STATE OF THE PHISH 2018
This 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**
This 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 organisations 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.
# TABLE OF CONTENTS

**A Study in Four Parts**

- The 2018 State of the Phish Report is a Study in Four Parts: ................................................................. 4

**Business Intelligence**................................................................................................................................................. 4

- How Often Are Organisations Experiencing Phishing? ............................................................................. 4
- What Types of Phishing Emails Are People Falling For? ........................................................................... 5
- Types of Simulated Phishing Templates ................................................................................................. 6
- Software Vulnerabilities ......................................................................................................................... 6
- What Impact Is Phishing Having on Organisations? ............................................................................... 7
- What Are Organisations Doing to Change Behaviour and Reduce Risk? ............................................... 8

**Influential Factors**.................................................................................................................................................. 9

- Programme Maturity ................................................................................................................................. 9
- Email Personalisation ............................................................................................................................... 10
- Email Reporting ........................................................................................................................................ 10
- Industry Comparisons ............................................................................................................................. 11
- Consequence Models ............................................................................................................................... 12

**A Tale of Two Regions**.................................................................................................................................... 12

**End Users and Emerging Threats** ................................................................................................................. 13

- What Do Working-Age Adults Know About Phishing and Ransomware? ........................................... 13
- Smishing: An Attack Vector to Watch for in 2018 ................................................................................ 14
A STUDY IN FOUR PARTS

We’ve structured this report to clearly capture and deliver the types of data infosec professionals are seeking as they develop their own security awareness training programmes. These insights can help CISOs, CSOs and their teams identify opportunities to more effectively manage end-user risk in their organisations.

THE 2018 STATE OF THE PHISH REPORT IS A STUDY IN FOUR PARTS:

Business Intelligence

In this section, we explore simulated phishing data generated between 1st October 2016 and 30th September 2017. We also highlight the results gathered from more than 10,000 responses submitted via 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 organisations
• What steps organisations are taking to mitigate risk

Influential Factors

In this section, we explore how factors like programme maturity, email personalisation 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. What’s more, we present survey responses 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 is this heightened consciousness translating into a greater focus on cybersecurity education? To find out, we parsed quarterly survey data 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 data gathered that reveals end-user vulnerabilities, we surveyed infosec professionals to determine the trends they’re seeing in their organisations and the efforts they are undertaking to protect against the ever-dangerous phishing threat.

The results provide insight into the ongoing nature of security teams’ battles against social engineering attacks.

HOW OFTEN ARE ORGANISATIONS EXPERIENCING PHISHING?

The Anti-Phishing Working Group’s Phishing Trends Report for the first half of 2017 showed an uptick in overall volume compared 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.

The results from our quarterly 2017 surveys show nearly all infosec professionals reporting a steady or higher volume of attacks than in 2016.

<table>
<thead>
<tr>
<th>Weekly Variations</th>
<th>Yearly Variations</th>
</tr>
</thead>
<tbody>
<tr>
<td>76% experienced phishing attacks in 2017, which held steady from 2016.</td>
<td>45% experienced phishing via phone calls (vishing) and SMS/text messaging (smishing)</td>
</tr>
<tr>
<td>3% experienced a USB-based social engineering attack</td>
<td>2% increase from 2016</td>
</tr>
<tr>
<td>25% decrease from 2016</td>
<td>2% increase from 2016</td>
</tr>
</tbody>
</table>

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

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 organisations are experiencing a high number of these attacks each quarter.

**Frequency of Spear Phishing Attacks per Quarter**

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

On average, **53%** of infosec professionals reported experiencing spear phishing in 2017.

A **13% decrease** from 2016

**WHAT TYPES OF PHISHING EMAILS ARE PEOPLE FALLING FOR?**

In 2017, 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 organisations are doing a good job at making users aware of these types of attacks. But organisations 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.
TYPES OF SIMULATED PHISHING TEMPLATES

Corporate Emails
These types of emails look like official corporate communications. Examples include full mailbox notifications, spam quarantines, benefits enrolment 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 organisation-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. Sharing these alarmingly high failure rates can 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.)

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Template Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9%</td>
<td>Online shopping security updates</td>
</tr>
<tr>
<td>24%</td>
<td>Corporate voicemail from unknown caller</td>
</tr>
<tr>
<td>89%</td>
<td>Corporate email improvements</td>
</tr>
</tbody>
</table>

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 can 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 organisations 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.
WHAT IMPACT IS PHISHING HAVING ON ORGANISATIONS?
As every organisation 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?

More than 30% of respondents chose the “other” option for this question, and the most common responses included:
- Loss of time
- Loss of money
- Business disruption
- Increased helpdesk calls

In addition to identifying the impacts they’ve experienced, contacts identified the ways they measure the cost of phishing incidents, as well as the technologies they’re using to reduce phishing risk within their organisations. (Note: Multiple answers were permitted.)

How do you measure the cost of phishing?

What technical safeguards are you using?
WHAT ARE ORGANISATIONS DOING TO CHANGE BEHAVIOUR AND REDUCE RISK?

We help organisations focus on end-user risk management and provide the tools needed to improve employee knowledge. Ongoing attention to cybersecurity education leads to fewer risky behaviours in the workplace (and beyond).

There was an upward trend in intelligence gathering within the sphere of end-user security awareness training. Organisations can’t effectively change things that they can’t measure. This 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 programmes continue.

It’s also refreshing to see the majority of organisations 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.

---

**Do you measure your organisation’s susceptibility to phishing?**

<table>
<thead>
<tr>
<th>Year</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>61%</td>
<td>63%</td>
<td>66%</td>
<td>76%</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Year</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>86%</td>
<td>92%</td>
<td>92%</td>
<td>95%</td>
</tr>
</tbody>
</table>

**Which tools do you use to train your users?**

- Computer-Based Awareness Training
- Phishing Simulation Exercises
- Awareness Campaigns (video and posters)
- In-Person Security Awareness Training
- Monthly Notifications or Newsletters

We saw a big rise in organisations using computer-based training this year, up 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 surveyed infosec professionals said they assess the risk each end user poses to their organisation. As the 2017 Beyond the Phish™ Report showed, risky behaviours extend far beyond email inboxes. To that end, respondents were asked to identify the criteria they are using to determine the risk that end users pose to their organisations.

<table>
<thead>
<tr>
<th>78%</th>
<th>50%</th>
<th>40%</th>
<th>31%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security awareness and training performance</td>
<td>Business risk assessment</td>
<td>Technical policy violations</td>
<td>Administrative policy violations</td>
</tr>
</tbody>
</table>

INFLUENTIAL FACTORS

Our experience has shown that factors such as programme maturity, email personalisation 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.

PROGRAMME MATURITY

It stands to reason that, as a security awareness programme 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 programme. 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 recognise and respond to a threat when it presents itself. In-depth education about phishing prevention is needed to create lasting behaviour 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’ PROGRAMMES

You might find yourself tempted by a “set it and forget it” security awareness training programme. 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 PERSONALISATION**

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 personalisation, and we looked in aggregate at the customisation around spoofing of email addresses and the addition of name fields within emails themselves.

![Click rates on personalised phishing tests](image)

What are the click rates on personalised phishing tests?

- **10%** Personalised email address
- **10%** Custom first name
- **9%** 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 organisations are doing a good job at communicating to their end users that personalised fields are not an automatic indication that an email is to be trusted.

It is worth noting, however, that programme administrators incorporated personalisation on just 40% of campaigns that have been sent through our system. We recommend that organisations 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.

![Suspicious email reporting](image)

When are suspicious emails reported?

<table>
<thead>
<tr>
<th>Day</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sunday</td>
<td>2%</td>
</tr>
<tr>
<td>Monday</td>
<td>19%</td>
</tr>
<tr>
<td>Tuesday</td>
<td>21%</td>
</tr>
<tr>
<td>Wednesday</td>
<td>22%</td>
</tr>
<tr>
<td>Thursday</td>
<td>21%</td>
</tr>
<tr>
<td>Friday</td>
<td>14%</td>
</tr>
<tr>
<td>Saturday</td>
<td>1%</td>
</tr>
</tbody>
</table>
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.
CONSEQUENCE MODELS

What types of consequences are enforced in your organisation?
We asked infosec professionals about the types of consequences (if any) they have in place to incentivise employees to avoid becoming ‘repeat offenders.’ (Note: Multiple answers were permitted.)

45% of organisations said there are ramifications if their users continue to click on simulated phishing attacks.

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
- Counselling from the IT department
- One-on-one training from the IT department
- Entry into the organisation’s formal discipline process

A TALE OF TWO REGIONS

As a global organisation, we have witnessed firsthand the differences between US and UK approaches to end-user risk management. We parsed 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.

What phishing threats did organisations experience in these regions?

It’s possible that organisations 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).

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

In-Person Security Awareness Training
Computer-Based Online Security Awareness Training
Awareness Campaigns: Videos and Posters
Monthly Notifications/Newsletters
Simulated Phishing Attacks
UK organisations 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?
Below are results of a third-party survey of 3,000 technology users—1,000 each in the US, UK and Germany—in which working-age adults were asked 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 they were surveyed in 2017.

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:

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. There were significant improvements in awareness among US and UK respondents in comparison to mid-2017 (see sidebar).

<table>
<thead>
<tr>
<th></th>
<th>United States</th>
<th>United Kingdom</th>
<th>Germany</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>46%</td>
<td>55%</td>
<td>71%</td>
</tr>
<tr>
<td>Incorrect</td>
<td>22%</td>
<td>21%</td>
<td>10%</td>
</tr>
<tr>
<td>No Guess</td>
<td>32%</td>
<td>24%</td>
<td>19%</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>What is smishing? (global average)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16% Right</td>
</tr>
<tr>
<td>17% Wrong</td>
</tr>
<tr>
<td>67% No guess</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Average click rate for smishing tests</th>
<th>9%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average click rate for phishing tests</td>
<td>9%</td>
</tr>
</tbody>
</table>

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.
ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps and social media), protect the critical information people create and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organisations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today’s mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.