

STATE OF THE ~~2017~~ PHISH

to try to obtain financial or other confidential information from internet users, typically by sending an email that looks as if it is from a legitimate organization, encouraging an end user to take an action that compromises their computer or reveals sensitive information.



wombat[®]
security technologies

Introduction and Overview

Welcome to the third annual State of the Phish Report. This year's report not only looks at data around tens of millions of simulated phishing emails sent last year, but survey data from both infosec professionals and end users to gain a better idea of what the impact and understanding of phishing was in 2016 as we move into 2017. While not a scientific study, this report does offer important insights into what proactive organizations are doing to better train their end users to identify and avoid phishing messages.



Data Analyzed for This Report:

10s of millions of simulated phishing emails sent over a **12-month period** from **October 1, 2015 to September 30, 2016**.

155% increase

A **155% increase** over the number of emails that we looked at for our last report

500+ answers

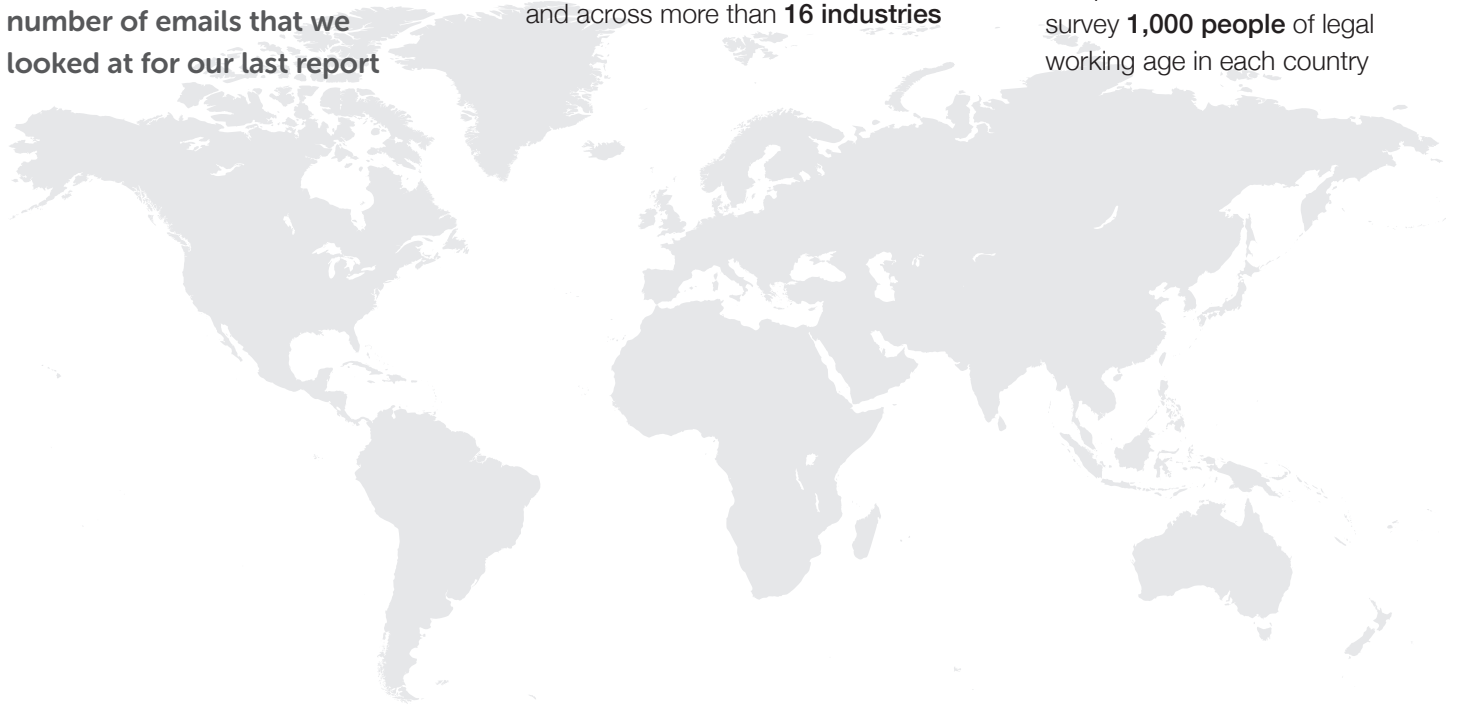
More than **500 answers** to a survey that we launched to security professionals in our database

Responses were from companies all around the world, of all sizes, and across more than **16 industries**

2,000+ answers

More than **2,000 answers** from end users in the US and UK on their knowledge of phishing

We worked with an independent research firm to survey **1,000 people** of legal working age in each country



Summary of Findings

This year's report shows some positive trends. Organizations that are working to raise awareness and change behavior are seeing results. From 2015 to 2016, there was a **64% increase** in organizations measuring the risk that end users pose — and security awareness and training is the leading way that they are doing it. We know that administrators who use measurements to strategically steer their programs see better results overall. A few other high-level findings from this year's report:

Simulated Phishing and Training Is Working

This year, we had **155% more** simulated phishing emails to look at than in our previous year's report, with good news overall. Click rates are improving for many industries and for those with mature programs. As we saw in our [Beyond the Phish](#) Report released in September 2016, some industries have more work to do than others, but with continuous programs and measurement becoming the norm, we expect to see improvement.

Phishing Attacks Appear to be Slowing

In this year's survey, **10% fewer** infosec professionals reported that their organization had been a victim of a phishing attack. Only **51%** of this same group felt phishing attacks were increasing overall (compared to **60%** in our 2016 survey). We don't believe this means that cybercriminals are going anywhere; rather, we feel it could be an indication that they are diversifying their tactics now that end users are becoming more savvy.

Awareness Is Growing, but Risky Behaviors Still Exist

Our survey of the general public revealed that more people are aware of the concept of phishing than most of us probably thought. However, these same people struggled to identify what ransomware is. These end users also showed that they put their organizations at risk by doing things like checking personal email on their work devices. Overall, this survey points to the fact that there is work to be done to teach people how to stay safe.

Phishing: Knowledge Is Power

This year, before we started looking at what infosec professionals reported back to us, we wanted to understand what the ‘man on the street’ knew about phishing. To do this, we worked with a consumer research company to ask a simple question:

	US	UK
What is phishing?	65% Answered Correctly 17% Answered Incorrectly 18% Do Not Know	72% Answered Correctly 18% Answered Incorrectly 10% Do Not Know

If knowing is half the battle, organizations can take comfort in the fact that awareness is growing. This hopefully means that people are more alert to cyber threats and the associated risks, which would make these users even better candidates for further training.

What Infosec Professionals Are Experiencing

In the third quarter of 2016, the Anti-Phishing Working Group’s *Phishing Trends Report* showed some drop in the numbers of brands targeted by phishers and also that phishers were, on average, creating fewer phishing URLs.

(Source: https://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf).

Around the same time, we surveyed our database of infosec professionals, who seemed to be reporting the same thing -- phishing is still a threat that is not necessarily growing as quickly, but is evolving:

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

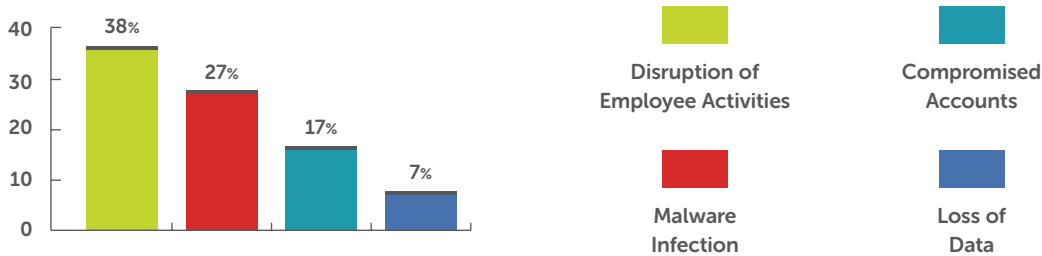
Decrease of **33%** from 2015

While attacks seem to be slowing, that does not mean that organizations should not continue to be vigilant in training their end users about security threats. The key is continuous training and reinforcement to keep security top of mind every day.

Impact of Phishing

Phishing attacks can be devastating to organizations, so we wanted to learn more about the specific impacts.

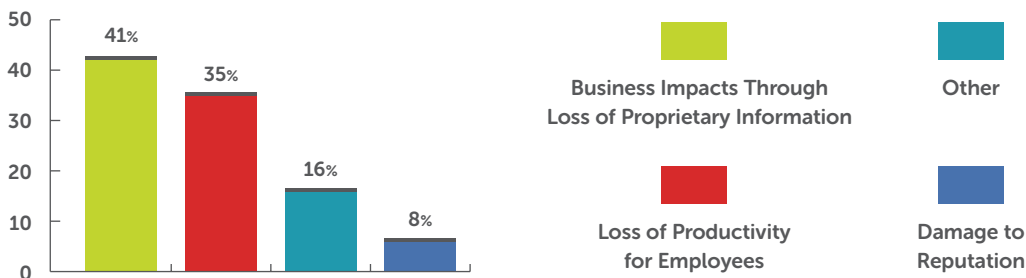
What has the impact of phishing been on your organization? (choose all that apply)



More About the Cost of Phishing

In 2015, the Ponemon Institute released the paper *The Cost of Phishing and the Value of Employee Training* which concluded that lost employee productivity is the largest cost associated with phishing (roughly **\$1.8M** for a 10,000-person company).

How do you measure the cost of phishing incidents?



Software Vulnerability

When end users' plug-ins are out of date, it increases their exposure to attack. Our ThreatSim® simulated phishing tool performs fingerprinting of users' browsers and plug-ins when they fall for a simulated phish. Organizations can use this info to pinpoint risky end users. From 2015 to 2016 the results show that our customers have gotten significantly better at patching out-of-date software. The overall volume of emails clicked was almost **three times larger** than last year, but the percentage of vulnerabilities has decreased significantly for each piece of software assessed.

Adobe PDF
outdated
31%
of the time

49% reduction
from 2015

Microsoft Silverlight
outdated
17%
of the time

37% reduction
from 2015

Adobe Flash
outdated
12%
of the time

73% reduction
from 2015

Java
outdated
8%
of the time

68% reduction
from 2015

What Is Ransomware?

To anyone in information security, asking what ransomware is seems silly. But when you acknowledge that awareness is half the battle, it becomes clear that you need to understand if your end users know what ransomware is. Once again, we worked with a consumer research firm to ask **1,000 people in the US**, and **1,000 people in the UK** of legal working age if they knew what ransomware was:


	US	UK
What is ransomware?	34% Answered Correctly 14% Answered Incorrectly 52% Do Not Know	38% Answered Correctly 21% Answered Incorrectly 41% Do Not Know

While we expected the awareness of ransomware to be lower than phishing, we were surprised how much lower this number was. In both the US and the UK, more than half of end users either answered incorrectly or declined to even venture a guess. Hopefully, their phishing awareness keeps them somewhat safe, but if they don't know what ransomware is and the risks of falling for an attack, then they probably don't know best practices such as backing up files.

Ransomware Q&A


What Is Ransomware?

Ransomware is a type of malicious software — i.e., malware — that blocks access to a device or data until a ransom is paid.



What Does Ransomware Do?

When a device is infected with ransomware, some type of encryption is applied, effectively locking you out of your files or your device. If you are infected, you will receive a ransom message from the attacker asking for payment which, allegedly, will grant you access to the digital key needed to unlock your files and/or system.




How Much Are Ransoms?

Many ransoms are small; they commonly range from \$25 to \$600. However, some ransomware strains (like those that target healthcare institutions or other larger organizations) carry significantly higher payment demands, into the thousands of dollars.

How Are Ransoms Collected?

Attackers generally require ransoms to be paid in Bitcoin or another “untraceable” electronic format. These “cryptocurrencies” are fully digital. They are created and held electronically, have no physical form, and are not controlled by any banking entity.



To download the full Ransomware infographic visit the Wombat Blog.

<https://info.wombatsecurity.com/blog/infographic-help-users-understand-ransomware-and-prevent-infections>

To Pay or Not to Pay?

With the backdrop of this end-user awareness and explosion of ransomware in 2016, we wanted to understand what infosec professionals were experiencing.

34%

said that they had experienced a ransomware attack in 2016



2%

of organizations that were hit with ransomware said they paid the ransom

This number that paid was a bit surprising as we have heard many other sources cite figures as high as two-thirds. They also indicate that during 2016 more companies became smarter about backing up files and came to the realization that there is no honor among thieves and paying doesn't necessarily mean that these extortionists will keep their word.

Ransomware Prevention and Protection

To Pay or Not to Pay?

Security experts generally advise against paying a ransom. Paying only encourages these types of attacks.

However, if an organization has not backed up files to a secure location, paying the ransom might be regarded as the only option for recovering data. Though some services claim they can recover files without the decryption key, it can be next to impossible to reverse an infection.

Will Paying a Ransom Restore My Files?

Sometimes. But there have been known instances of ransomware with critical flaws that render data unrecoverable (even if the ransom is paid). In other cases, an organization has paid the ransom only to be hit with a second, larger payment request.

Bottom Line: **DON'T COUNT ON 'HONOR AMONG THIEVES!' »**

DON'T BECOME A RANSOMWARE VICTIM!

Know how to prevent an infection and be prepared to recover your data if you do get hit.



AVOID

unknown links, ads, and websites



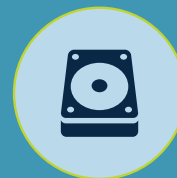
DON'T

download unverified attachments or apps



KEEP

software up to date and patch known vulnerabilities



BACK UP

data and files to a secure location daily or even hourly (if possible)

Read more on our blog: [Ransomware: Don't Count on Honor Among Thieves](#) for examples.

Spear Phishing

Spear phishing is one way that attackers are getting more targeted with their attacks. Criminals gather information on key people in an organization to craft a personalized and convincing email to encourage an end user to provide confidential information.

61%

reported experiencing
spear phishing
(aka targeted attacks)

Decrease of almost **10%**
from the previous year



Our simulated phishing tool enables administrators to craft their own spear phishing emails. Anecdotally, we have heard of customers who craft very specific spear phishing attacks for board members or executives to show the need for more robust training programs and tools. However for the purposes of this report, we looked in aggregate at the customization around spoofing email addresses, and doing things like adding first and last names to emails.

	Average Click Rates in Programs Less Than 6 Months Old	Average Click Rates in Programs After a Year
First Name Personalization	14%	10%
Last Name Personalization	13%	8%
Email Address Personalization	13%	6%

Week at a Glance: Days Suspicious Emails Are Reported

Our PhishAlarm® email reporting button allows end users to report emails that come into their email box that they feel are suspicious. Our data shows that users are more likely to recognize and report messages during the middle of the week.

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday and Sunday
18%	21%	21%	22%	16%	1% each



When do most reported emails clock in?

The early hours of the work day are when people seem to report the most suspicious emails.

Risky Behaviors

Our independent end-user survey indicates that there are significant cultural differences between employees in the US and the UK and how much they blur the lines between work and home, which can pose a large risk for organizations.

	US	UK
Do you check personal email on your work computer?	50% Answered Yes 49% Answered No 1% Not Sure	31% Answered Yes 68% Answered No 1% Not Sure
Do you check work email on your personal mobile phone?	49% Answered Yes 50% Answered No 1% Not Sure	29% Answered Yes 71% Answered No

The important takeaway here is that end users must practice safe behaviors. A filter on work email does nothing when an employee clicks a malicious link in their personal email while on a work computer or loses their personal phone with work email and information on it. That may be why we are seeing changes in the technology used to protect organizations from phishing attacks:

Which of the following technologies are utilized by your organization to reduce the risk from phishing?

94%

Email/Spam Filters

A decrease of **5%**
from last year

63%

Advanced
Malware Analysis

An increase of **26%**
over last year

48%

Outbound
Proxy Protection

A decrease of **14%**
from last year

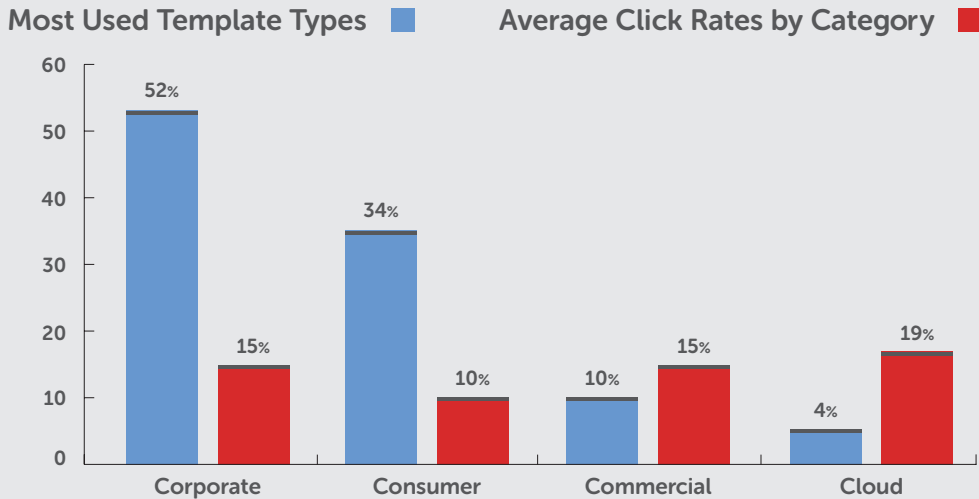
31%

URL Wrapping

An increase of **30%**
over last year

What Types of Phishing Emails Are People Falling For?

Year over year, the types of simulated phishing templates that our administrators have used remain very similar. End users seem to be more likely to click on emails that they would expect to find in their work email boxes (such as a password change notification, or shipping confirmation) and less likely to click on something consumer-related.



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 a cloud storage service, or going to an online file sharing service to create or edit a document.

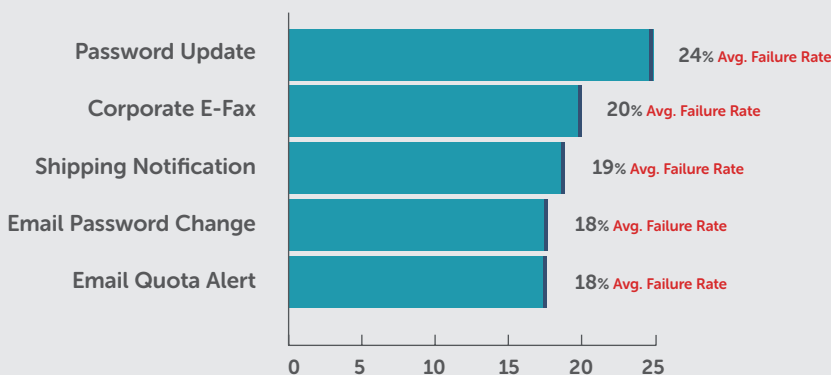
Commercial Emails

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

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 flier accounts, bonus miles, photo tagging, frozen accounts, big-box store memberships, social networking, gift card notifications, and more.

Most Popular Attack Templates

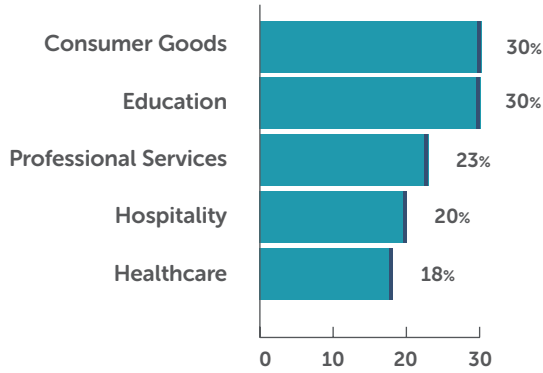


A template called “**Message from Administrator**” had the highest average click rate of **34%**. This simulated attack asks the user to click a link if they feel they have received the message in error and didn't sign up for a certain type of account.

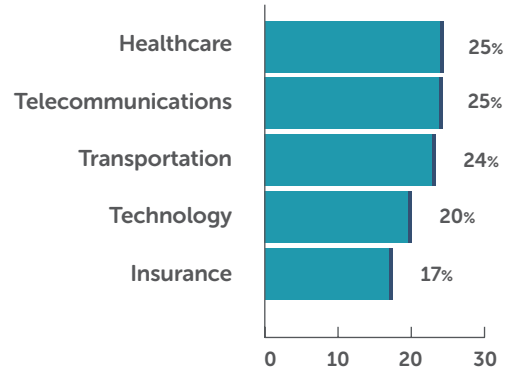
How Do Different Industries Perform?

For this section, we looked at the three most used template categories (Corporate, Consumer, and Commercial) and used our data to see which industries fell above the average click rates.

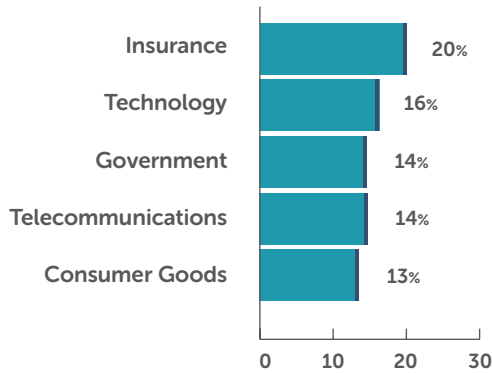
Corporate (15% average click rate)



Commercial (15% average click rate)



Consumer (10% average click rate)



What Industries Have Shown the Most Improvement Year Over Year?

More than half of the industries we looked at have improved click rates year over year, but there are a few that showed a large improvement and commitment to continuous simulated phishing programs and measurement to drive awareness:

Professional Services

47%

improvement in click rates

Technology

32%

improvement in click rates

Energy

27%

improvement in click rates

Telecommunications

26%

improvement in click rates

Finance

19%

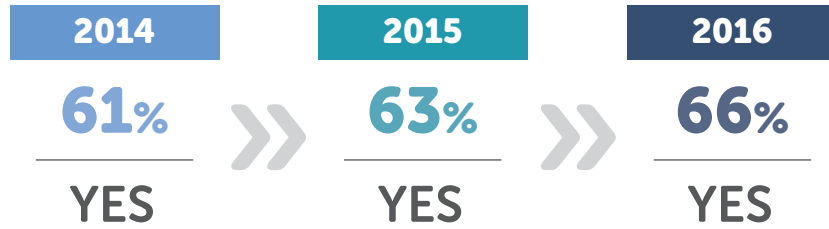
improvement in click rates

Telecommunications was the industry with the highest failure rate in our 2016 report.

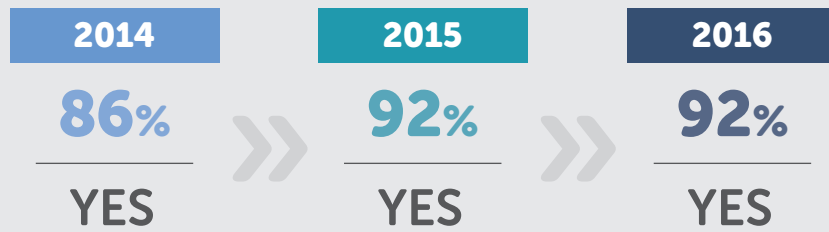
Measurement Is Key

The only way to truly understand the success of any program is to set goals and baselines from the beginning to measure against, so we were glad to see an upward trend in those who are measuring.

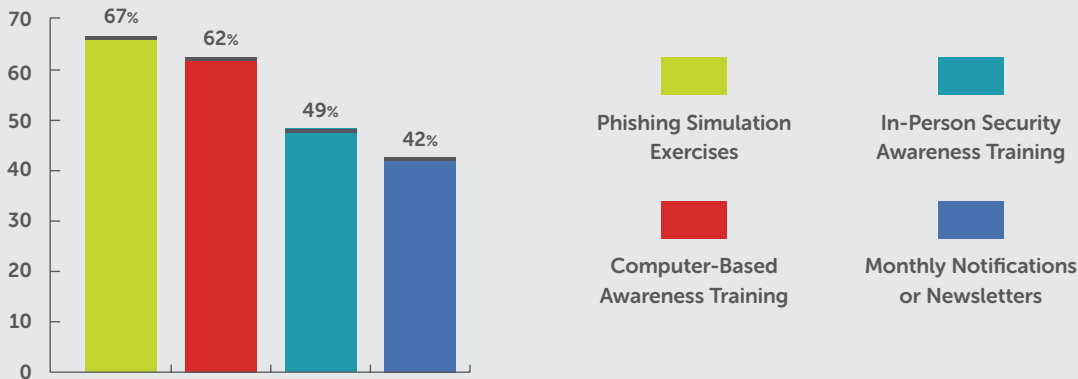
Do you measure your organization's susceptibility to phishing?



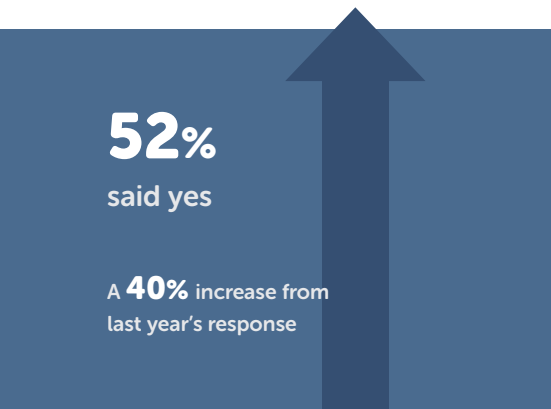
Do you train end users how to identify and avoid phishing attacks?



If yes, which of the following activities are used? (choose all that apply)



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



Change Behavior. Reduce Risk.

This happens to be our tagline, and for good reason – we believe that true behavior change through assessing and educating end users is what brings about the reduction of risk to an organization. So we once again asked the question:

Do you assess the risk each end user poses to your organization?

72% **SAID YES**

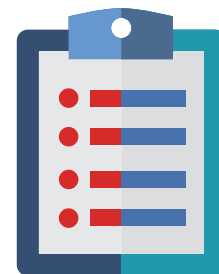
This is a dramatic increase of **64%** year over year. We know that information security professionals have to assess risk in order to make decisions on what tools to invest in. And now more than ever, infosec teams have to provide data-driven reasoning. Not surprisingly, most use security awareness to measure end-user risk.

What criteria are infosec professionals using to determine the risk end users pose?



Want to understand your risk and how a program could impact it?

The Aberdeen Group report, *The Last Mile in IT Security: Changing User Behavior* provides a Monte Carlo analysis that can help identify the level of risk reduction your organization could achieve with a security awareness program. We help our customers use the data to make a business case for implementing security education at their organizations. The model shows an average of **60% reduction** in security risk by changing end-user behaviors.





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