proofpoint®

AUTUMN 2018

PROTECTING PEOPLE

A Quarterly Analysis of Highly Targeted Cyber Attacks

proofpoint.com

NOT EVERYONE IN YOUR ORGANIZATION IS A VIP.

But anyone can be a VAP: Very Attacked Person™

And these VAPs aren't always the people you expect. That's because today's attacks target users in countless ways, across new digital channels, with objectives that aren't always obvious.

They trick your workers into opening an unsafe attachment or clicking on a dubious web link. They impersonate your CEO and order your finance department to wire money. And they con your customers into sharing login credentials with a website they think is yours.

Protecting against today's threats starts with understanding who's being targeted by them and how they're being attacked.

This report presents data gathered between July–September 2018, along with previously collected data for historical comparisons. We examine which employees and organizational departments receive the most highly targeted email threats. Then we explore how they're being attacked, analyzing attackers' techniques and tools.

Based on these findings, we recommend concrete steps organizations can take to build a defense that focuses on their people.

WHO'S BEING ATTACKED

Among the most targeted email addresses in the quarter, more than

99% didn't rank in our last report.

Someone who seems unappealing to attackers today can easily become a Very Attacked Person tomorrow.

Individual contributors and lower-level management accounted for

67% of highly targeted malware and phishing attacks

Attacks against executives and upper-level managers rose 4 points to about a third of all attacks.

Workers in operations and production functions represent

23% of highly targeted attacks.*

Marketing, public relations and human resources departments accounted for a larger share of these attacks vs. the previous quarter.

*malware and credential phishing

Email fraud attacks rose to

36 per targeted organization
Up 80% vs. the year-ago quarter and 4% vs. the previous quarter.

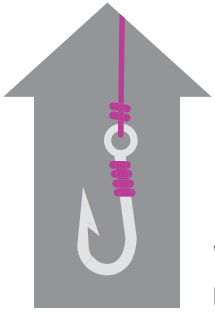
The number of spoofed identities plunged

68% vs. the previous quarter

Most companies were targeted at least once.

HOW THEY'RE BEING ATTACKED

Email-based corporate credential phishing attacks rose

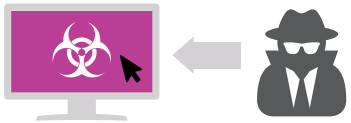


4X vs. the previous quarter.

It's too early to tell whether the spike is seasonal or represents a broader shift.

Web-based social engineering attacks jumped

233% vs. the previous quarter.



These attacks tricked users into downloading malicious software or visiting malicious or compromised websites.

Banking Trojans, downloader, credential stealer and remote-access Trojan attacks rose to

94% as a share of all malware attacks

Ransomware dropped sharply.

Customer-support fraud on social media soared

486% vs. the year-ago quarter.

These attacks, also known as **"angler phishing," use fake customer-support accounts** on social media to trick people looking for help.

SECTION 1 WHO'S BEING ATTACKED

Protecting people starts with understanding who in an organization is being attacked and why they might be targeted. That includes knowing their roles, what data they might have access to and their potential exposure.

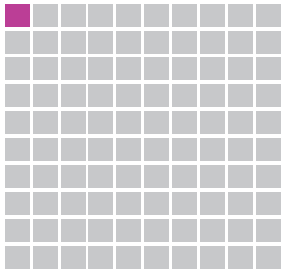
Very Attacked People

METHODOLOGY

For insight into threats focused on specific people, we examined the most highly targeted attacks against Fortune Global 500 customers. We collected the most-targeted email addresses (determined by our Very Attacked Person score, which factors in the quantity, severity and sophistication of threats received) in each company. Then we found the recipients' titles and functions using social-media profiles, internet databases, public records, news stories and other sources. We excluded dummy accounts and email addresses of cybersecurity teams and vendors.

Attackers try to compromise people at all career levels. And their targets are always changing.

A whopping 99% of email addresses identified as the most highly targeted recipients did not rank as such in our last report. This is a dramatic shift, even factoring in normal employee turnover (11% on average worldwide, according to a recent LinkedIn study[1]). The change suggests that attackers are constantly shifting focus. Someone who seems unappealing to attackers today may well become a Very Attacked Person tomorrow.



FRESH TARGETS

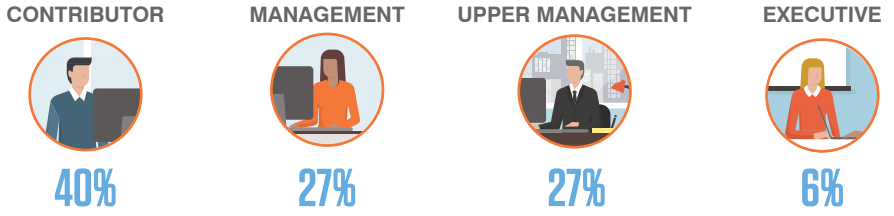
Less than 1% of email addresses identified as the most highly targeted recipients during the quarter ranked as such in our last report, reflecting attackers' shifting focus.

As a group, individual contributors and lower-level management account for about 67% of highly targeted malware and phishing attacks, a slight drop vs. the previous quarter.

Attacks against upper managers and executives rose to about a third of all such attacks, a 4-point jump vs. the previous quarter. Given that upper management represents a smaller proportion of the total workforce, the figure suggests that board members, C-level executives, directors, and department heads are targeted disproportionately more often than other people.

Highly Targeted Employees

As a group, lower-level employees receive 67% of highly targeted attacks. But C-level executives, directors, department heads may be targeted disproportionately more often.

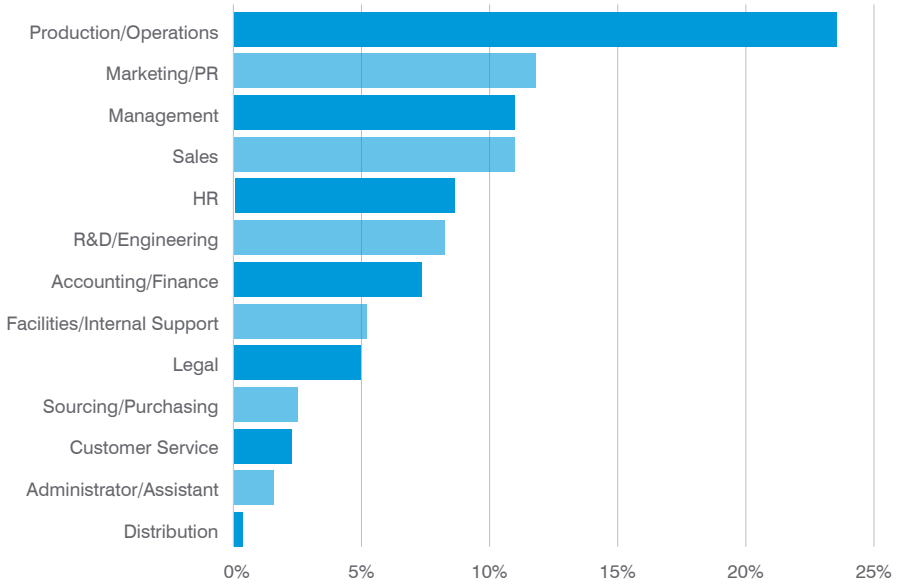


By department, workers in operations and production functions are the most exposed, representing 23% of highly targeted attacks, roughly the same as the previous quarter.

1 Michael Booz (LinkedIn). "These 3 Industries Have the Highest Talent Turnover Rates." March 2018.

At the same time, workers in marketing, public relations and human resources departments represented a significantly larger share of these attacks vs. the previous quarter. Together, they accounted for about a fifth of all highly targeted malware and phishing attacks.

Highly Targeted Departments
Employees involved in companies' main operations are the most highly targeted, followed closely by administration and engineering.



Industries targeted by email fraud

Overall, the number of email fraud attacks rose to 36 per targeted organization on average. That's an 80% increase vs. the year-ago quarter and 4% over the previous quarter.

As in previous quarters, we saw no correlation between an organization's size and how likely it is to see an email fraud attack—email fraudsters are equal-opportunity attackers.

By its nature, email fraud targets specific companies and recipients. It works by impersonating someone the recipient knows and trusts. The attacker may request a wire transfer or sensitive information. In either case, the order looks like an everyday business request.

METHODOLOGY

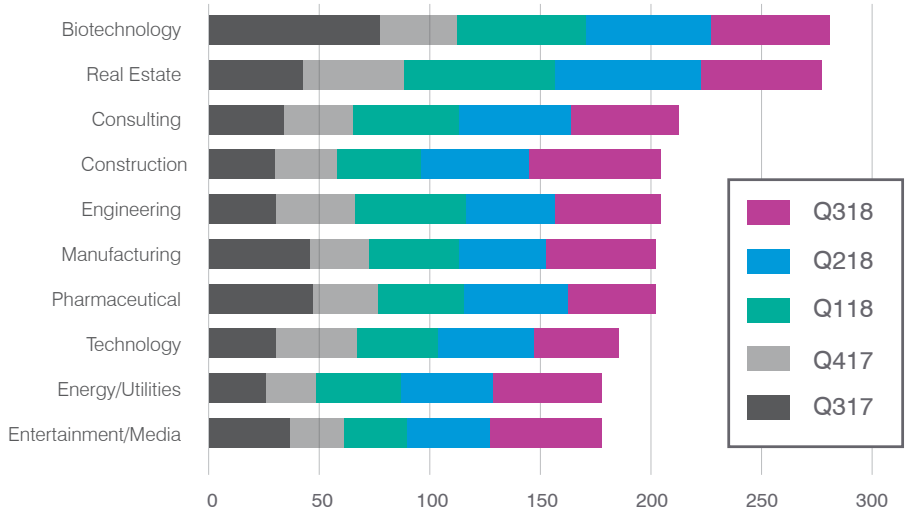
We compiled email fraud attempts detected by our email classification engine, which protects customers around the world. We correlated those attacks to company size and industry category to determine what kinds of companies are most targeted. We also examined the emails to analyze attackers' techniques.

ATTACKS BY INDUSTRY

Drug makers were the most targeted industry in the quarter at 71 email fraud attacks per company on average. (The sector also saw the largest quarterly increases and one of the largest year-over-year surges, as shown in the following section.)

Construction companies were close behind at 61 attacks per company. Real estate companies averaged 54 attacks. Looking back over cumulative email fraud attacks over the last five quarters, companies in the sector encountered nearly 282 email fraud attacks on average, higher than any other industry. Real estate was close behind with 277 attacks per company.

Attacks by Industry
Biotech, medical device makers and real estate firms are targeted with email fraud more than other industries.



Fraudsters ramp up attacks against retail, public sector, and media

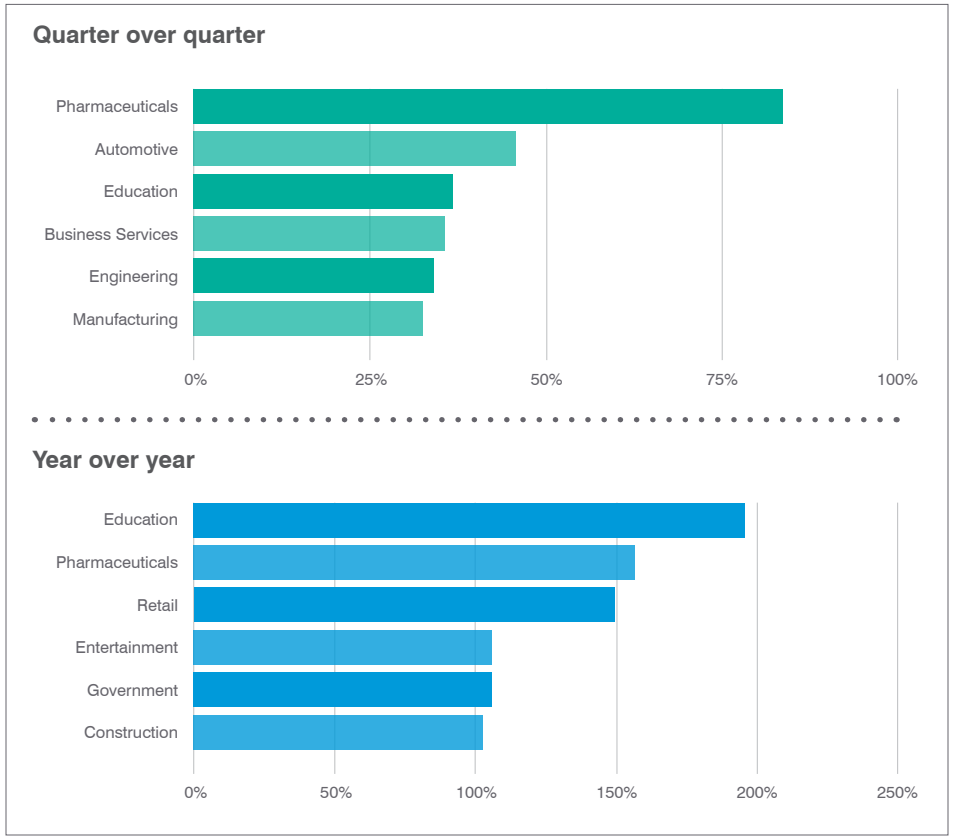
The education sector saw the biggest year-over-year increase as email fraud attacks soared 192% to 40 attacks per organization on average. Drug makers were close behind with a 149% increase. Attacks against retailers grew 144% to about 50 attacks per company.

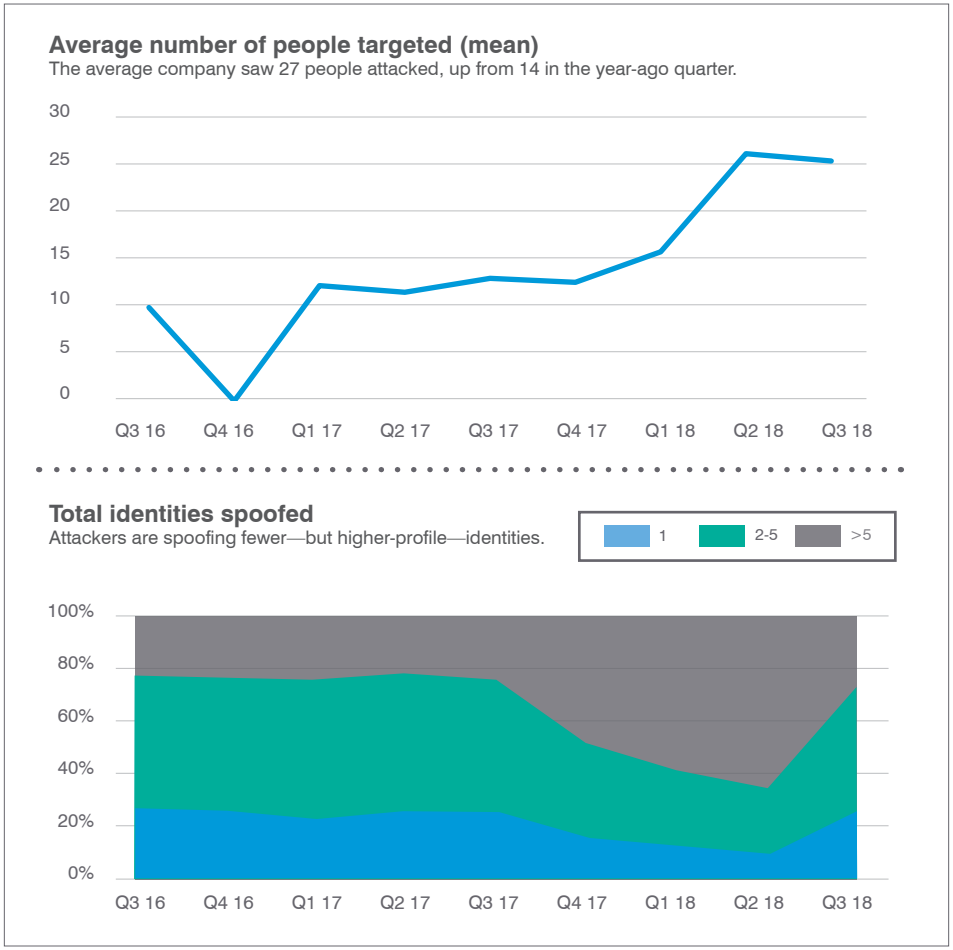
People targeted

Email fraud starts when an attacker impersonates, or spoofs, someone else—usually someone the victim knows or is inclined to trust. In recent quarters, attackers had been spoofing more and more people, suggesting that fraudsters were trying new ways to target recipients.

That's changing. In the most recent quarter, the number of identities spoofed fell 68% vs. the previous quarter even as overall email fraud volume rose. The shift suggests that spoofing a wider range of identities didn't bear fruit. Now attackers have returned to the tried-and-true tactic of spoofing people who wield the greatest authority.

At the same time, the number of recipients targeted by email fraud continues to rise. Amid a small seasonal dip, the average number of people targeted nearly doubled from the year-ago quarter to 27.





SECTION 2 HOW THEY'RE BEING ATTACKED

Protecting people also means understanding how they're being attacked. This includes the volume of attacks, who's attacking, and what techniques and tools they use.

METHODOLOGY

Our real-time data that spans email, social media and cloud apps to correlate threat intel from more than 5 billion daily emails, 200 million social media accounts, and 250,000 daily malware samples. We use this insight to understand how people are attacked to better protect them.

Credential phishing skyrockets

Credential phishing soared 300% vs. the previous quarter, though it's too early to say whether the spike represents a seasonal blip or lasting trend.

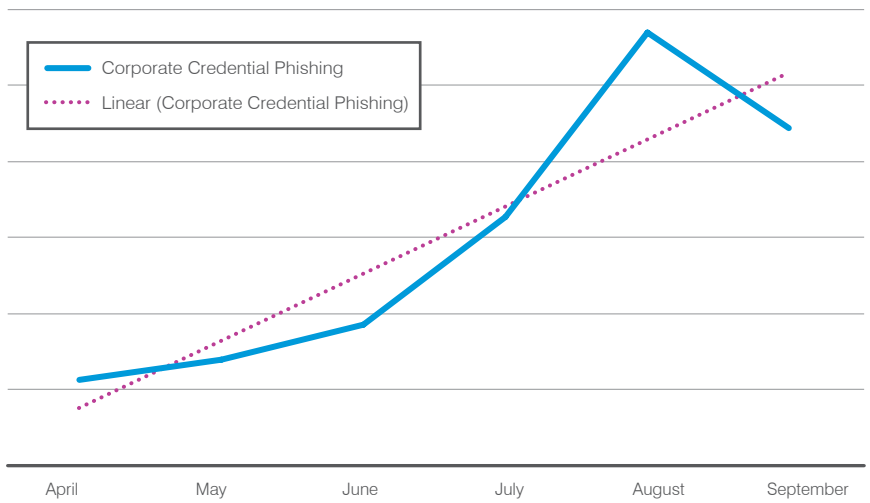
By stealing users' credentials, attackers get access to all the sensitive data those users have access to and can impersonate them for future attacks.

URL-based attacks far outstrip attachment-based attacks

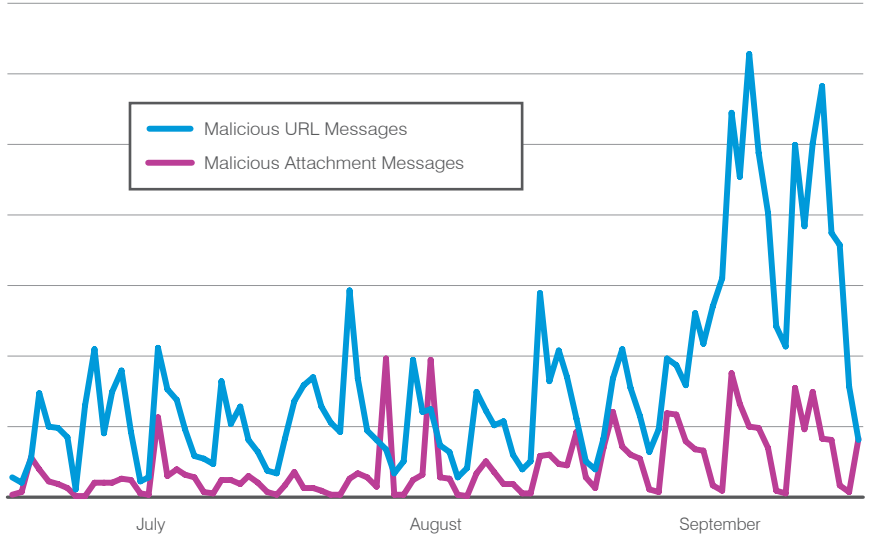
Whether they use malicious file attachments or URLs that lead to unsafe files and websites, email remains the top vector for malware and phishing attacks.

As has been the case for most of 2018, URL-based email attacks far outnumbered attachment-based attacks, though volumes surged for both types.

Credential phishing volume
Credential phishing soared 300% vs. the previous quarter.



Malicious message volume
URL-based attacks far outstripped attachment-based attacks for most of the quarter.



Ransomware fades as payloads diversify

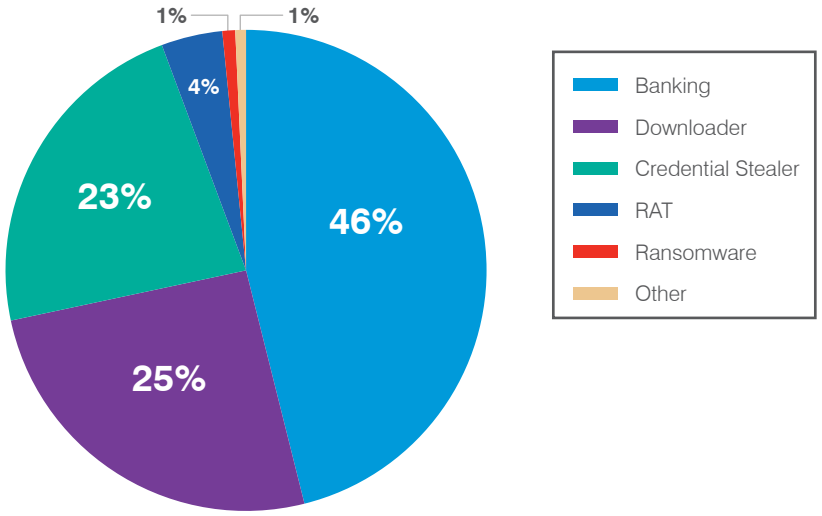
A range of banking Trojans, credential stealers, and downloaders appeared in both large and small campaigns. Ransomware represented just 1% of all payloads, a 10-point drop from the previous quarter.

Ransomware, which locks away victims' data until they pay to get it back, is anything but subtle. Organizations know when they've been attacked—the whole point is to be as disruptive as possible and get a quick payout. Other types of malware, by contrast, are designed for stealth. The longer they go undetected, the more value they can extract from their victims.

The growing prevalence of stealthier malware such as RATs and bankers (see "Malware crib sheet") represents a continued shift towards large investment, large return campaigns. Attackers appear to be seeing greater rewards for investing the time and effort into monitoring and managing hosts infected with malware designed stay hidden and exploit victims on an ongoing basis.

Malware mix

A range of banking Trojans, credential stealers, and downloaders appeared in both large and small campaigns.



MALWARE CRIB SHEET

HERE ARE COMMON TYPES OF MALWARE AND WHAT THEY DO.

BANKER
Steals victims' bank login credentials

DOWNLOADER
Gains a foothold on a targeted system to download other malware components

CREDENTIAL STEALER
Steals users' account credentials

RAT (REMOTE ACCESS TROJAN)
Gives attacker total control over the compromised system

RANSOMWARE
Locks away victims' data until they pay a "ransom" to unlock it

Email fraud techniques

Email fraudsters use a range of techniques to trick recipients into opening the email and acting on it. These include subject lines, spoofing trusted senders and choosing the right targets.

SUBJECT LINES

Email fraudsters tried to convey a greater sense of urgency in the quarter by making their requests timebound and warning employees of consequences for any delay. "Request," "urgent" and "payment" were the top three subject lines, together accounting for 58% of all email scams. That's up from 48% the previous quarter.

At the same time, we saw a 549% increase in payroll-related scams quarter over quarter, though they still represent a small fraction of the total volume.

DISPLAY-NAME SPOOFING

More than 99% of all fraudulent emails used a spoofed display name, up from 90% in the previous quarter.

In many cases, email fraud attacks use the technique in tandem with other methods such as domain spoofing. The display name is what appears in the email's "From:" field. It's unrelated to the sender's actual email address or where any replies are sent—it can be anything. In display-name spoofing, the attacker uses a familiar name and email address to gain the recipient's trust.

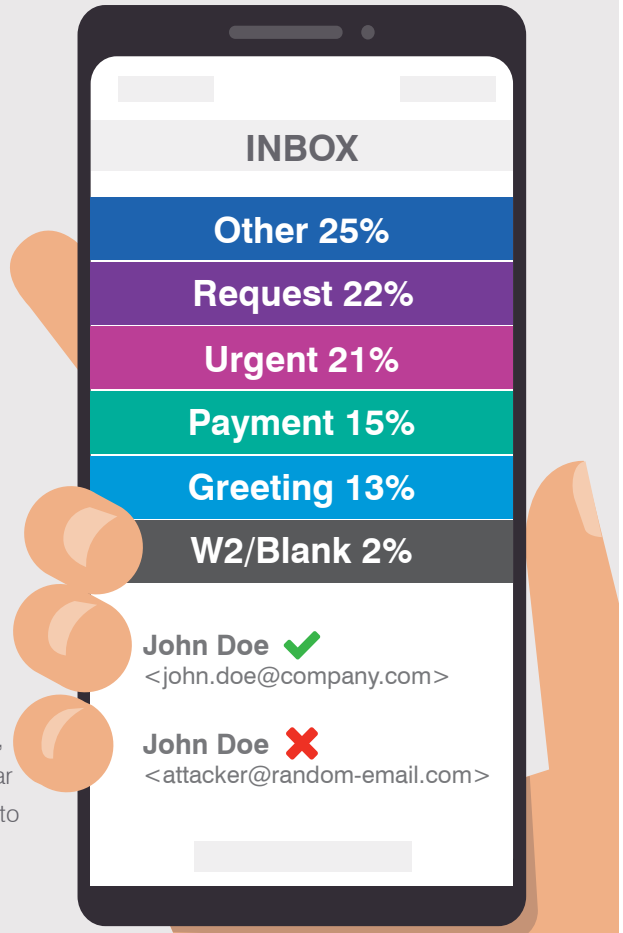
Given that display name is the easiest email identifier to spoof and the most visible to recipients, it's easy to see why most email fraud attacks use the technique.

Email Fraud Subject Lines

Email fraudsters tried to convey a greater sense of urgency in the quarter with subject lines such as "Request," "urgent" and "payment."

Display-name spoofing

In display-name spoofing, the attacker uses a familiar name and email address to gain the recipient's trust.



Social media attacks

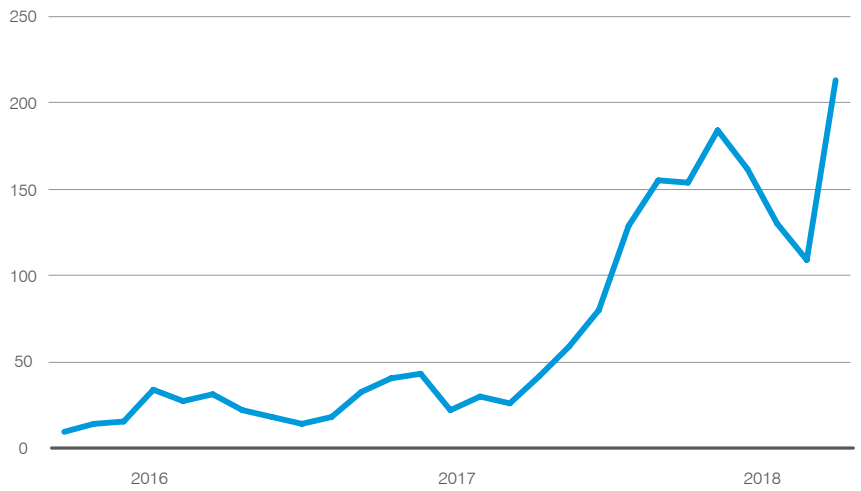
METHODOLOGY

Using our social fraud protection solution, we examined social media accounts that used the name or likeness of our global customer base and any phishing URLs they propagated.

Social media channels remain key vectors for fraud and theft. Twitter, Facebook and others continue to develop automated protections, which has cut phishing links by 90% vs. a year ago. But customer-support fraud, also known as "angler phishing," remains a key challenge.

Customer-support fraud on social media soared 486% vs. the year-ago quarter to its highest level ever. These attacks use create fake customer-support accounts on social media to trick people looking for help into visiting a phishing site or providing account credentials.

Fraudulent customer-support accounts on social media
Customer-support fraud on social media soared 486% vs. the year-ago quarter to its highest level ever.



Web-based attacks

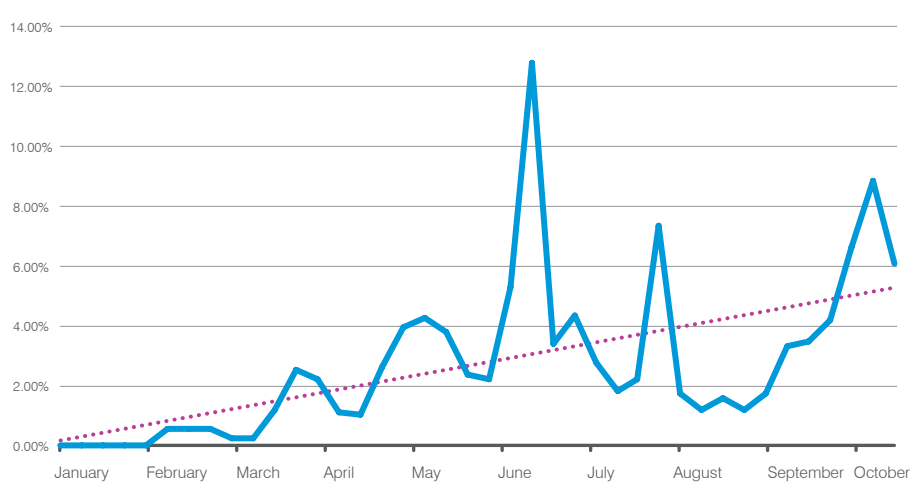
METHODOLOGY

Using our global network of intrusion detection systems (IDS), we studied attack techniques to identify vulnerabilities that are being exploited and new social-engineering schemes.

The volume of social-engineering attacks on the web—which trick people with fake antivirus notifications and software updates—rose 233% vs. the previous quarter. The increase comes on the heels of a ninefold increase in such attacks in the previous quarter vs. the quarter before.

Such attacks lead to malware downloads, phishing sites and more. These include sites running Coinhive, JavaScript code that hijacks visitors' computers to mine cryptocurrency. After falling from summer peaks, Coinhive activity rebounded in the latest quarter, though short of its June peak.

Percentage of intrusion events caused by Coinhive
Coinhive activity rebounded in the latest quarter.



SECTION 3 HOW TO PROTECT THEM

Threats that target people require a people-centric cybersecurity strategy. We recommend the following as a starting point:

ADOPT A SECURITY POSTURE FOCUSED ON PEOPLE.

Attackers do not view the world in terms of a network diagram. Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.

TRAIN USERS TO SPOT AND REPORT MALICIOUS EMAIL.

Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into current trends and the latest threat intelligence.

AT THE SAME TIME, ASSUME THAT USERS WILL EVENTUALLY CLICK SOME THREATS.

Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. And stop outside threats that use your domain to target customers.

BUILD A ROBUST EMAIL FRAUD DEFENSE.

Email fraud can be hard to detect with conventional security tools. Invest in a solution can manage email based on custom quarantine and blocking policies.

PROTECT YOUR BRAND REPUTATION AND CUSTOMERS IN CHANNELS YOU DON'T OWN.

Fight attacks that target your customers over social media, email and the web—especially fake accounts that piggyback on your brand. Look for a complete social media security solution that scans all social networks and reports fraudulent activity.

PARTNER WITH A THREAT INTELLIGENCE VENDOR.

Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques to detect new attack tools, tactics, and targets—and then learns from them.

LEARN MORE

To learn more about what a people-centric approach looks like in practice, watch our webinar.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations 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 organizations 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.