THE STATE OF PHISHING DEFENSE

Susceptibility, Resiliency, and Response to Phishing Attacks

2018

A FEW WORDS ABOUT THIS REPORT

Cofense™ has a clear mission: we help the world stop phishing attacks. To do that we gather data, lots and lots of it. The data in this report is mostly drawn from our work with customers - thousands of global organizations including half the Fortune 100 - and the analysis performed on threats in the wild by our research and intelligence teams. Here's a little about Cofense and the data we analyze:

- Cofense sends over 10 million phishing simulations each month and enables over 15 million users to report malicious emails (as of 10-1-18)
- The Cofense Phishing Defense Center (PDC) analyzes over 3,000 reported emails every day, with more than 10% found to be malicious
- The Cofense Intelligence™ team analyzes more than 4,000 emails and campaigns each month
- Cofense Research teams have access to more than 1 million active phishing threats every day via monitored honeypots and botnets

Our sole focus is phishing defense. Our teams in professional services, consulting, and support have decades of experience in helping organizations stop the most active threats they face.

No one can eliminate the risk entirely, but there are ways you can reduce it. Read on to learn what attacks pose the most risk and how you can best manage that risk.

Rohyt Belani
Co-founder and CEO

Aaron Higbee
Co-founder and CTO

EXECUTIVE SUMMARY

Phishing defense is really a form of risk reduction—a very powerful form, since most agree that phishing remains the #1 cyber-attack vector. Not only does email deliver over 92% of malware[1], by the end of 2017 the average user received 16 malicious emails per month.[2]

With limited resources to mitigate threats, companies need to identify their critical business value and the threats most likely to drain it. They need to stay focused on real threats, both active and emerging.

In this report, Cofense™ presents real data, not the results of a market survey with opinions. The data comes from millions of simulated phishing attacks, zeroing in on user susceptibility, reporting behavior, and resiliency.

We correlate that data with real attack data seen in our Phishing Defense Center (PDC), a managed service that analyzes thousands of reported emails each day. Our findings are also backed by the insights of Cofense Intelligence™, which collects millions of malicious emails daily and performs human analysis on thousands of phishing campaigns per month.

For this report, we've linked insights on real threats to simulated attack results—keeping them connected as they should be. The report focuses on the Top 10 active threats our customers see, as reported by users and verified by the PDC.

THE DATA

As mentioned, we have plenty of data. This report reflects:

- The experiences of a 1,400 client-sample in 23 industries and more than 50 countries. The 1,400 organizations were chosen because they have complete datasets that included susceptibility metrics as well as phish reporting metrics.
- Simulation data from July 2017 to June 2018
- Approximately 135 million simulated phishing emails
- 48,000 "in-the-wild" phishing campaigns analyzed by Cofense Intelligence
- Approximately 800,000 reported emails into the Cofense PDC from January 2018 to July 2018

KEY FINDINGS

- On average, 1 in 10 emails reported by users are identified as malicious. That 10% has bypassed other security solutions such as email gateways to make it to users' inboxes.
- Over 50% of reported malicious emails are tied to credential phishing (see chart p. 8 for details)
  - Credential phishing is the runaway leader in user-reported malicious emails
  - It's also the threat to which users are most susceptible during simulations
- Simulations drive resiliency to the Top 10 active threats
- By industry, utilities and energy build the most resiliency to phishing over time
- Most industries considered "critical infrastructure" need to improve their phishing defense

KEY TERMS

Simulation - Cofense simulates phishing emails to condition and educate users. Our simulations are not random. They are carefully chosen scenarios based on real phishing threats.

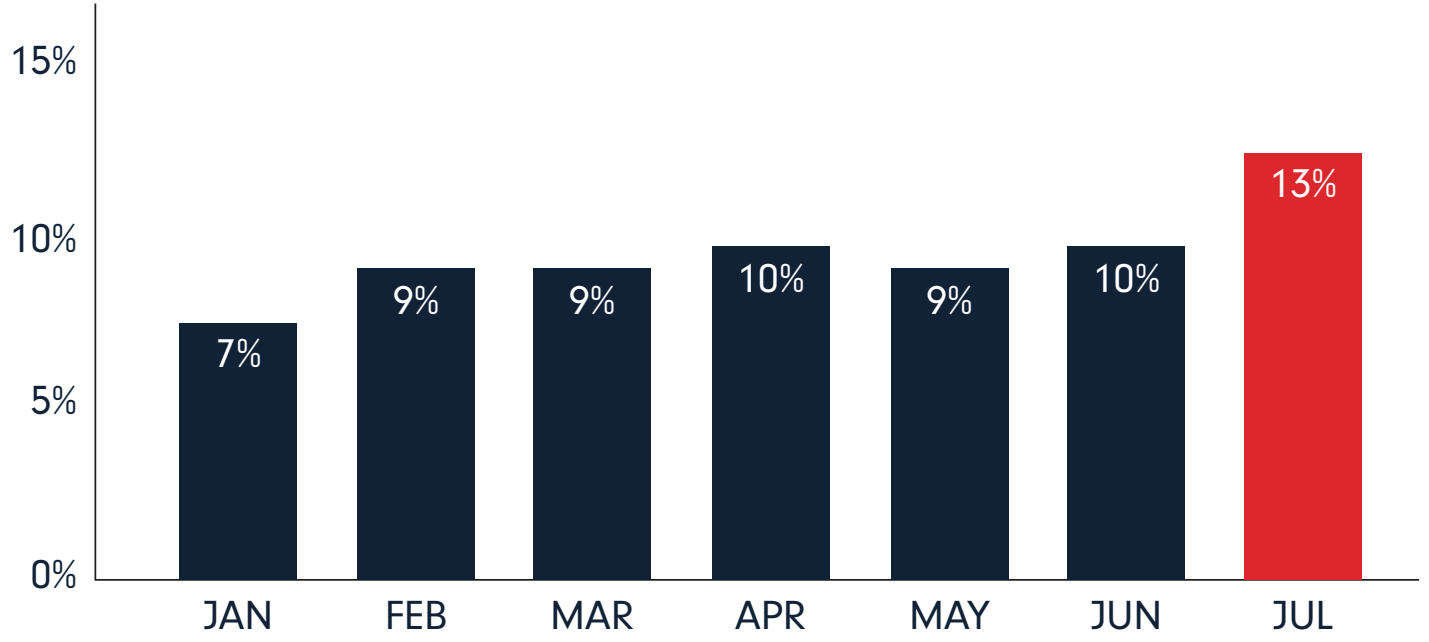
Susceptibility – The measure of users falling for simulated phishing emails.

Reporting – The measure of users identifying threats and reporting simulations to security teams.

Resiliency – The ratio of users reporting simulations to those that fall susceptible. A 1 to 1 ratio is a good start, while 2 to 1 is strong and 3 to 1 stellar.

WHAT'S REAL? **REPORTED THREATS**

ON AVERAGE, 10% OF REPORTED EMAILS ARE MALICIOUS

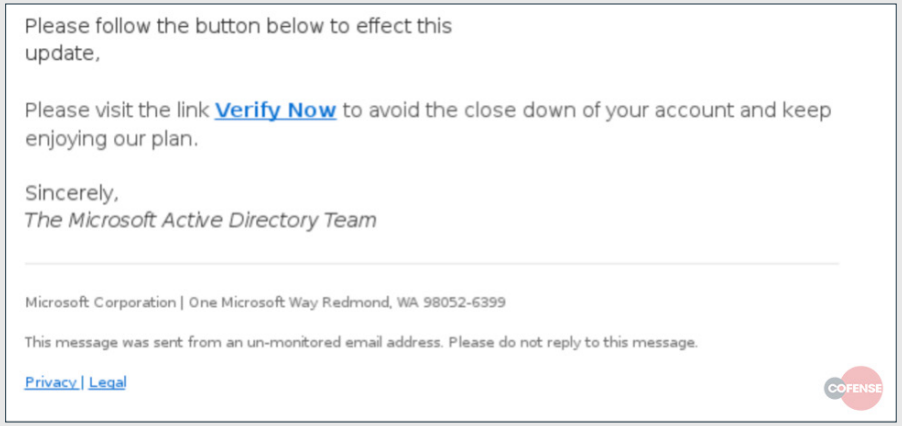


PDC: PERCENT OF MALICIOUS EMAILS REPORTED

Thus far in 2018, the Cofense Phishing Defense Center has verified 1 in 10 reported emails as malicious. Again, the total volume of analyzed emails is approximately half a million. With email volumes steadily growing, it's important to educate users on the telltale signs of phishing. Organizations should also deploy reliable spam filtering, both for corporate email and security teams sorting through reported threats. (See the Noise Reduction feature in Cofense Triage™.)

WHAT GETS THROUGH: EMAIL WASN'T STOPPED BY POPULAR EMAIL GATEWAY, PROOFPOINT

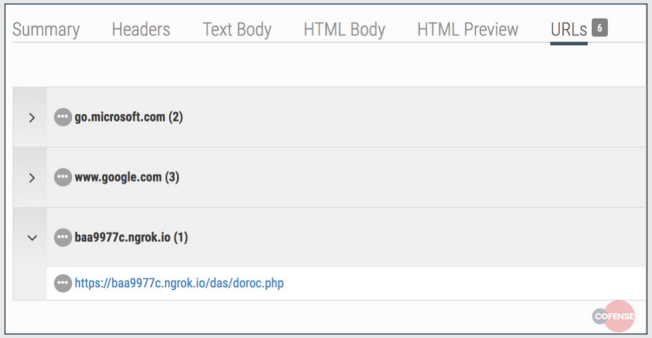
Despite the millions of dollars invested in layers of security, threats continue to bypass even the most popular security solutions. The Cofense PDC sees the malicious emails that were delivered to users' inboxes and then reported by them – the last line of defense. Below is an example of an email reported:



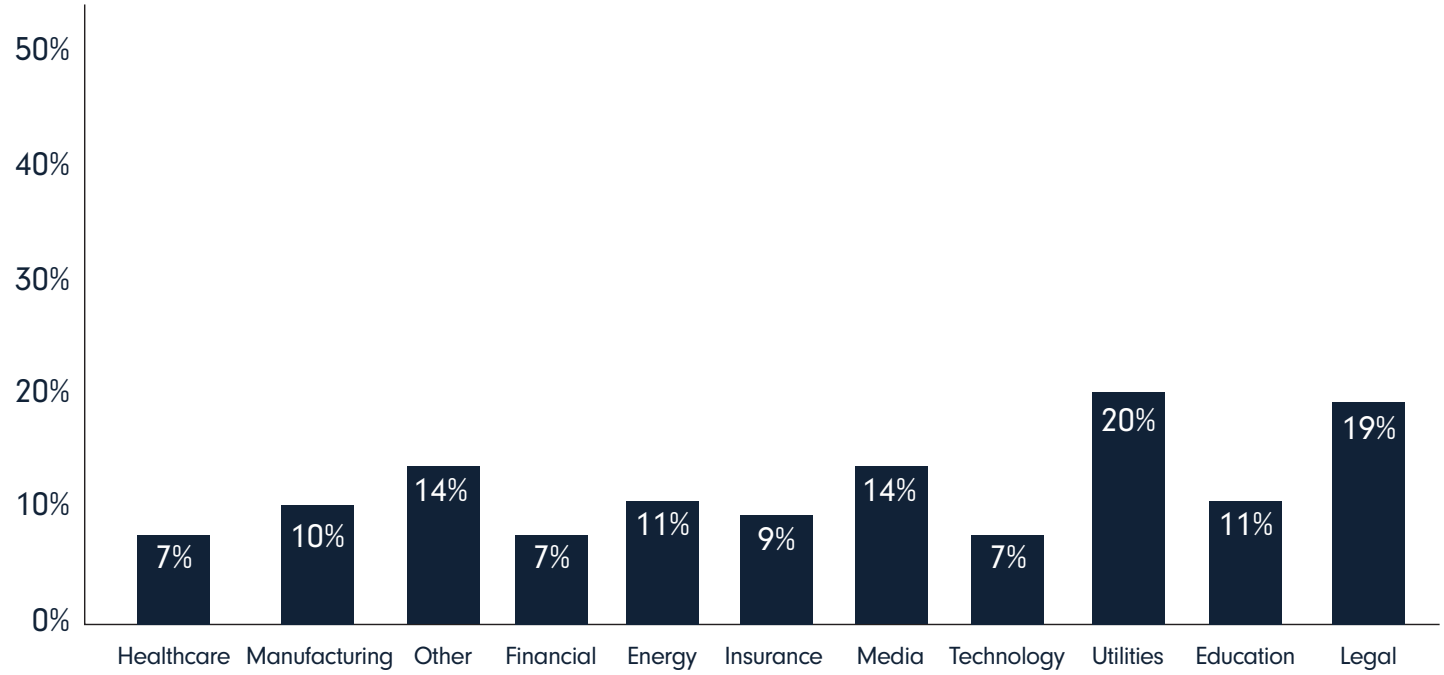
In analyzing this email reported by a user, we see the attackers are acting as if they are from Microsoft, perhaps posing as support for the Office365 account and using a common tactic of playing on the user's sense of urgency. The phish is crafted to convince the user they must act quickly to save his or her account with a link to do just that.

Digging deeper into the HTML of the attacking email we see that the "Verify Now" link does not go to Microsoft or an attributed site, but to a malicious site that mimics Office365. Looking in the header we see that it was analyzed by the Proofpoint email gateway but it was not stopped from being delivered to the inbox of an employee.

Luckily, this company had trained its employees to recognize phishing attempts and gave employees an easy way to report them to IT Security.



WITH A FEW EXCEPTIONS, THE 10% RATE HELD TRUE IN KEY INDUSTRIES.



INDUSTRY: PERCENT OF MALICIOUS EMAILS REPORTED

In major industries, malicious messages as a percentage of reported emails were virtually the same as the cross-industries average. Of course, even in an industry where the rate is lower—financial services for example, at only 7%, it takes just one successful phish to inflict a costly toll. According to the Ponemon Institute, the average cost of a data breach is approaching $4 million[3].

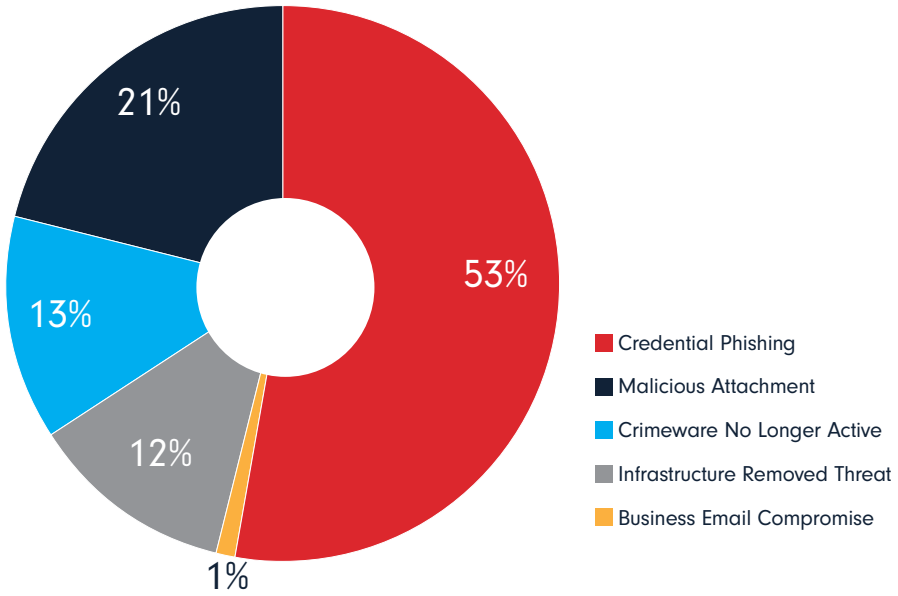
OVER HALF OF REPORTED MALICIOUS EMAILS ARE TIED TO CREDENTIAL PHISHING.

Hackers are following the money. Over half of reported phishes are sent to harvest user logins. These emails include a link to a malicious landing page, so hackers can gain access to corporate data or establish a network foothold.

It's important to note the low percentage of reported Business Email Compromise (BEC) emails, aka CEO fraud. BEC is hardly rare. It is simply more targeted and thus reported in lower volumes. With employees in finance departments becoming increasingly vigilant, we are beginning to observe attackers use similar tactics in other domains. Namely, submitting fake invoices from legitimate vendors (ex: from compromised supply-chain email accounts) and targeting people involved in mortgage brokerage, and legal services related to title and home purchase closing. It is critically important to condition skepticism of any email asking for sensitive data or payment details.

The most well-known type of BEC is wire-transfer phishing. Typically, a hacker will email someone in finance with an urgent request to wire funds. The email spoofs an internal sender, sometimes even the CEO. When it comes from a compromised email account, it's even harder to spot the ruse. To the right is a real example reported to the PDC.

Key takeaway: Are next-gen filters working to stop BEC? There is a new crop of security vendors claiming to have machine learning email filters in place to identify BEC emails. Cofense is observing BEC emails coming from real compromised accounts in the wild, as well as CEO names encoded in UTF-8. These two tricks are effortlessly bypassing the latest crop of next-gen phishing detection technologies.



MALICIOUS EMAILS CATEGORY BREAKDOWN

Hi Otis,

How are you today? We have a payment of $6,500 that need to go through,kindly check if you can get this amount sent right away and get back to me via this email for me to send you the bank payment information details immediately .

Regards,

[redacted]

Sent From My Iphone <president_pt@hotmail.com> [redacted]

REAL BEC EXAMPLE REPORTED TO THE PDC

EXAMPLES OF CREDENTIAL PHISHING + SIMULATION RESULTS

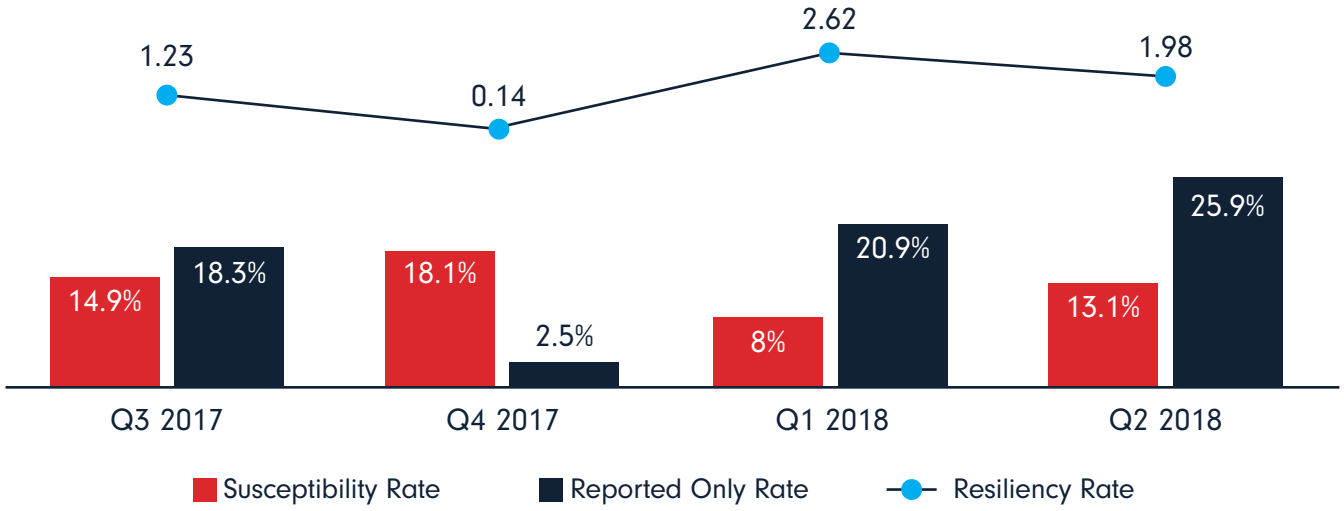
Office365 adoption by businesses has not gone unnoticed by attackers.

Businesses are faced with three variants of credential phishing attacks. The most popular of these are phishing pages resembling Microsoft themed login pages. The second common variant is a grab-bag approach asking a user to use one of perhaps several popular authentication providers on the same page. For instance, a phishing page may ask the user to login with any credential from Dropbox, LinkedIn, Facebook, Hotmail, Gmail, or Yahoo in hopes that the victim's password can be reused.

The data below is focused on credential phishing that can actually compromise the business — not phishing emails asking for someone's Netflix password. While a nuisance, they are not the threat a business should focus on.

EXAMPLE 1: HSA CUSTOMER SERVICE EMAIL (DATA ENTRY)

Normally, these emails are bogus notifications of a customer-service inquiry from a healthcare savings account. The lure requires the target to view an embedded link. The results of Cofense simulations:



HSA CUSTOMER SERVICE EMAIL (DATA ENTRY)

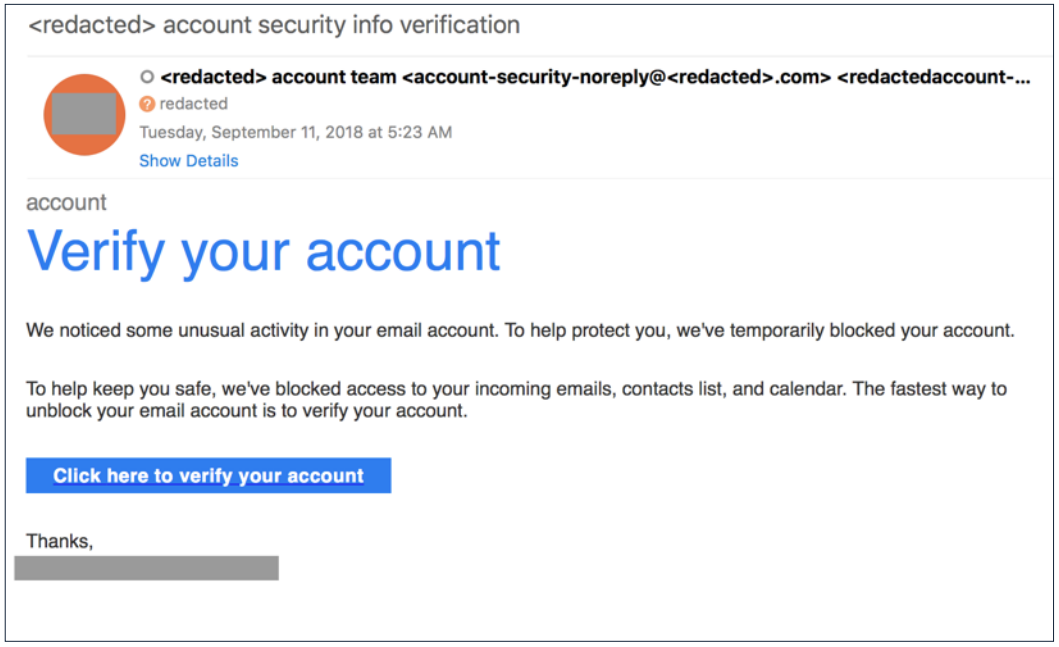
The scores are not bad, with a resiliency ratio of over 1 to 1. The next goal would be a ratio of 2 users reporting for each 1 falling susceptible. The data is from a simulation based on a real phishing scam, targeting employees with HSAs. The email creates urgency with the subject of healthcare finances, another example of how money talks in phishing.

THE HEALTHCARE INDUSTRY IS A PHISHER'S PARADISE

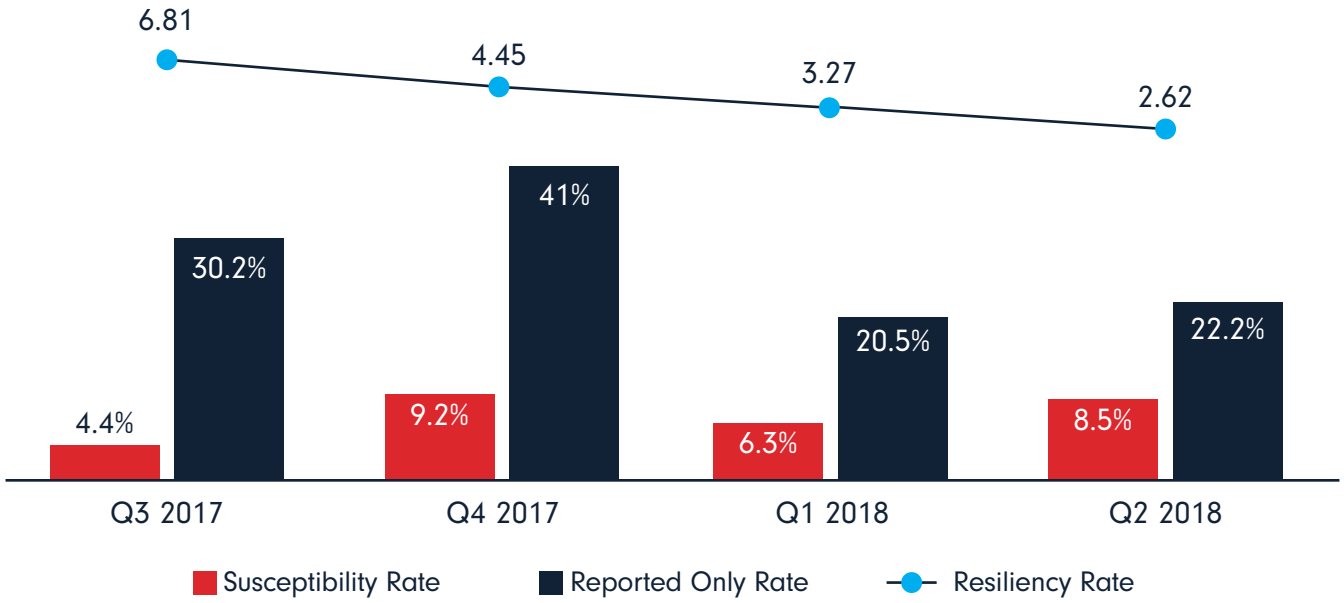
Why do phishing attackers love healthcare? Because few industries collect more lucrative personal data: name, Social Security number, email address, home address, date of birth, and usually one or more credit card numbers. Over a third of all data breaches occur at healthcare companies.[4] Measured by their replacement cost, healthcare records command a premium price. It costs $408 to replace a single record vs. the cross-industries average of $148.[5] For a closer look at phishing in healthcare, see the Cofense Industry Brief.

EXAMPLE 2: ACCOUNT SECURITY ALERT

Another phish telling the recipient to "click here," in this case to verify an account due to suspicious activity. A real example:



And results from simulations:



ACCOUNT SECURITY ALERT

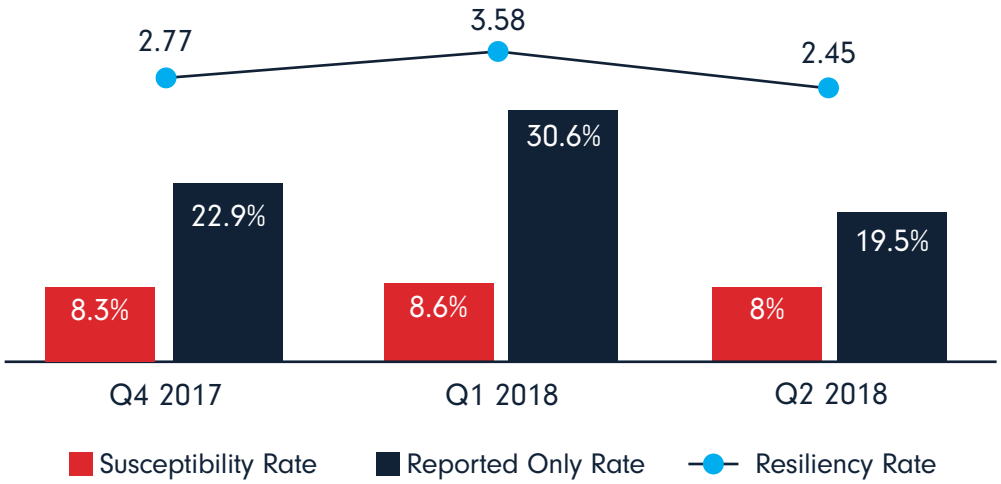
Resiliency rates are strong, with lower recent rates explained by the growing number of organizations using this scenario (a wider test pool normally brings the average down). The simulation notifies users their accounts have been compromised and instructs them to reset passwords, or else. Failure to comply would be deemed a policy violation. It's a classic phish our customers' users do a good job of spotting.

EXAMPLE 3: LOGIN TO DOWNLOAD

This phishing theme typically asks the recipient to login to their account to view a document or notification. Sometimes, these messages contain an attached PDF containing a link to a credential-phishing website. Attackers are stuffing URLs inside of PDFs to effectively bypass URL scanning and click-wrapping technologies.

REAL EXAMPLE OF A NOT-SO-REAL PAGE

And results from simulations:



LOGIN TO DOWNLOAD

Here, Cofense customers are consistent in seeing and saying something. The next milestone is to build on Q1 2018 and maintain over 3 to 1 resiliency. Once again, the simulation is based on a real phish spotted by Cofense Intelligence. It asks recipients to login to view a file online, purportedly a PDF document, and aims to compromise the network via shared/secure file services, exploiting the popularity of cloud storage and sharing. Companies using these services should absolutely test this scenario.

DO YOU HAVE A CLOUDY VIEW OF YOUR CLOUD SERVICES?

Cloud services offer ample phishing opportunity, especially rogue accounts created outside of IT's purview. To help companies see which cloud services are live in their environments, including unauthorized services, Cofense created a free tool, Cloudseeker™. It gives a comprehensive view to protect your organization.

MALICIOUS ATTACHMENTS REMAIN A PHISHING EMAIL FAVORITE.

Twenty percent of reported phishing emails contained malicious attachments. By burying links in attachments, hackers seek to evade URL scanning and detection by email security software—one more reason to condition users to recognize and report phishing via a security awareness solution like Cofense PhishMe™. This cannot be overstated: malicious emails with attachments fool machines all the time, in particular emails with links inside of PDF files. Our data on attachment-based phishing aligns with Cofense Intelligence data on how often hackers abuse Microsoft Office macros.

BEST PHISHING LURES

6 OF THE TOP 10 REAL PHISHES USE 'INVOICE' AS THE SUBJECT.

Not since the Beatles has a Top 10 chart been dominated like this. According to Cofense Intelligence, the subject "Invoice" appears in 6 of the 10 most effective phishing campaigns in 2018. Not only that, "Customer Invoice" snags the #7 spot. The other 3 winners also pose as financial transactions: "Payment Remittance," "Statement," and "Payment."

It's a powerful reminder that hackers stick with techniques that work—and that organizations should focus their defenses on threats they actually face, instead of asking employees to become experts on everything. Employees in finance and accounting should train repeatedly for these scams, plus anyone else authorized to spend the company's money.

In any business, invoices are as common as email itself. People receiving them have access to the information hackers want. If infected, financial employees' machines are potential goldmines. No wonder "Invoice" is the lure de jour.

MICROSOFT OFFICE MACROS ARE THE DOMINO'S OF MALWARE DELIVERY.

No other vehicles deliver more malware. According to Cofense Intelligence, 45% of all malware analyzed currently lurks in Office macros[6]. The reason is simple: the world runs on MS documents, the face of a trusted brand. When these docs are weaponized, malware installation is as easy as a careless click.

While businesses can disable macros, productivity might suffer. A more surgical approach is better: blocking or gray-listing documents from unknown or unsavory sites and balancing security automation with user education. Of course, as soon as you finetune your approach, attackers will pivot again. Witness the new .PUB file extension (Microsoft Publisher) which Cofense discovered is used to embed macros in phishing emails.

SUBJECTS FOR 2018'S TOP PHISHING CAMPAIGNS

1. Invoice
2. Payment Remittance
3. Invoice
4. Invoice
5. Invoice
6. Invoice
7. Customer Invoice
8. Invoice
9. Statement
10. Payment

'ATTACHED INVOICE' IS THE MOST-REPORTED THREAT IN SIMULATIONS.

RANK	PHISHING SUBJECT/THEME	# REPORTED
1	Attached Invoice	4,796
2	Payment Notification	2,267
3	New Message in Mailbox	2,088
4	Online Order (Attachment)	679
5	Fax Message	629
6	Secure Message - Office Macro	408
7	Online Order (Click Only)	399
8	Confidential Scanned Documents (Attachment)	330
9	Conversational Wire Transfer (BEC)	278
10	Bill Copy	251

MOST-REPORTED TOP 10 ACTIVE THREAT SIMULATIONS

It's not even close. By more than 2 to 1, "Attached Invoice" is the active threat users report most often. Two other attachment-based threats made this Top 10, "Online Order" at #4 and "Confidential Scanned Documents" at #8.

Organizations need to train users to view attachments suspiciously, especially invoices, online orders, and anything with macros. Also, it's not a bad idea to send a gentle reminder: even though online shopping and BYOD are facts of life, users should be careful before opening messages from Internet retailers, even favorite brands.

Another tip: be mindful of the financial calendar. End of month, end of quarter, and end of year are ripe for phishing attacks disguised as financial messages. When it's heads-down processing time, give employees a heads-up.

Many of the most-reported emails have to do with money, something to drive home in security training. If you're unsure of the active threats your organization faces, this list is a good place to start when launching an awareness program.

A SIMULATED 'ATTACHED INVOICE' EMAIL

To the right is a simulated phishing email whose lure is a phony invoice. It's based on a real phish seen by Cofense Intelligence, designed to distribute malware through macro-enabled Microsoft Word docs.

THE RED FLAGS

- Generic customer name
- Not a standard business signature
- Cherub Springs Ltd. isn't a real company, though it's a plausible counterfeit; when attackers use real names their scams are harder to see

From: Invoice <invoices@edoctransfer.com>
Subject: Your attached invoivce from Cherub Springs Ltd.

Dear Customer,

Please find attached your latest document (s). You may have noticed that we have changed the way you receive your new attached documents from Cherub Springs.

Following feedback from our customers we've invested in upgrading our billing systems to make things a little easier for you.

Here's a few ways we've made it easier for you:

- Your new documents are now attached to your email. You don't have to follow a link now to get to your documents.
- Our customer portal has been upgraded to give you a clearer, simpler view of your documents and any outstanding invoices.
- You can simply and easily raise any queries you may have through the customer portal.
- You can also connect to our E-Billing solution to access other relevant documents through the customer portal.

Detailed below are your latest documents.

Account Number	Date	Invoice Number	Document Type
STA054C	SCENARIO_START_DATETIME	3027769	Invoice

Please note: you may wish to save your documents on initial viewing. However, after your first viewing you will be able to access copy documents by simply clicking the link.

If you would like to discuss or have any queries in relation to any of the documents then please do not hesitate to contact us on the phone number found on your invoice and we will be more than happy to assist you. Please do not reply to this email.

To see Cherub Springs latest special offer that will save you money and help support those in need, please click on the attached document.

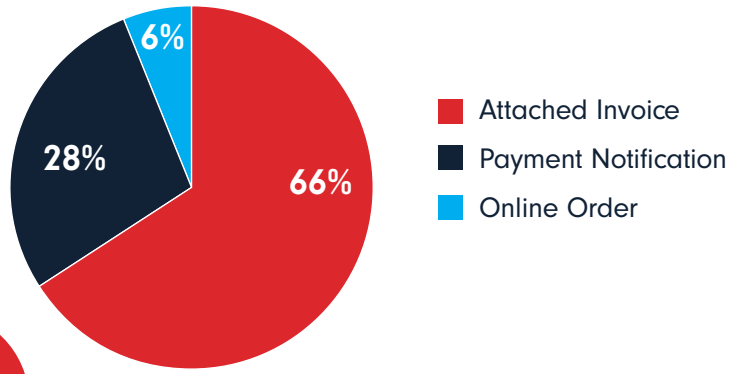
With Kind Regards,

Cherub Springs Ltd

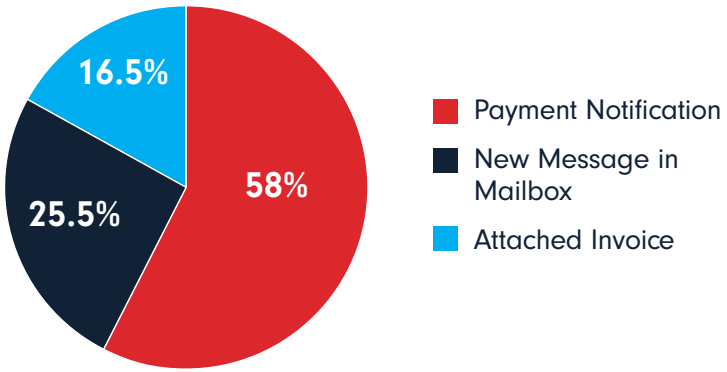
TOP 3 REPORTED PHISHING SUBJECTS/SIMULATION THEMES IN KEY INDUSTRIES

If your business operates in any of the following industries, you'd be smart to focus on these common phishing tactics across your threat intelligence, incident response, and security awareness programs. The industry findings track with the Cofense PDC's overall data.

Education

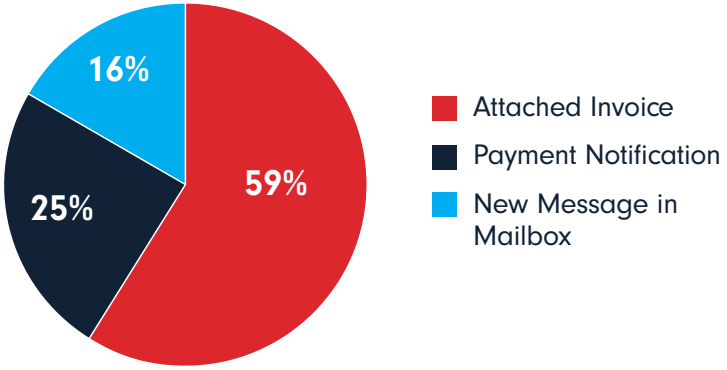


Healthcare

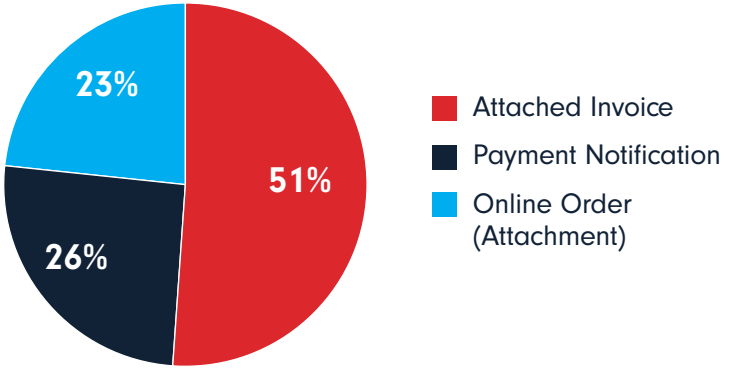


TOP 3 REPORTED PHISHING SUBJECTS/SIMULATION THEMES IN KEY INDUSTRIES (CONTINUED)

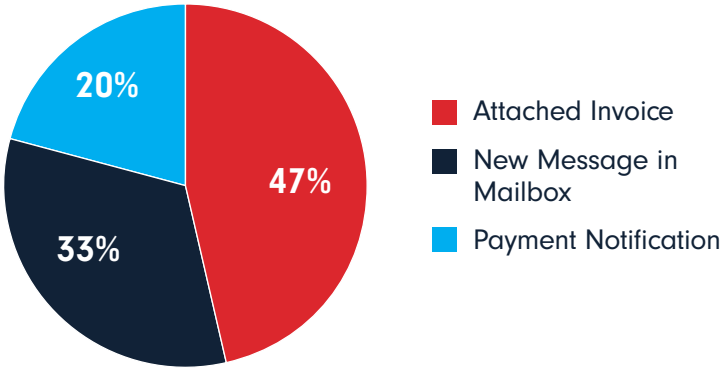
Manufacturing



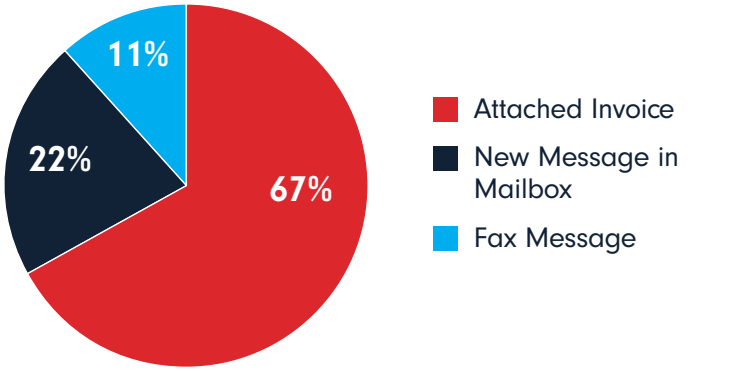
Financial Services



Energy

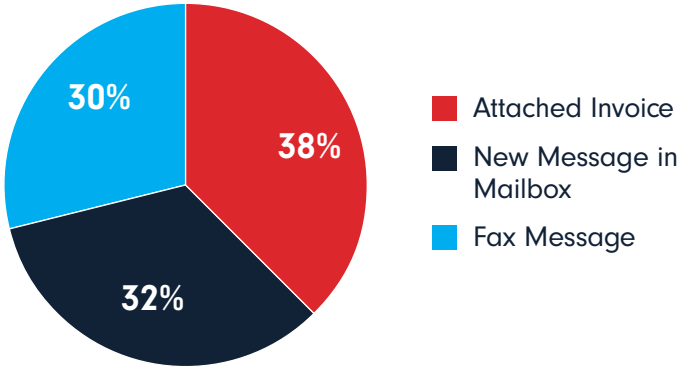


Insurance

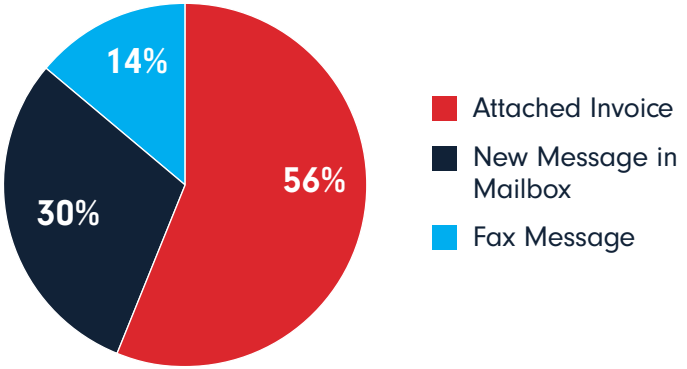


TOP 3 REPORTED PHISHING SUBJECTS/SIMULATION THEMES IN KEY INDUSTRIES (CONTINUED)

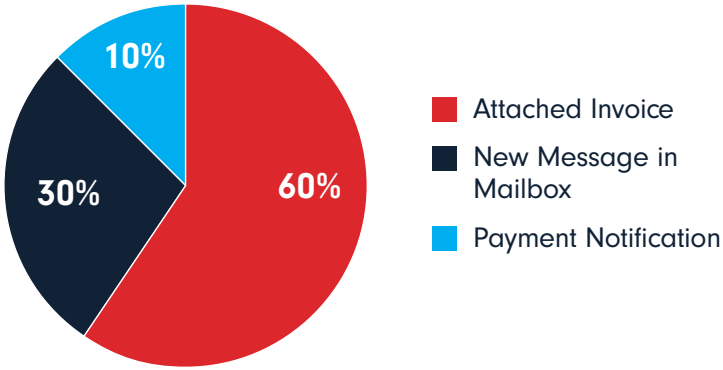
Media



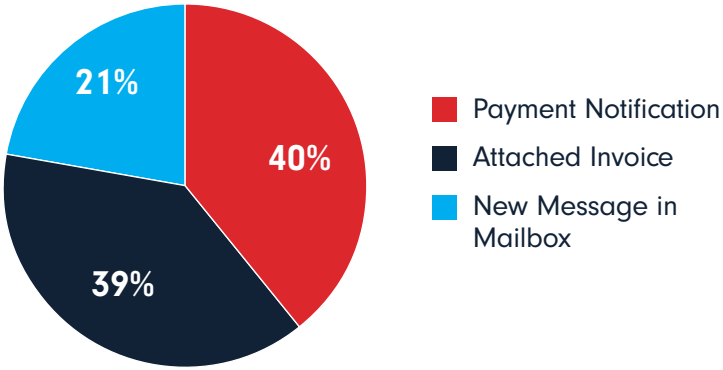
Professional Services



Utilities



Other (Miscellaneous Industries)



RESISTING THE LURES

RESILIENCY TO ACTIVE THREATS: THE DATA SHOWS THAT TRAINING HELPS.

The following data comes from Cofense phishing simulations. It shows how alert employees are to the Top 10 active threats. Active-threat simulations mimic real-world phishing attacks. They are the best indicator of what may happen when an actual phishing attack is launched against your employees.

Resiliency rates tend to fluctuate quarter over quarter. Rates can depend on many factors, such as the number of simulations, by whom, and how often. As seen in the data on "Invoice" phishes, timing can be a factor too, with users less alert during busy periods.

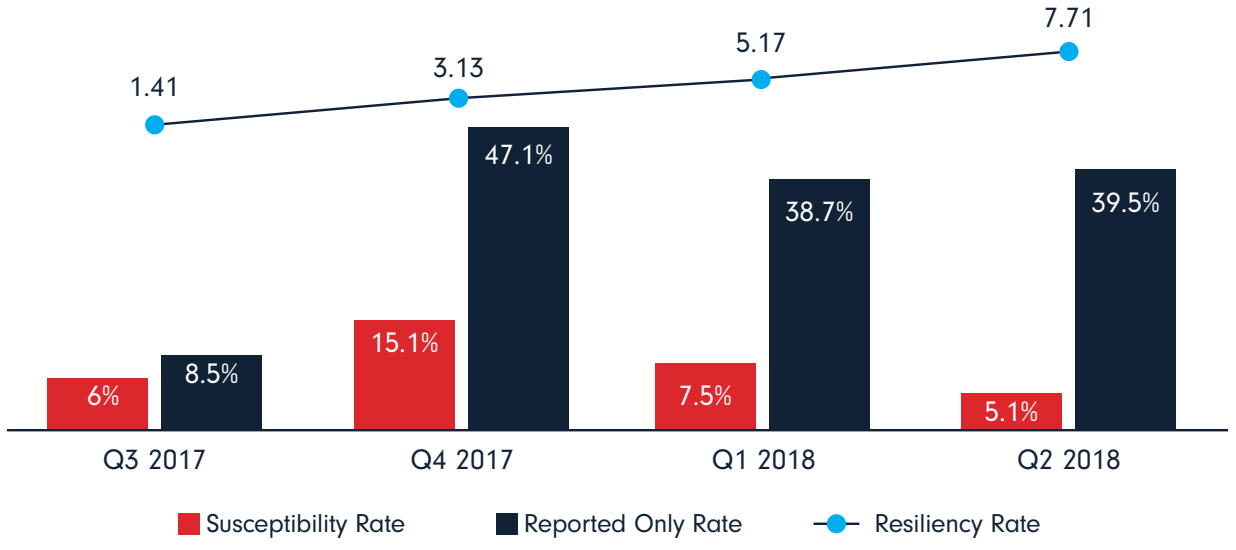
As a reminder, resiliency is the ratio of users reporting simulations to those that fall susceptible. Consider the impact of a phishing attack when 30% report it vs. 15% taking the bait. Building resiliency helps your organization respond faster to eliminate the risk.

3 TIPS FOR SIMULATION PROGRAMS

To get the best results as you condition users to report phishing:

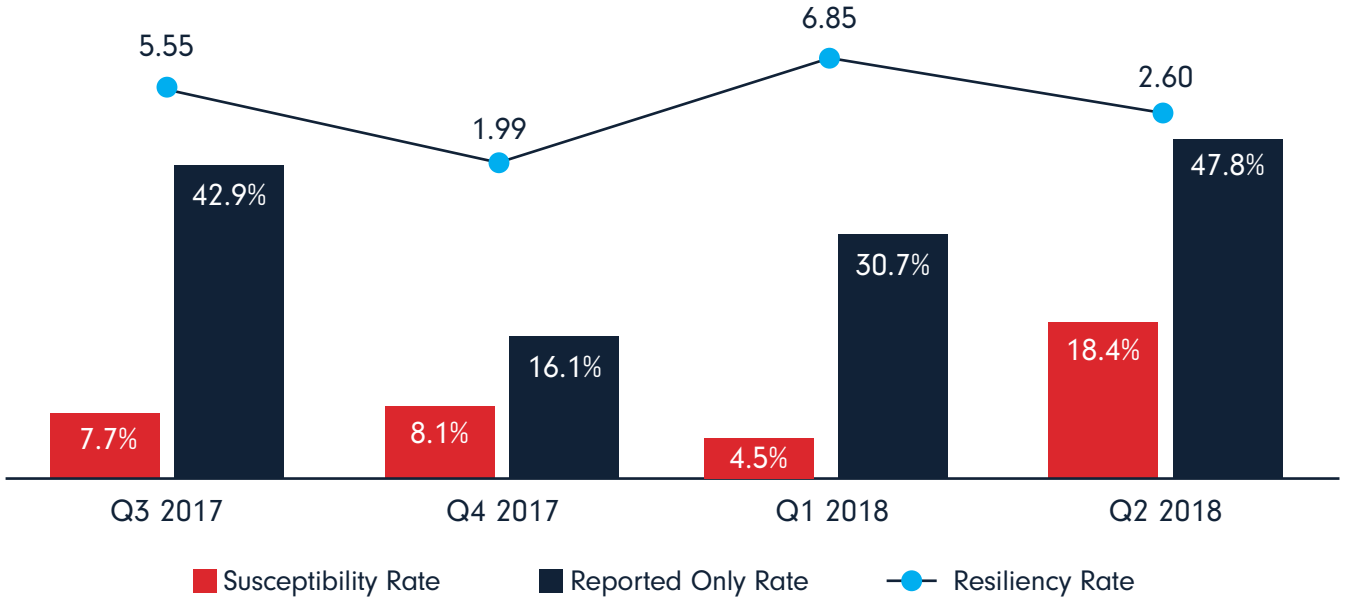
- Focus your simulations on active threats
- Train employees regularly, at least once a quarter
- Encourage reporting instead of scolding employees for falling susceptible

The last point is especially important, since the key to improvement is running the hardest simulations time and time again.



NEW VOICE MESSAGE IN MAILBOX

One possible explanation for good performance against this threat: users are familiar with email standards, making variances easier to spot. These emails tell recipients to click to check voicemail.



ONLINE ORDER EMAIL WITH ATTACHMENT

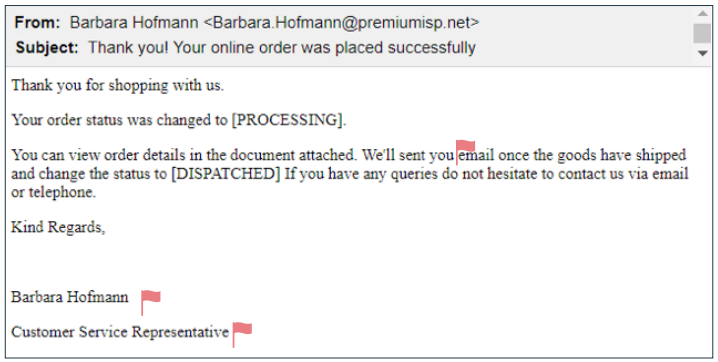
On this one, resiliency swings up and down, but the ratios–from 2 to 1 to nearly 7 to 1–are encouraging. During any given day, most employees will not have made a purchase online, so many will report a message claiming that they did. Of course, without proper training they may just ignore the email.

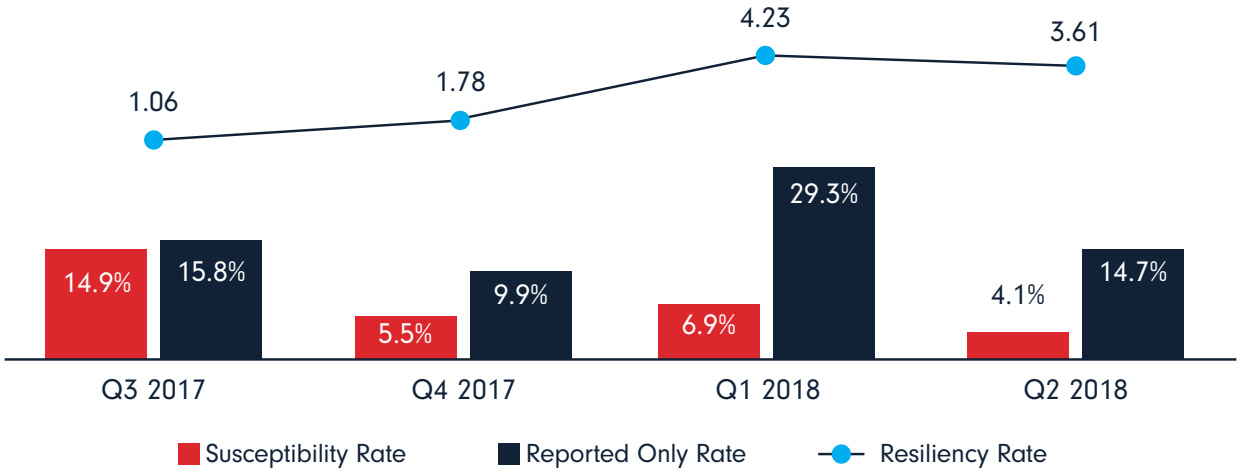
A SIMULATED 'ONLINE ORDER' EMAIL

This simulated email claims to update an online order. The recipient is urged to download a Microsoft Word document, a proven malware delivery vehicle.

THE RED FLAGS

- Typos
- No customer name
- Not a real signature

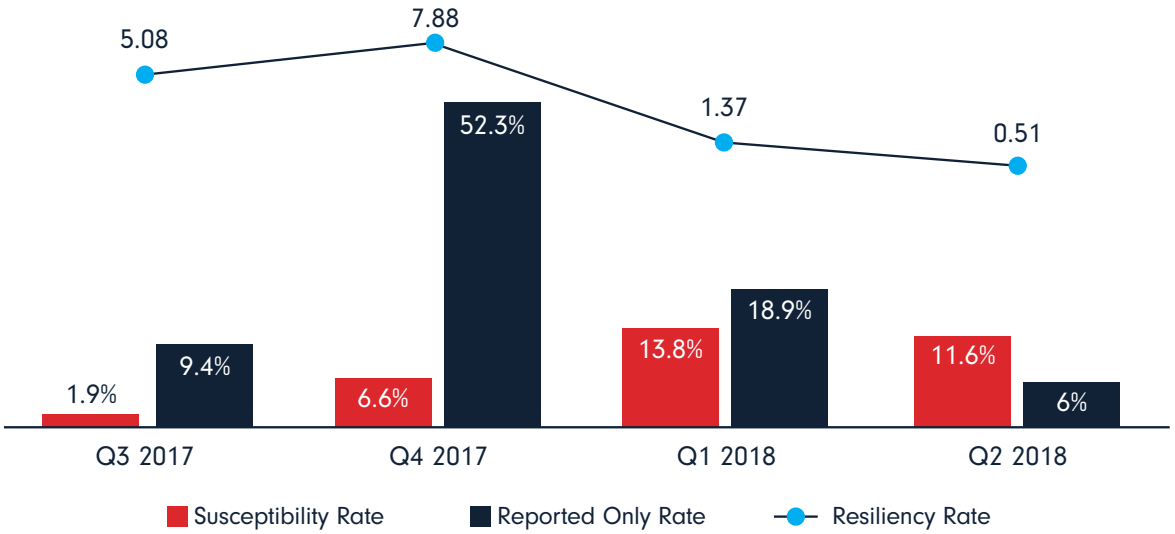




SECURE MESSAGE - OFFICE MACRO

Resilience is holding steady here, good news considering our template is personalized by company and the sender name, giving the patina of an internal message. Like other phishes that either come from within or appear to, "Secure Message" tips its hand by not matching the corporate email format, a clue not lost on alert users. Companies are smart to make sure users can tell the difference between their standard format and a counterfeit.

'ATTACHED INVOICE' (NO SURPRISE) IS AN ONGOING CHALLENGE.

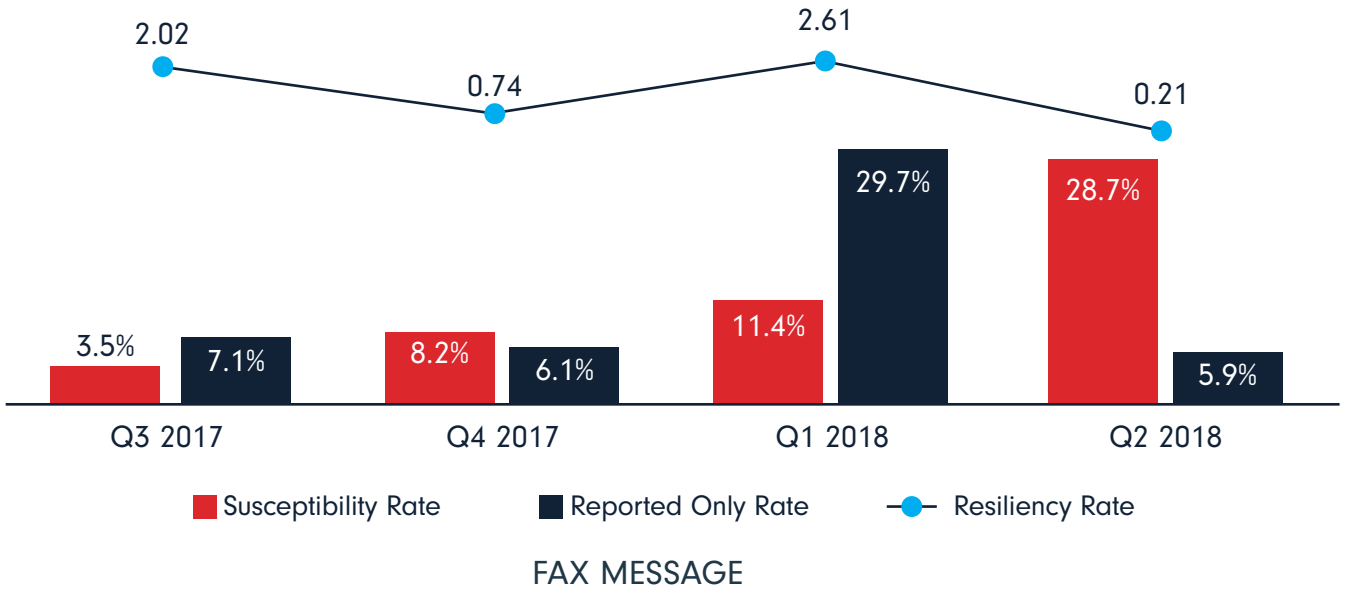


ATTACHED INVOICE

The resiliency rate has fluctuated since 2017, further proof that "Attached Invoice" is a formidable weapon and one users are likely to continue to face (as evidenced by our PDC and intel data above). The ubiquity of invoices, both for business and personal billing, makes them an especially potent phishing tool. As companies understand this, they are running more invoice simulations. It's not surprising that users need continued training to recognize this threat and clear instructions on how to respond.

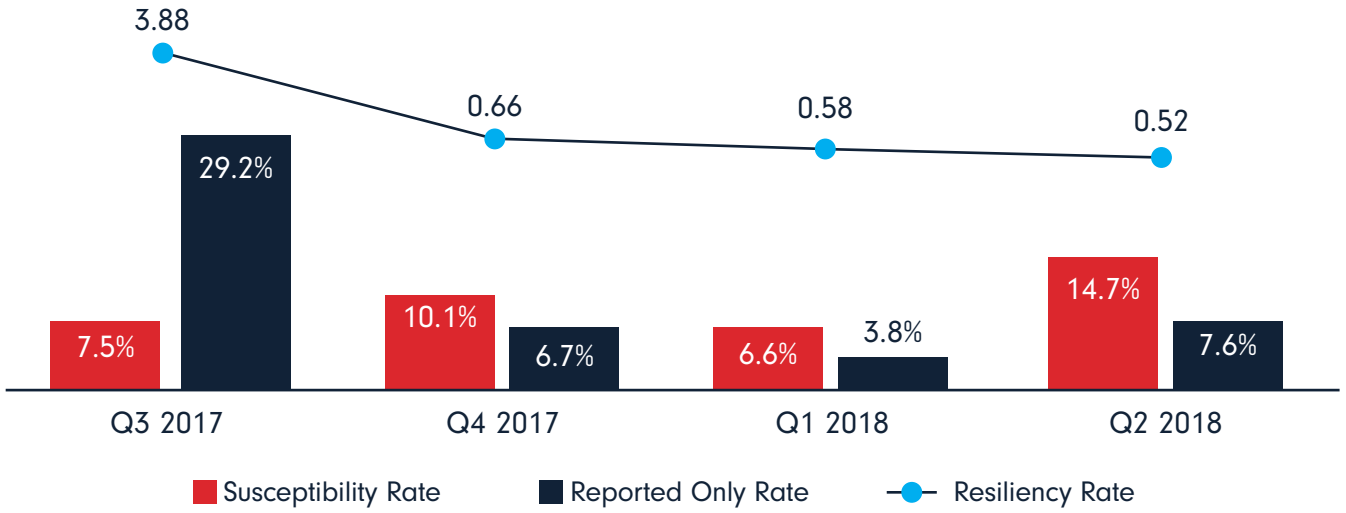
Cofense advises using a mix of "Attached Invoice" scenarios, even though this will cause rates to dip periodically. Over time, users will learn the threat's varieties and nuances. It's also advisable to target employees with invoicing responsibility to build deeper awareness where it matters most. Another action item: make sure everybody understands proper invoicing procedures, so users can compare suspicious attachments to the genuine article.

AT TIMES, RESILIENCY TO THESE 2 PHISHES DROPS.



FAX MESSAGE

Highly personalized emails make this one harder for users. Like "Attached Invoice," "Fax Message" is a scenario you'd be smart to run and repeat.



PAYMENT NOTIFICATION

Our simulated email mentions an ACH deposit, so users who aren't careful click to see how much they allegedly received. The Cofense PDC sees a lot of these emails in the wild. Best practice: run an initial simulation to baseline user resiliency and repeat to see which people or groups need additional training.

A SIMULATED 'PAYMENT NOTIFICATION' EMAIL

Based on a real phish seen by Cofense Intelligence, this simulation urges the recipient to view a payment notification attachment that could unleash malware.

THE RED FLAGS

- Once again, no customer name
- No signature whatsoever
- When the subject is money and the tone is urgent—IMPORTANT: AVAILABILITY OF FUNDS—well, there's your sign.

From: no reply <no-reply@securebankinggroup.org>
Subject: ACH Payment Notification

SECURE BANKING GROUP Vendor:10288253 Pay Dt: 20150903
Pay Ref Num: 2000546942

Please download and view payment document attached.

Your invoice has been processed for payment by Secure Banking Group Accounts Payable. The following items are included in
this payment:

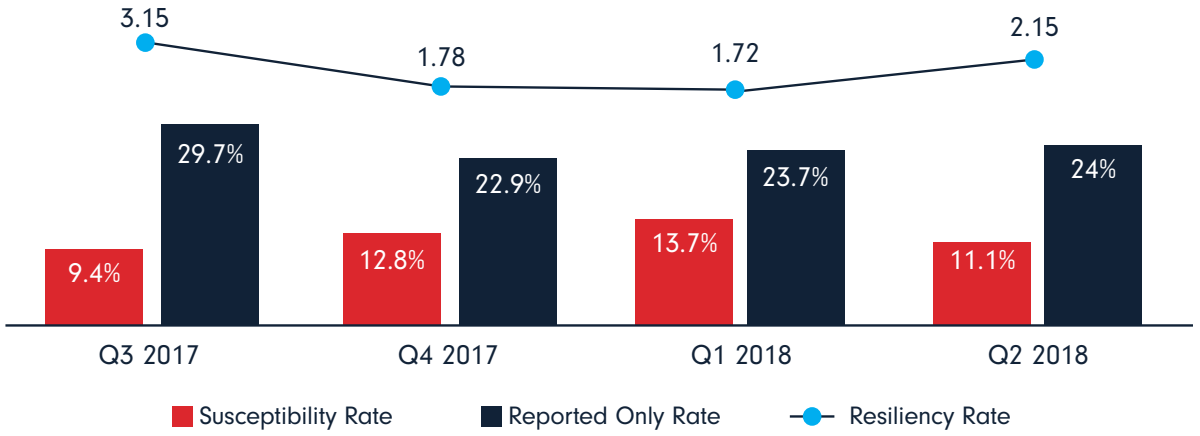
The net amount deposited to account number ending XXXX5311
designated by you is $1499.05

IMPORTANT AVAILABILITY OF FUNDS FOR WITHDRAWAL IS SUBJECT TO POSTING BY RECEIVING BANK (USUALLY WITHIN THREE BUSINESS DAYS)

Please do not respond to this e-mail. Should you have questions, please contact the Purchasing, Payment & Reimbursement helpline.

This message, and any attachments, is for the intended recipient's only, may contain information that is privileged, confidential
and/or proprietary and subject to important termsr. If you
are not the intended recipient, please delete this message.

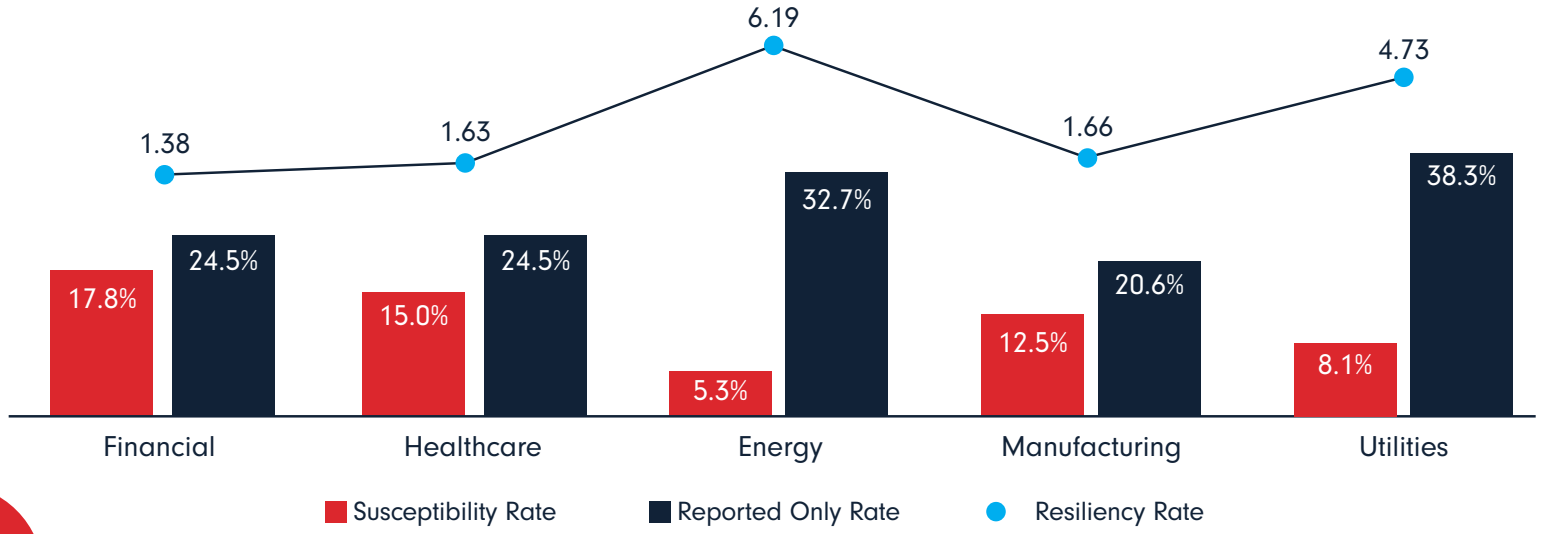
AGAINST THE TOP 10 THREATS IN TOTAL, OUR CUSTOMERS HAVE A 2 TO 1 RESILIENCY RATIO.



ACTIVE THREATS TEMPLATE PERFORMANCE

This data cuts across all Cofense PhishMe customers using our Reporter button. For every user who falls susceptible, two users report the active threat in simulation training. It's a positive trend with encouraging implications going forward as we add new templates to model the latest attacks.

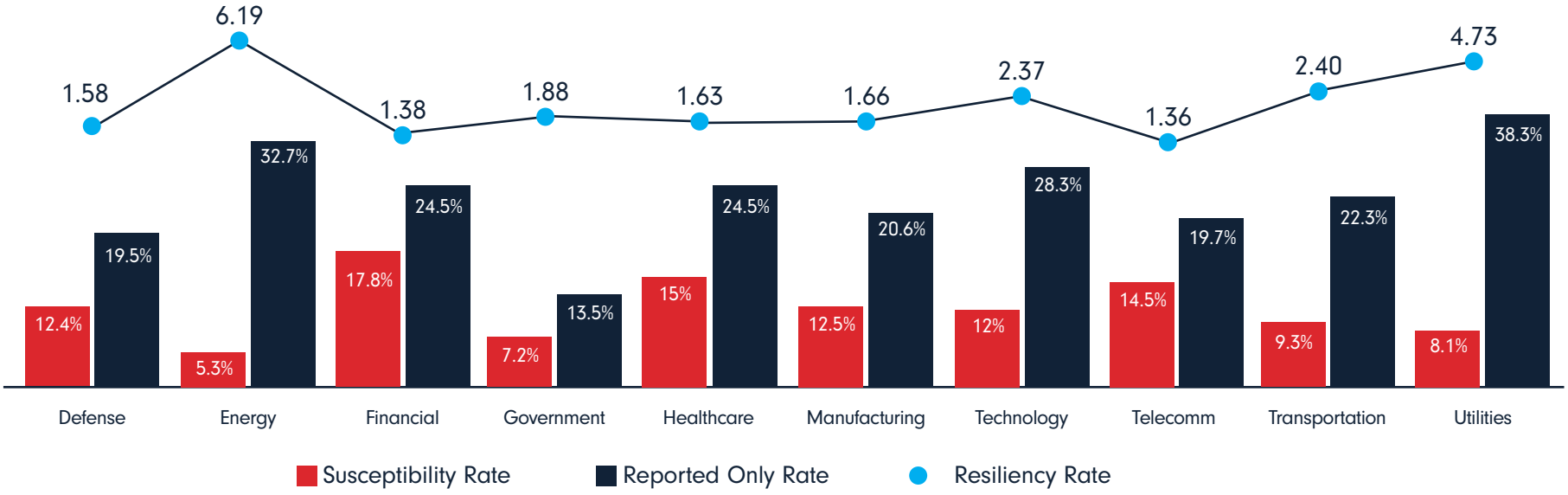
HIGHEST RESILIENCY IN INDUSTRIES THAT TRAIN THE MOST.



MOST ACTIVE INDUSTRIES

The previous charts show the industries using Cofense PhishMe to train against Top 10 threats. While utilities and energy show exceptional performance, other industries have room for improvement. This shows the value of repeated training, especially as well-known threats evolve and introduce new wrinkles. Why do utilities and energy do so well? Utilities and energy have always had a culture that promotes safety and training. It was easier for them to expand their culture into cybersecurity topics. Curiously, financial services spends more on cybersecurity products, but their people are not more resilient to phishing attacks.

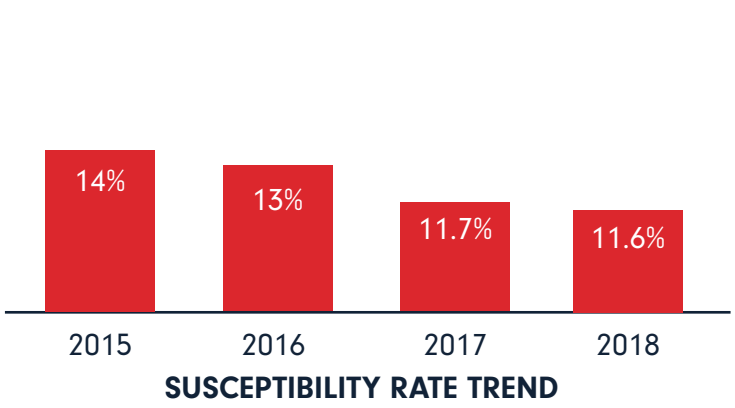
INDUSTRIES SEEN AS 'CRITICAL INFRASTRUCTURE' NEED TO IMPROVE.



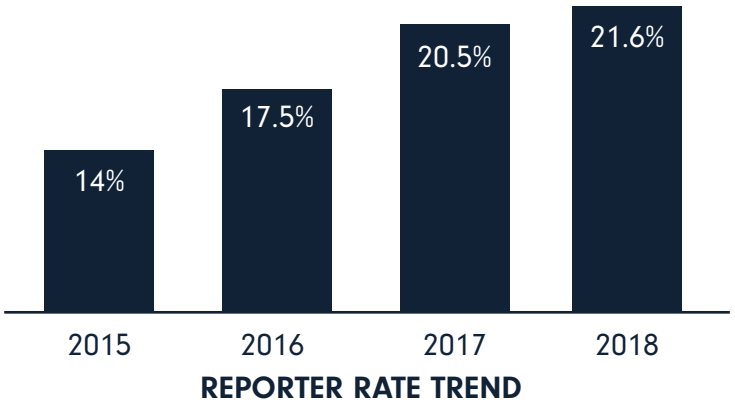
InfraGard, the partnership between the FBI and private sector, defines each of these industries as critical to national security. In phishing simulations, each has a ratio of at least 1 reporter to 1 victim. That's a decent start, but much more work remains to reach the more rigorous standards of a 2 to 1 or 3 to 1 ratio. The stakes are widespread damage—physical, financial, you name it—potentially affecting millions of people.

HOW RESILIENT ARE USERS YEAR OVER YEAR?

To show resiliency over the past four years, we'll look first at susceptibility and reporting rates. Note: this data is based on all Cofense simulations during this time, not just those that modeled active threats.

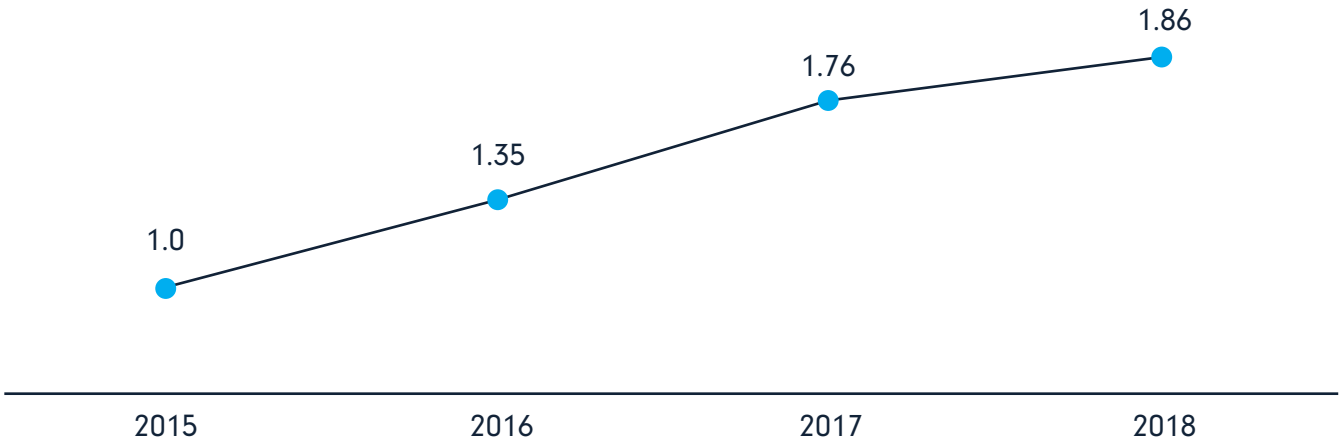


SUSCEPTIBILITY RATE TREND



REPORTER RATE TREND

THE RATIO OF REPORTING TO SUSCEPTIBILITY



RESILIENCY RATE TREND

During the past year improvement has leveled out, but the overall rate is approaching an encouraging 2 to 1. Given that phishing attackers continually change their techniques, even a modest gain in resiliency is good news. Customers commonly ask for benchmark data relative to their peers. While it might feel good to see that you are doing better than "Bank A", energy and utilities are demonstrating what is possible, and should be the benchmark to chase regardless of industry vertical.

The data in these charts comes from Cofense customers that have deployed our Reporter button. Administrators should create a safe environment for reporters and reward good behavior. The reporting button should appear on all educational pages used in simulations — show employees the tool you want them to use.

CONCLUSIONS

When hackers follow the money, businesses need to protect it. Sensible risk management dictates that a company should know (a) where its vital assets are and (b) which types of attacks pose the gravest threats. In other words, focus your efforts on what matters most.

With the rapid adoption of phishing simulations as accepted best practice, more vendors have entered the space. While this is great, we are monitoring a trend where the person who is titled "Security Awareness Trainer" is showing an affinity to use phishing lures of the imagination, instead of threats from the wild. In fact, they are only choosing phishing themes based on active threat content 15% of the time.

In this year's report, we felt it was important to highlight data about **real phishing** and phishing simulation data based on samples plucked from the wild. If you are starting the journey to condition your users' resiliency, our list of Top 10 active threats is a smart place to start. While human behavior data in cybersecurity is exciting, we must be mindful of the ultimate goal: **stopping actual phishing attacks**.

TEN RECOMMENDATIONS

1. Concentrate on conditioning users to report, not simply to recognize and resist sketchy emails. The high reporting volumes shown in our data prove that trained users make good intelligence agents .
2. Run phishing simulations based on active threats. Focus on actual threats your organization faces. If you're unsure, ask your SOC team.
3. A different perspective on that last point: in building a phishing awareness program, favor quality over quantity. Be selective in the threats you ask your users to know and report. If they're resilient to the most pressing threats, you can't ask for more.
4. With credential phishing still the most active category, educate your users to be careful with their logins. Also, require two-factor authentication for users with access to high-value data.
5. On a related note, make sure your users know what a real email looks like; communicate corporate email formats so people can spot a fake and lower your vulnerability to compromised email accounts.
6. Financial transactions are popular subjects/themes for phishing emails. They work. Include plenty of these in your awareness program and be sure to target finance and other departments that disburse funds.
7. As you measure improvements in recognition and reporting, aim for an initial ratio of 1 reported email to 1 susceptible user.
8. Your anti-phishing program must keep up with the newest subjects/themes. Hackers never rest.
9. Make use of automation to remove reported spam and streamline email analysis.
10. The constant evolution in phishing techniques shows that focusing on the "known bad" is hardly good enough. Security appliances and software geared to fight known threats create a gap that hackers happily exploit.

RECOMMENDED READING

National Institute of Standards and Technology, User Context: An Explanatory Variable in Phishing Susceptibility, 2018: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/07/usec2018_01-2_Greene_paper.pdf

ABOUT COFENSE

Cofense™, formerly PhishMe®, is the leading provider of human-driven phishing defense solutions world-wide. Cofense delivers a collaborative approach to cybersecurity by enabling organization-wide engagement to active email threats. Our collective defense suite combines timely attack intelligence sourced from employees with best-in-class incident response technologies to stop attacks faster and stay ahead of breaches. Cofense customers include Global 1000 organizations in defense, energy, financial services, healthcare and manufacturing sectors that understand how changing user behavior will improve security, aid incident response and reduce the risk of compromise. To learn more, visit https://cofense.com/.

SOURCES

1. Verizon, Data Breach Investigations Report, 2018.
2. Symantec, Internet Security Threat Report, 2018.
3. Ponemon Institute, Cost of a Data Breach Study, 2018.
4. RevisionLegal.com, 2017.
5. HipaaJournal.com, 2018.
6. Cofense blog, Sep. 13, 2018.