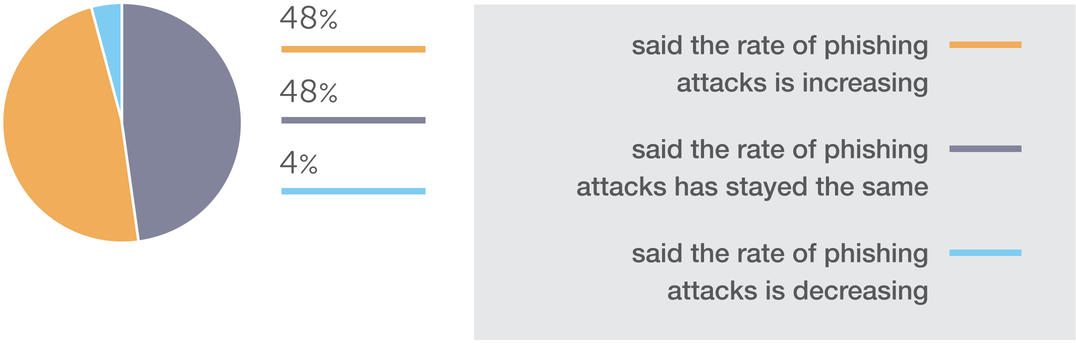
The most active quarter for the US was Q1, in which 81% of organizations said they experienced a phishing attack. In the UK, Q3 was the most active, with 75% reporting phishing.

45% experienced phishing via phone calls (vishing) and SMS/text messaging (smishing).

A 2% increase from 2016

3% experienced a USB-based social engineering attack.

A 25% decrease from 2016



When it comes to targeted spear phishing — which includes damaging business email compromise (BEC) attacks — the good news is that, on average, fewer companies said they experienced this form of social engineering in 2017. The bad news, however, is that many organizations are experiencing a high number of these attacks each quarter.

On average,

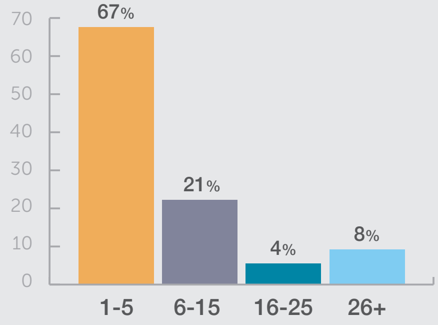
53%

of infosec professionals reported experiencing spear phishing in 2017.

A 13% decrease from 2016

Frequency of Spear Phishing Attacks per Quarter

Of those organizations that experienced spear phishing, the following are the average number of attacks they received per quarter.

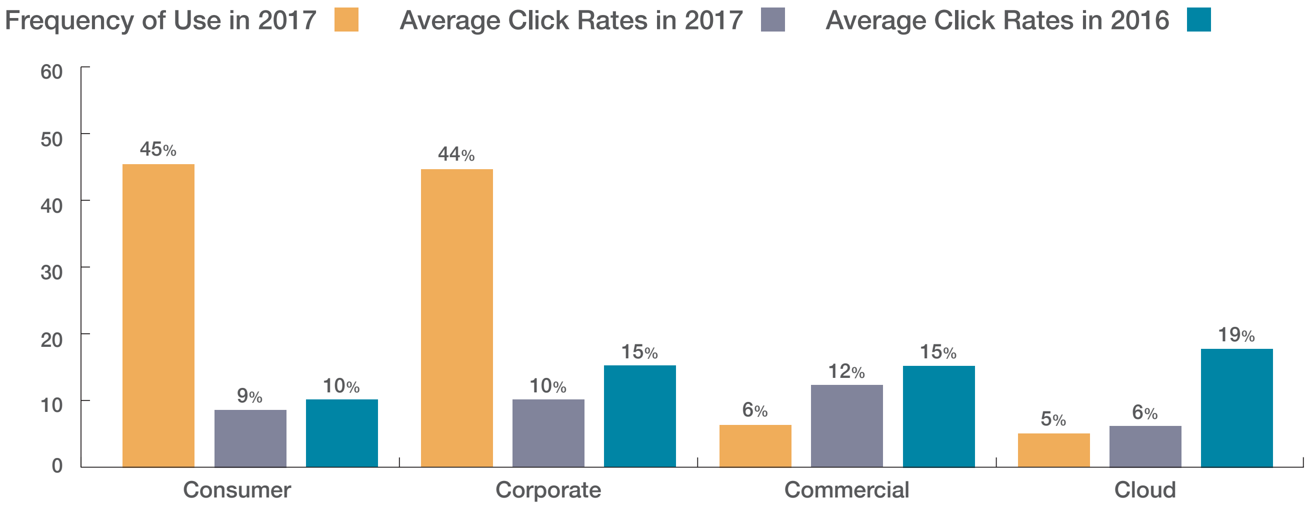


What Types of Phishing Emails Are People Falling For?

In 2017, our customers gravitated toward the same types of email templates they'd used in years past to assess their end users' vulnerabilities. We did, however, see a marked increase in the number of Consumer-themed phishing tests, which displaced Corporate-style phishing simulations as the most popular category.

The great news is that **average click rates fell across all four categories** this year in comparison to 2016. We saw a significant improvement in click rates on Cloud-based templates, which indicates that organizations are doing a good job at making users aware of these types of attacks. But organizations should consider including **more Commercial-style phishing tests** in their assessment mix in the future, given that these messages tend to fool users most often.

9% average click rate across all simulated attacks



Types of Simulated Phishing Templates

Corporate Emails

These types of emails look like official corporate communications. Examples include full mailbox notifications, spam quarantines, benefits enrollment messages, invoices, and confidential HR documents.

Cloud Emails

Examples of these business-related emails include messages about downloading documents from cloud storage services, or going to an online file-sharing service to create or edit a document.

Commercial Emails

These are business-related emails that are not organization-specific. Sample topics include shipping confirmations and wire transfer requests.

Consumer Emails

These are the types of emails the general public gets on a daily basis that may try to replicate offers or accounts they already have. Examples include emails about frequent flyer accounts, bonus miles, photo tagging, frozen accounts, big-box store memberships, social networking, gift card notifications, and more.

Most ‘Successful’ Phishing Templates

Though click rates have come down on average, the war against phishing is most certainly still on. To that end, we took a look at the **templates that garnered the most interactions** from users in 2017. We wanted to share these alarmingly high failure rates in order to help infosec teams better understand the topics and themes that are most tempting to end users. *(Note: Click rates presented are based on templates sent to a minimum of 1,500 users.)*

86%
Online Shopping
Security Updates

86%
Corporate Voicemail
from Unknown Caller

89%
Corporate Email
Improvements

In addition, two simulated phishing templates had a **near 100% click rate**: one that masqueraded as a **database password reset alert**, and another that claimed to include an **updated building evacuation plan**.

Software Vulnerabilities

Our ThreatSim® Phishing Simulations tool is able to fingerprint users’ browsers and plug-ins when they fall for a simulated phish. Because outdated software can compound the risk associated with phishing attacks, it’s important for organizations to have insight into these types of vulnerabilities on their networks.

While Adobe PDF and Microsoft Silverlight vulnerabilities moved in the right direction this year, two of the more notorious plug-ins — Java and Adobe Flash — jumped up in 2017. This could simply be due to a diverted focus. Java and Flash have been hot topics in the past, but with ransomware taking advantage of other past-due software updates last year, infosec teams no doubt felt they had bigger fish to fry on the patching front.

Adobe PDF
outdated
22%
of the time
29% reduction from 2016

Adobe Flash
outdated
21%
of the time
75% increase from 2016

Java
outdated
12%
of the time
50% increase from 2016

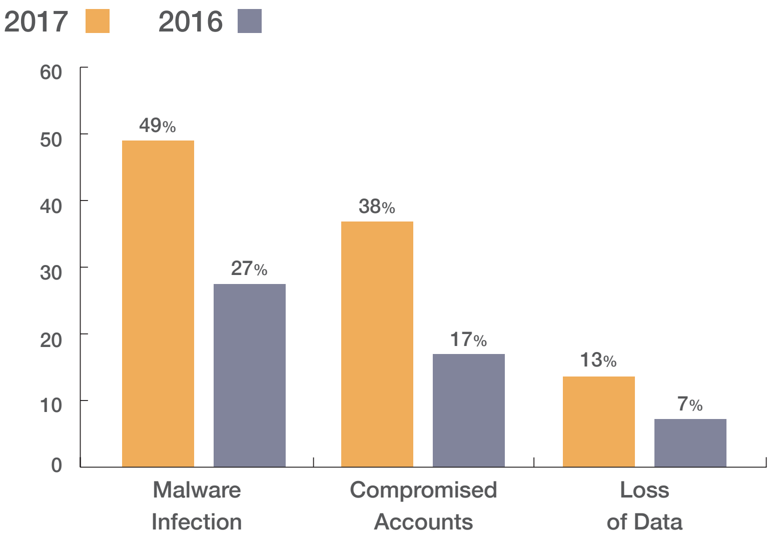
Microsoft Silverlight
outdated
9%
of the time
47% reduction from 2016

What Impact Is Phishing Having on Organizations?

As every organization knows, phishing is not a nebulous notion — it has real consequences and real impacts. And though phishing may start with end users, it certainly doesn't end there.

This year, impacts related to phishing attacks were either far more noticeable, or infosec professionals were more forthcoming than they were in 2016. *(Note: Multiple answers were permitted.)*

What phishing impacts have you experienced?

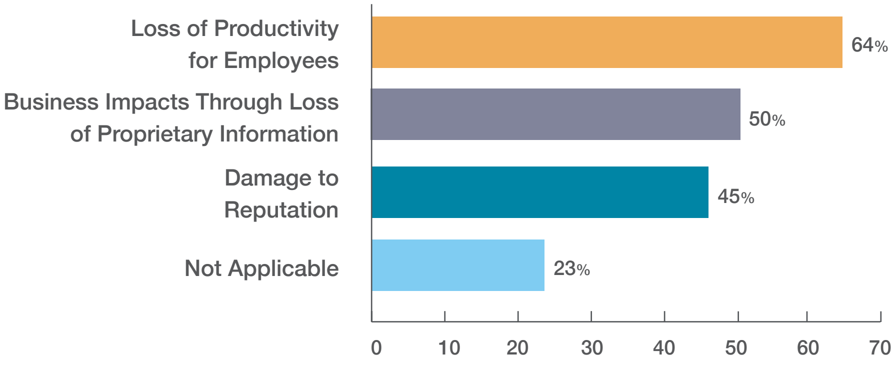


We also offered **"Other"** as an option on this question, with a request to specify. **More than 30% of respondents** chose this option; the most common impacts noted included the following:

- Loss of time
- Loss of money
- Business disruption
- Greater burden on IT/increased helpdesk calls

In addition to identifying the impacts they've experienced, we asked our contacts to identify the ways in which they **measure the cost of phishing incidents,** as well as the **technologies they are using** to reduce phishing risk within their organizations. *(Note: Multiple answers were permitted.)*

How do you measure the cost of phishing?



What technical safeguards are you using?

97% Email/Spam Filters

47% Advanced Malware Analysis

44% Outbound Proxy Protection

31% URL Wrapping

What Are Organizations Doing to Change Behavior and Reduce Risk?

Change Behavior. Reduce Risk. This is our tagline for a reason; our mission is to help organizations focus on end-user risk management and provide the tools needed to improve employee knowledge. Ongoing attention to cybersecurity education leads to fewer risky behaviors in the workplace (and beyond).

We were thrilled to see continued **upward trends in intelligence gathering** within the sphere of end-user security awareness training. It is our firm belief that organizations cannot effectively change those things which they cannot measure, which is why it's critical that infosec teams opt for tools that allow them to determine baseline measurements that can be used to gauge progress as programs continue.

It's also refreshing to see the **majority of organizations opting for monthly and quarterly training cycles** rather than relying on once-a-year activities to get the job done — the benefits of which are echoed in the reduced click rates we noted earlier.

	2014	2015	2016	2017
Do you measure your organization's susceptibility to phishing?	61% YES	63% YES	66% YES	76% YES
Do you train end users on how to identify and avoid phishing attacks?	86% YES	92% YES	92% YES	95% YES

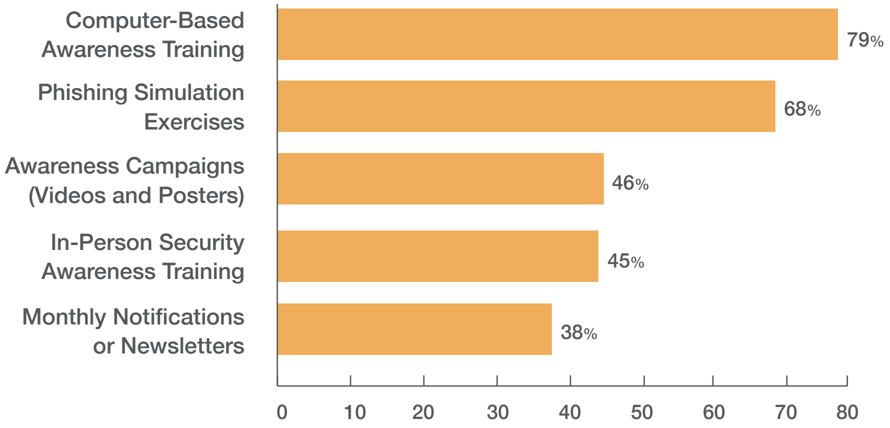
54%

of infosec professionals surveyed said they have been able to quantify a reduction in phishing susceptibility based on their training activities.

A 4% increase from 2016

Which tools do you use to train your users?

We saw a big rise in organizations using computer-based training this year, **up from 62% in 2016**. *(Note: Multiple answers were permitted.)*



How often do you use these tools?

5% Biweekly

35% Monthly

40% Quarterly

19% Yearly

Evaluating Risk Beyond the Phish

More than two-thirds — 69% — of our surveyed infosec professionals said that they assess the risk each end user poses to their organization. As our *2017 Beyond the Phish™ Report* showed, risky behaviors extend far beyond email inboxes. To that end, we asked respondents to identify the criteria they are using to determine the risk end users pose to their organizations.

78% Security Awareness and Training Performance

50% Business Risk Assessment

40% Technical Policy Violations

31% Administrative Policy Violations

Influential Factors

Our experience has shown that factors such as **program maturity, email personalization,** and even **days of the week** can influence simulated phishing click rates and end users' likelihood to report suspicious messages. In addition, our data shows that **failure rates can vary significantly by industry,** and that industries perform differently across different template categories.

In this section, we explore those factors as well as the **'carrot vs. stick'** dilemma, which has been increasingly debated within today's modern workplace.

Program Maturity

It stands to reason that, as a security awareness program becomes more mature, click rates will decrease. And our data bears that out, showing a **30% improvement in average click rates between year one and year two**.

You might find yourself tempted by a "set it and forget it" security awareness training program. Be cautious of taking a hands-off approach to employee education. When you plan and schedule your phishing tests months (or even years) in advance, you lose the ability to be responsive to emerging threats and to tailor activities based on your results.

Workforces change over time.

Employees come and go — and change roles — with regularity, so cybersecurity awareness training needs to be an ongoing effort.

Threats change over time.

Take ransomware, for example, which was a vastly different consideration two years ago than it is today. Taking a step back on cybersecurity education is only going to give attackers a leg up.

Awareness isn't the same as knowledge.

Phishing tests are a great way to assess susceptibility levels and raise awareness about social engineering — but they shouldn't be confused with training. Just knowing a threat exists isn't the same as knowing how to recognize and respond to a threat when it presents itself. In-depth education about phishing prevention is needed to create lasting behavior change.

Knowledge is not a constant.

We've likely all heard the phrase, "use it or lose it." When it comes to cybersecurity, best practices must be regularly reinforced, and end users must be able to practice what they've learned to keep their skills sharp.

Beware the Pitfalls of 'Set It and Forget It' Programs

You might find yourself tempted by a "set it and forget it" security awareness training program. Be cautious of taking a hands-off approach to employee education. When you plan and schedule your phishing tests months (or even years) in advance, you lose the ability to be responsive to emerging threats and to tailor activities based on your results.

Email Personalization

Based on the effectiveness of targeted spear phishing campaigns, it is reasonable to assume that the more personal an email seems, the more likely it is to trigger a response. Our ThreatSim tool supports personalization, and we looked in aggregate at the customization around spoofing of email addresses, and the addition of name fields within emails themselves.

What are the click rates on personalized phishing tests?

10%	10%	9%
Personalized Email Address	Custom First Name	Custom Last Name

Interestingly, the click rates don't vary significantly from the 9% average failure rate across all campaigns. This could be an indication that organizations are doing a good job at communicating to their end users that personalized fields are not an automatic indication that an email is to be trusted.

It is worth noting, however, that program administrators incorporated personalization on just 40% of campaigns sent through our system. We recommend that organizations **consider testing this factor more frequently and thoroughly** on their end-user populations.

Email Reporting

Our PhishAlarm® email client plug-in extends phishing prevention to desktop and mobile devices, allowing end users to quickly and easily report suspicious email messages. During the 12 months of this year's data tracking, end users reported **nearly 2,000,000 emails** to their infosec teams, and **nearly 60%** of those were classified by our system as potential phishing messages.

We took a look at the days of the week that users are most likely to report suspicious emails. As in 2016, reports drop off significantly on Fridays, and they occur infrequently on weekend days.

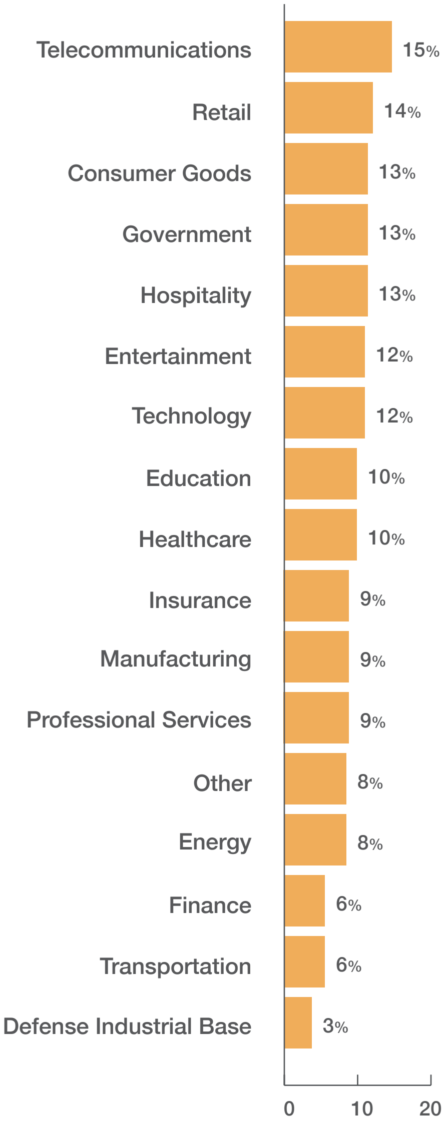
When are suspicious emails reported?

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
2%	19%	21%	22%	21%	14%	1%

Industry Comparisons

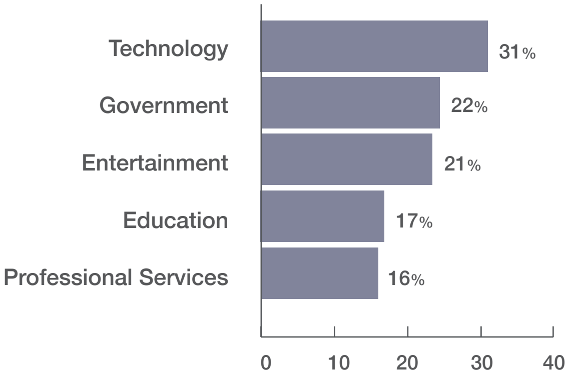
Below, we present the average click rate on phishing tests (across all template types) for each industry. We also examine how different industries performed on our top three template types (Consumer, Corporate, and Commercial). The industries highlighted in each category represent those that **performed the worst in comparison to average click rates** across all industries.

Average Click Rates by Industry

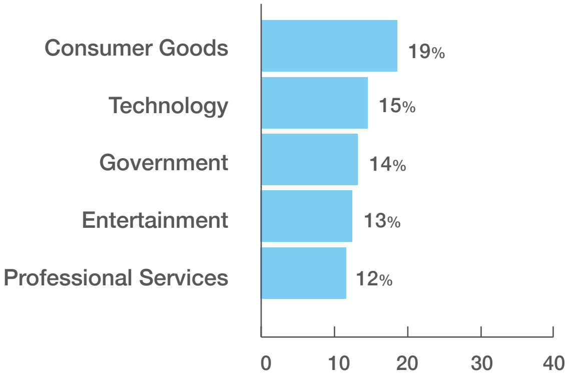


Worst Performing Industries by Template Type

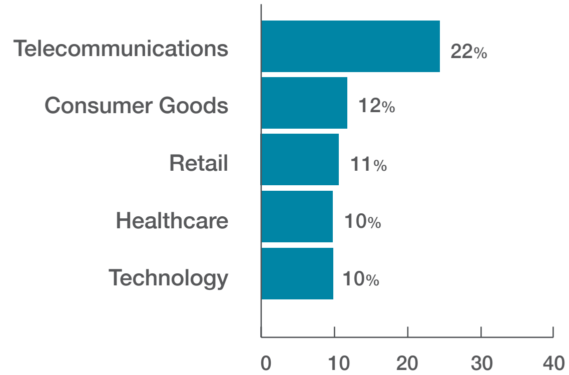
Commercial Click Rates (12% average)



Corporate Click Rates (10% average)



Consumer Click Rates (9% average)



Consequence Models

45%

of organizations said there are ramifications if their users continue to click on simulated phishing attacks.

What types of consequences are enforced in your organization?

We asked infosec professionals about the types of consequences (if any) they have in place to incentivize employees to **avoid becoming 'repeat offenders.'** *(Note: Multiple answers were permitted.)*

74% Counseling from Manager	**25%** Removal of Access to Systems
11% Termination	**5%** Monetary Penalty

We also offered "Other" as an option on this question, with a request to specify. **More than 30%** of respondents chose this option; the most common consequences noted included the following:

- Additional computer-based training
- Counseling from the IT department
- One-on-one training from the IT department
- Entry into the organization's formal discipline process

Looking for More About Consequence Models?

View the 'Risky Business' SecureWorld webinar replay and Wombat Security blog for additional insights about this topic.

A Tale of Two Regions

As a global organization, we have witnessed firsthand the differences between US and UK approaches to end-user risk management. This year, we parsed our quarterly survey data in order to compare **US and UK infosec professionals' perceptions** of the phishing threat and the **different tactics** applied to security awareness and training in these regions.

Organizations That Experienced Spear Phishing in 2017

US	UK
57%	36%

Organizations That Experienced Data Loss as a Result of Phishing in 2017

US	UK
14%	5%

It's possible organizations in the US and UK alike are reluctant to admit to data loss — particularly those in the UK, given the requirements set forth in the looming General Data Protection Regulation (GDPR).

Organizations That Assess Susceptibility to Phishing Attacks

US	UK
86%	53%

What tools do you use to train end users to recognize and avoid phishing attacks?

	US	UK
In-Person Security Awareness Training	41%	58%
Computer-Based Online Security Awareness Training	88%	58%
Awareness Campaigns: Videos and Posters	44%	60%
Monthly Notifications/Newsletters	35%	55%
Simulated Phishing Attacks	79%	45%

How often do you use these tools?

	US	UK
Biweekly	5%	6%
Monthly	41%	15%
Quarterly	40%	44%
Yearly	14%	35%

Have you been able to quantify a reduction in phishing susceptibility based on these activities?

	US	UK
YES »	61%	28%

UK organizations generally opt for more passive training methods over hands-on practice for their users, and are far more likely than their US counterparts to rely on once-a-year training to keep employees informed about cybersecurity. Given that, it's not surprising that they are less likely to see quantifiable results from their efforts.

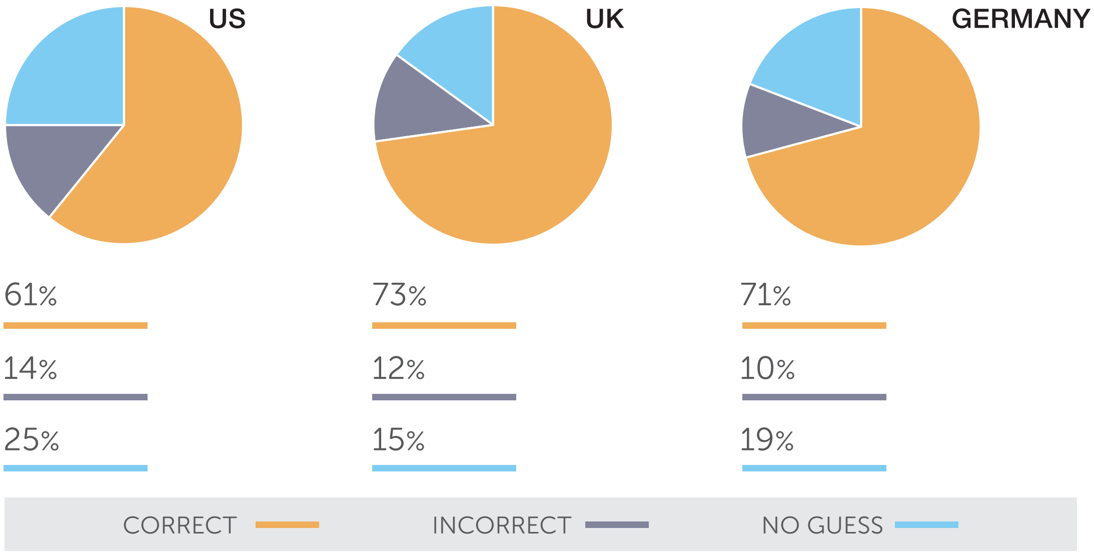
End Users and Emerging Threats

What Do Working-Age Adults Know About Phishing and Ransomware?

Following, you will find the results of our **third-party survey of 3,000 technology users** — 1,000 each in the US, UK, and Germany — in which we asked working-age adults questions related to **phishing and ransomware.** *(Note: When results were similar across regions, we calculated an average percentage.)*

What is phishing?

We unfortunately saw US end users lagging behind their UK and German counterparts on this question, but UK respondents have shown an improvement since the survey we completed for our *2017 User Risk Report* (see the sidebar on the next page).



Phishing Awareness: Millennials vs. Baby Boomers

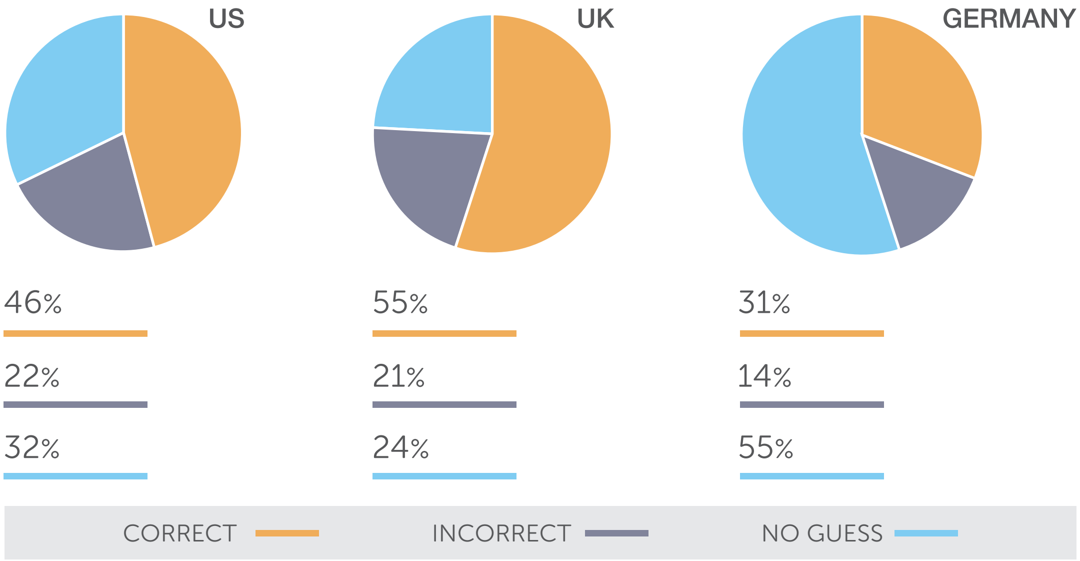
Interestingly, across all populations, adults aged 55 and older significantly outpaced millennials in their recognition of what phishing is:

55+	18-29
72% Correct	61% Correct

FACT:
Only 52% of US respondents between ages 18 and 29 answered this question correctly.

What is ransomware?

We found German respondents far less likely to know what ransomware is in comparison to adults in the US and the UK. The good news is that we saw significant improvements in awareness among US and UK respondents in comparison to mid-2017 *(see sidebar)*.



Flashback to the
2017 User Risk Report

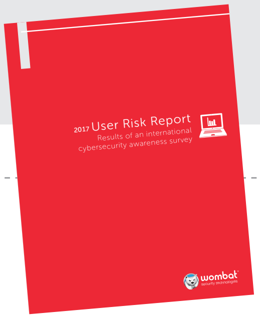
In May 2017, we conducted an international survey of 1,000 US and 1,000 UK working adults for our *User Risk Report*.

What is phishing?
(global average)

Correct	70%
Incorrect	17%
No Guess	13%

What is ransomware?

	US	UK
Correct	37%	42%
Incorrect	42%	19%
No Guess	21%	39%



Smishing: An Attack Vector to Watch for in 2018

Smishing (SMS/text message phishing) has generally been considered a regional, consumer-based threat as opposed to a global cybersecurity concern. However, media coverage of successful smishing attacks rose during 2017 — a trend that's sure to increase in 2018 given that awareness of this threat vector is low among US, UK, and German adults:

What is smishing? (global average)

16%	17%	67%
Right	Wrong	No Guess

Though our customers are assessing their users far less frequently on smishing than they are on phishing, data gathered from thousands of simulated attacks sent through our ThreatSim Smishing Simulations tool shows that, on average, failure rates are the same for both of these attack vectors.

9%	9%
average click rate for smishing tests	average click rate for phishing tests

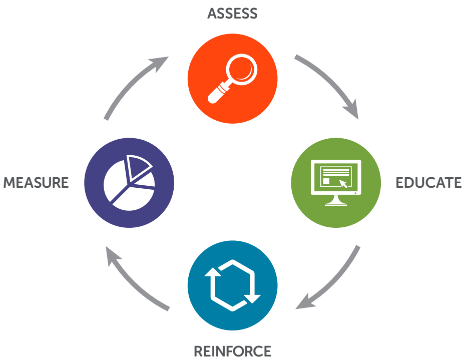
As more and more employees use smartphones to connect to corporate systems and data, the potential ramifications of an uneducated workforce should not be ignored.

Notes:

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. 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 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.



wombat security technologies

Change Behavior. Reduce Risk.

Contact Us: wombatsecurity.com | info@wombatsecurity.com | +1 (412) 621 1484 | UK +44 (20) 3807 3472