proofpoint

WINTER 2019

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 and 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 and how they're being attacked.

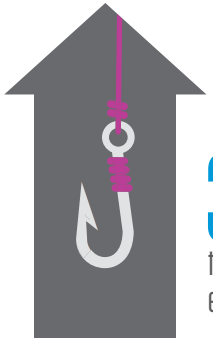
This report presents data gathered between October–December 2018, along with previously collected data for historical comparisons. We examine which employees and organizational departments receive the most highly targeted email threats. Then we explore how they're being attacked, analyzing attackers'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

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

Note: Our data was collected from customer deployments in a given quarter. In some cases, historical comparisons may include data from overlapping—but not identical—sets of customers.

WHO'S BEING ATTACKED

Among the most targeted malware and credential phishing attacks, nearly

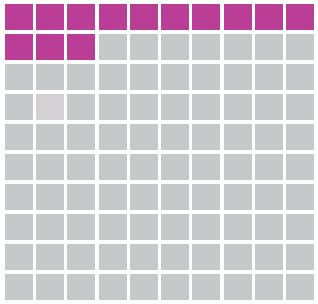


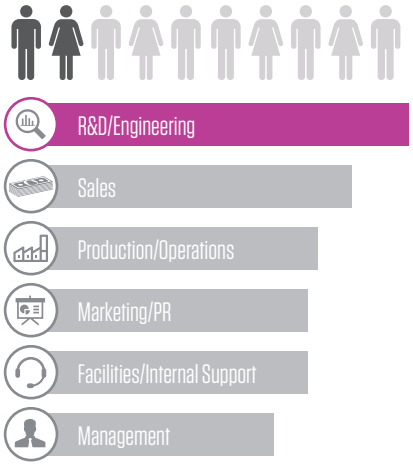
30%
targeted generic email aliases.

These email addresses are typically shared within an organization.

13% of email addresses identified as the most highly targeted recipients

during the quarter ranked as such in our last report, reflecting attackers' shifting focus.





Workers in R&D and engineering were targeted the most heavily.

Your VAPs aren't always your VIPs.

Among organizations' Very Attacked People, lower-level workers were at even more risk than those in higher-level roles.

HOW THEY'RE BEING ATTACKED

Among organizations targeted by email spoofing, nearly

60%
saw attempts that spoofed more than five identities.

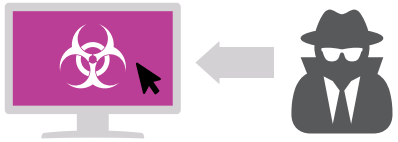
Nearly 80% were targeted in attacks that tried to send email to six or more people.

Among organizations targeted by email spoofing, more than

40%
were the intended recipients of 50 or more fraudulent emails.

That's 4x the year-ago percentage.

Web-based attacks that use social engineering grew



150%
vs. the previous quarter.

Fraudulent social media support account phishing, jumped

442%
vs. the year-ago quarter.

Unless otherwise indicated, figures represent the October-December 2018 quarter.

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.

Get to know your VAPs

METHODOLOGY

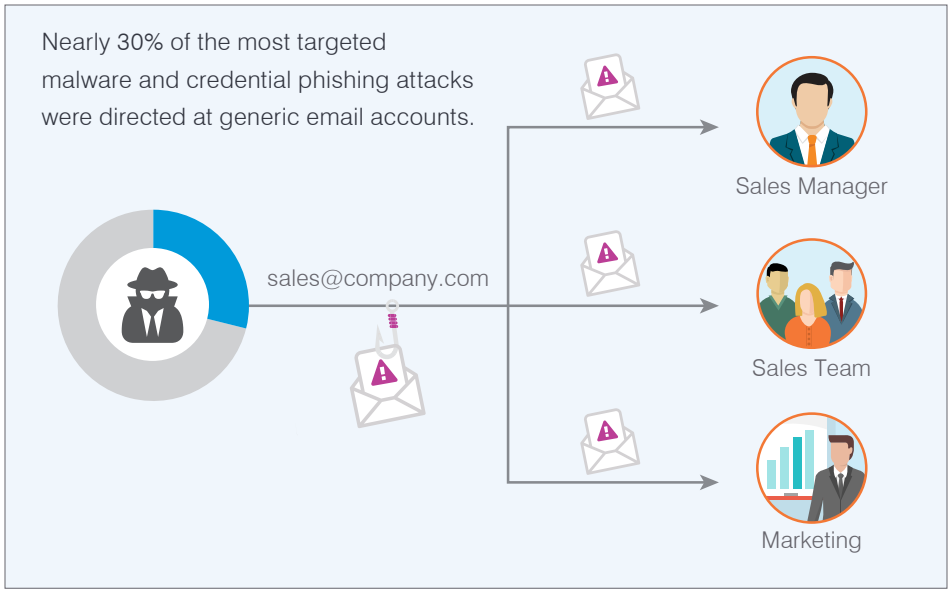
For insight into threats focused on specific people, we examined the most highly targeted attacks against Fortune Global 500 customers. We collected the most-targeted email addresses (determined by our Very Attacked Person score, which factors in the quantity, severity and sophistication of threats received)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

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

SHARED EMAIL ALIASES

Nearly 30% of the most targeted malware and credential phishing attacks were directed at generic email accounts typically shared by two or more employees within an organization. Addresses such as sales@company.com and inquiries@company.com have value to attackers for three main reasons:

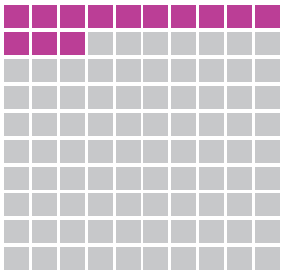
- They are sent to multiple victims.
- They are easy to obtain (often public-facing).
- They are harder to protect—multifactor authentication, for instance, doesn't work well with email addresses shared among several colleagues.



SHIFTING FOCUS

A full 87% of the most attacked email addresses did not rank as such in our previous report. This figure is yet another signal that attackers are constantly shifting focus. Someone who seems unappealing to attackers today can easily become a VAP tomorrow.

(While this number is lower than the 99% figure last quarter, the newest percentage includes shared email addresses for the first time.)



FRESH TARGETS

Just 13% of email addresses identified as the most highly targeted recipients during the quarter ranked as such in our last report, reflecting attackers' shifting focus.

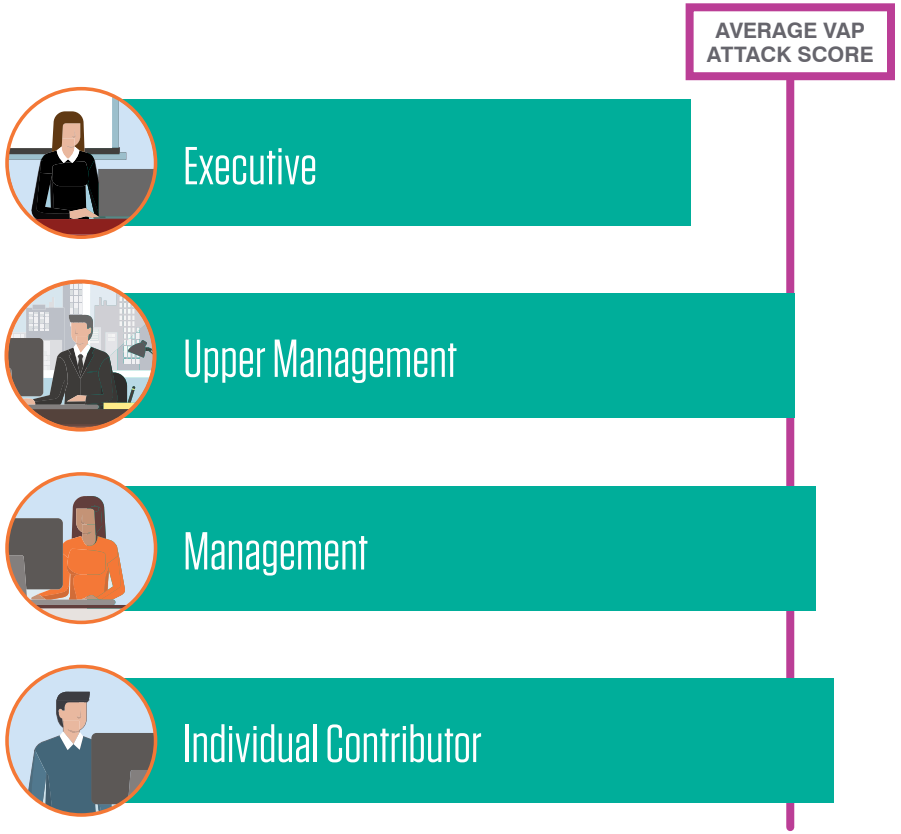
VAPS AREN'T ALWAYS VIPS

Among organizations' VAPs, lower-level workers were targeted slightly more heavily than upper-management and executives. (We measure these levels using an aggregate score that factors in the volume and concentration of the attacks as well as the sophistication of the attacker.) In other words, people at the bottom of the corporate ladder were even more at risk than those at the top. This gap underscores a simple truth: your VAPs aren't always your VIPs.

SOME DEPARTMENTS ARE MORE TARGETED THAN OTHERS

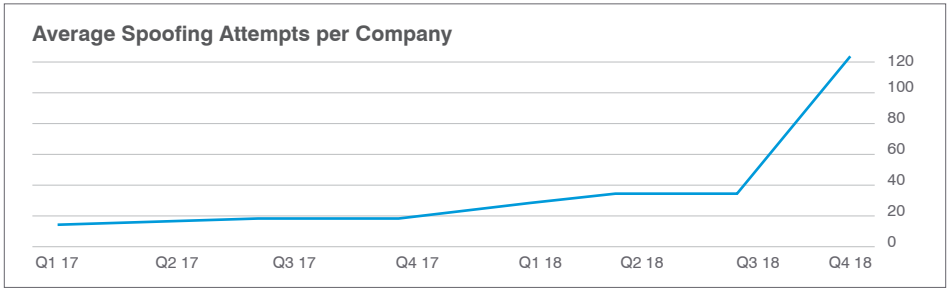
Among organizations' Very Attacked People, workers in R&D/engineering and sales departments were the most targeted (30% more heavily and 15% more heavily, respectively, than the average VAP).

AVERAGE VAP THREAT SCORE BY MANAGEMENT LEVEL



AVERAGE VAP THREAT SCORE BY FUNCTION

Overall, email spoofing soared, with the number of attacks per company up 944% on average vs the year-ago quarter. As in previous quarters, we saw no correlation between an organization's size and how likely it was to see a spoofing attack—email attackers are equal-opportunity attackers.



SPOOFING

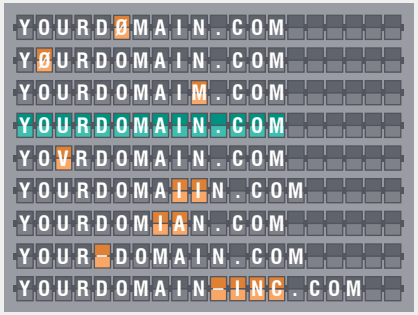
Cyber attackers target people in countless ways using an array of tools, tactics, and approaches. But all people-focused attacks have one thing in common: they rely on identity deception.

They trick victims into opening a malicious attachment, clicking an unsafe link, entering account credentials, sending sensitive files or wiring money by pretending to be someone the victim knows or is likely to trust. In email attacks, identity deception usually involves some form of spoofing. Here are three types and how they work:

DOMAIN SPOOFING

Domain spoofing is shockingly easy. Anyone with a mail server can define what appears in the email's "from" and "reply to" headers—even domains they don't own. Attackers often send email from a well-known or trusted domain so that recipients are more likely to take the bait.

Authentication controls such as DMARC can help ensure that only someone from your company—or someone you authorize—can send email using your domain. This stops many domain-spoofing attacks in their tracks.

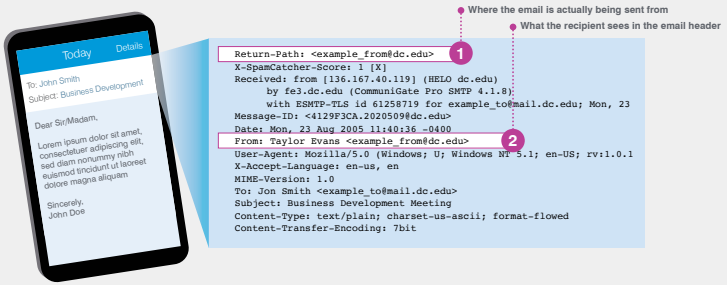


LOOKALIKE DOMAIN SPOOFING

But even with authentication, it's easy for attackers to register domains that look a lot like yours. This tactic is sometimes called "typosquatting."

Some lookalike domains may swap out characters, such as the numeral "0" for the letter "O", an uppercase "I" for a lowercase "L", or a "V" for a "U." Others might insert additional characters, such as an "S" at the end of the domain name, that a casual viewer won't easily notice.

There are endless combinations fraudsters can use to counterfeit trusted email domains. And unless your organization has registered them all, DMARC alone won't stop them. For these attacks, you need a solution that finds lookalikes and helps you shut them down.



DISPLAY-NAME SPOOFING

No matter what other tactics they use, most attackers spoof the sender display name in fraudulent emails.

The display name is what appears in the "From:" field when reading the message. It's unrelated to the sender's actual email address or where any replies are sent—it can be anything.

To stop these attacks you need a solution that can detect display-name spoofing in the content of email messages and block them at the source.

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 correlates 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.

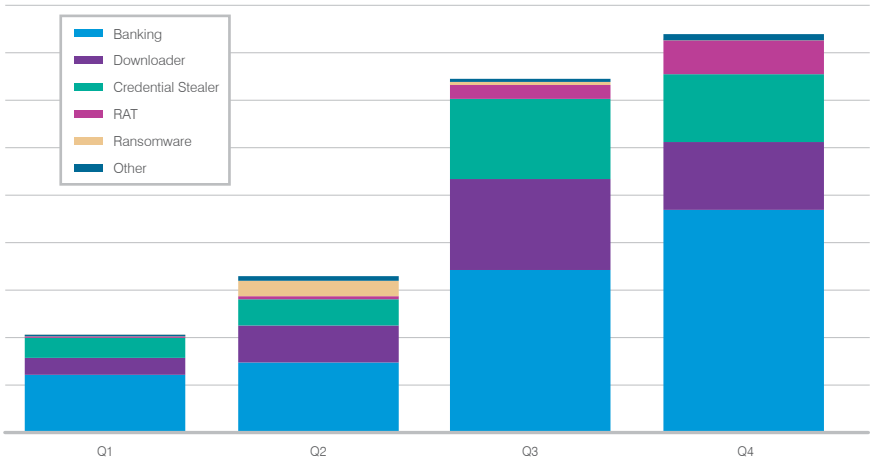
Malware

Banking Trojans remained the top email-borne threat. They made up 56% of all malicious malware payloads, led by a strain called Emotet.

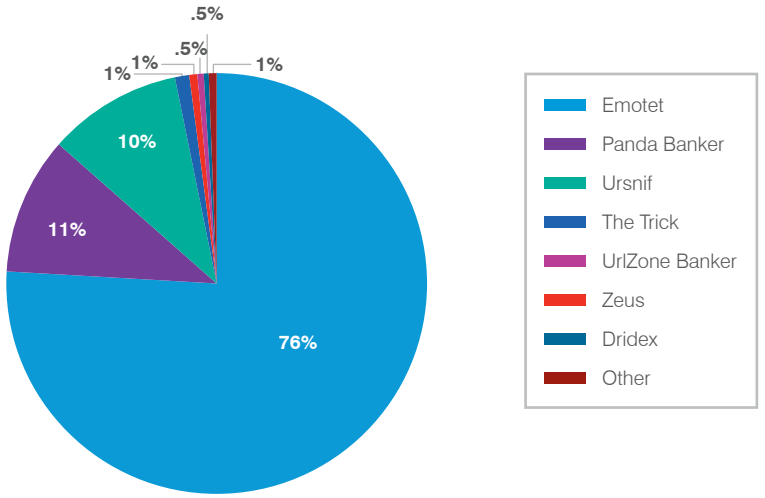
Coinhive, JavaScript code that co-opts victims' computers to harvest electronic currency, spiked in December. It's not clear whether this represents a seasonal spike or broader trend.

FOR MORE ON COINHIVE AND EMOTET, SEE OUR Q4 QUARTERLY THREAT REPORT.

Message Volume by Malware Family



Relative Volume of Banking Trojan Campaigns, Q4 2018



MALWARE CRIB SHEET

HERE ARE COMMON TYPES OF MALWARE AND WHAT THEY DO.

BANKER/BANKING TROJAN
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

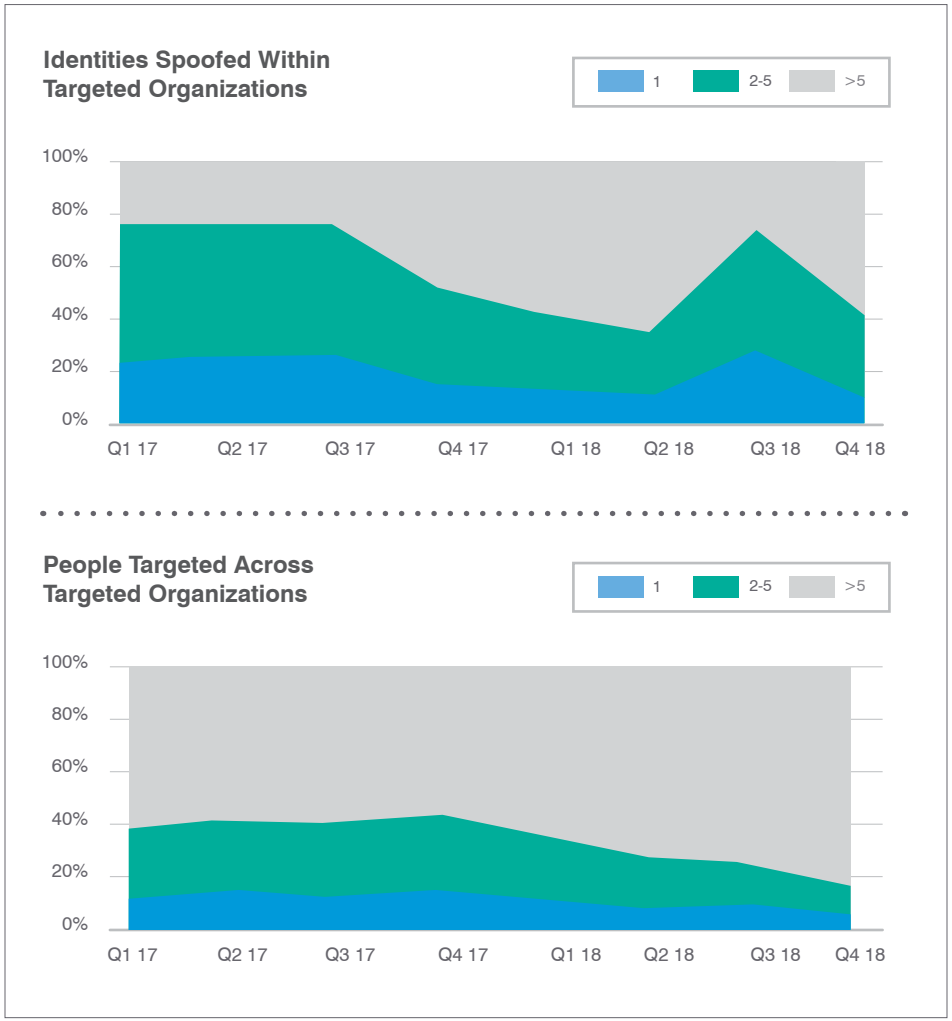
RANSOMWARE
Locks away victims' data until they pay a "ransom" to unlock it

Email fraud techniques

Email fraudsters use a range of techniques to trick recipients into opening the email and acting on it. These include spoofing trusted senders and choosing the right targets. On that front, email fraud attacks are both impersonating and targeting more people.

Among organizations targeted in such attacks, nearly 60% were the intended recipients of attempts that spoofed more than five identities. That's a shift from the previous quarter, when attackers focused more on spoofing fewer, higher-authority identities.

At the same time, nearly 80% of targeted organizations were on the receiving end of attacks that tried to send spoofed email to six or more people, extending a yearlong trend.



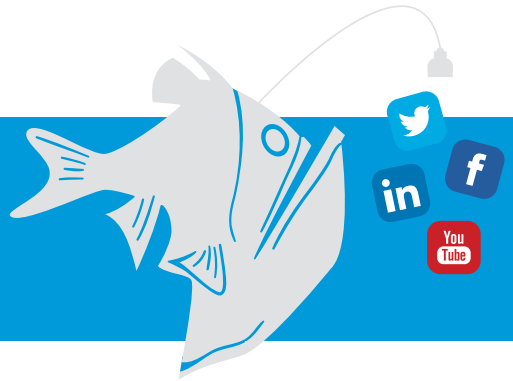
Social media attacks

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, despite the best efforts of Twitter, Facebook and others continue to develop automated safeguards. These efforts have dramatically reduced phishing links on their platforms. But customer-support fraud, also known as "angler phishing," remains a key challenge.

Accounts suspected of being created for support fraud—also known as "angler phishing"—accounts increased about 40% over the previous quarter.



HOW ANGLER PHISHING WORKS

Named after the anglerfish—known for its luminous fleshy lure that draws prey into striking distance—angler phishing has endured as a major threat on social media.

HERE'S HOW IT WORKS:

- Cyber criminals create highly convincing customer service accounts and then wait for your customers to reach out to your brand with a help request. Automated listening tools make it easy for criminals to monitor your social accounts to find a potential victim. They often strike on evenings or weekends when your customer service teams are less likely to monitor the account for requests.
- When the fraudster sees a customer contact your brand account, they spring into action and send a reply from the lookalike support account.
- The criminal assures your customer they'll resolve the problem and directs them to a lookalike website. There, the customer is invited to log in. By doing so, the customer inadvertently hands account credentials and sensitive data to the criminal.

Social engineering on the web

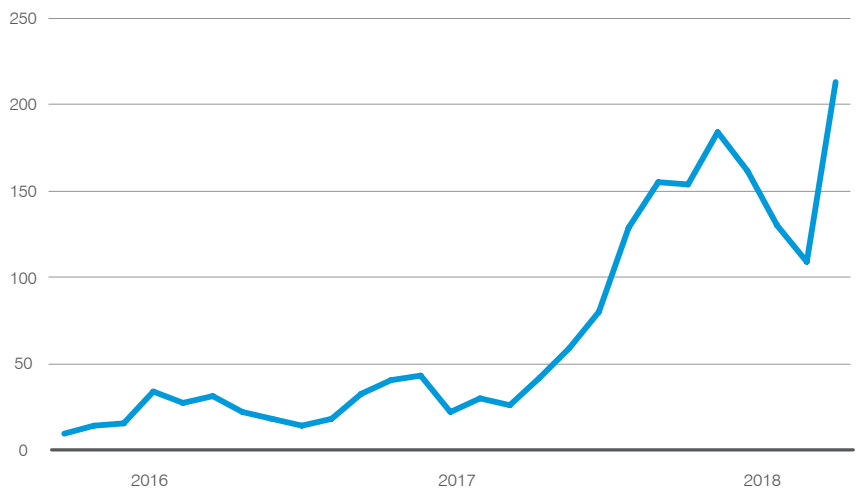
METHODOLOGY

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.

Web-based attacks that use social engineering grew 150% vs. the previous quarter. These attacks trick users into downloading malware or visiting a phishing site through fake antivirus notifications and software updates. That surge, while sizable by most measures, has moderated from even faster growth in prior quarters.

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.



Percent of Total Social Engineering Schemes

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 PEOPLE-CENTRIC SECURITY POSTURE.

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 that 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) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.