proofpoint®

PROTECTING PEOPLE

SUMMER 2018

A QUARTERLY ANALYSIS OF HIGHLY TARGETED ATTACKS

proofpoint.com

MOST CYBERSECURITY REPORTS FOCUS ON THREATS AND HOW THEY WORK. THIS ONE IS ABOUT PEOPLE AND HOW THEY'RE TARGETED.

That's because today's attacks target people, not technology. 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 or social-media account they think is yours.

No matter how well you're managing your IT infrastructure, you can't patch your way out of attacks that target people. Human nature is the ultimate vulnerability.

Protecting against today's threats starts with understanding who's being targeted by them. In this first-of-its-kind analysis, we studied which employees and organizational departments receive the most highly targeted email threats. Then we explored how they're being attacked, analyzing attacker's techniques and tools.

This report presents data gathered April–June 2018, along with previously collected data for historical comparisons. Based on our findings, we recommend concrete steps organizations can take to build a defense that focuses on 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

Individual contributors and lower-level management account for about

60%

OF HIGHLY TARGETED ATTACKS.*

But executives and upper-level managers, which are a smaller proportion of the total workforce, received a disproportionately large share of attacks.

**malware and credential phishing*

Workers in operations and production functions are the most exposed,

REPRESENTING

23% OF HIGHLY TARGETED ATTACKS.*

**malware and credential phishing*

Overall, the number of email fraud attacks per targeted company

ROSE **25%**

from the previous quarter (to 35 on average) and

85% FROM THE YEAR-AGO QUARTER.

MOST COMPANIES WERE TARGETED AT LEAST ONCE.

HOW THEY'RE BEING ATTACKED

The volume of malicious email

INCREASED BY **36%** compared to the previous quarter

WE SAW A WIDER RANGE OF EMAIL PAYLOADS AND ATTACKERS THAN IN THE YEAR-AGO QUARTER.

Ransomware rebounded, accounting for

NEARLY **11%** OF TOTAL MALICIOUS EMAIL VOLUME.

Phishing links sent through social media

SHOT UP **30%**

The spike reversed months of decline as attackers found ways around automated remediation tools.

Customer-support fraud

JUMPED BY **39%** vs. the previous quarter and

SOARED **400%** VS. THE YEAR-AGO QUARTER

SECTION 1 WHO'S BEING ATTACKED

Protecting people starts with knowing 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.

HIGHLY TARGETED MALWARE AND PHISHING RECIPIENTS

METHODOLOGY

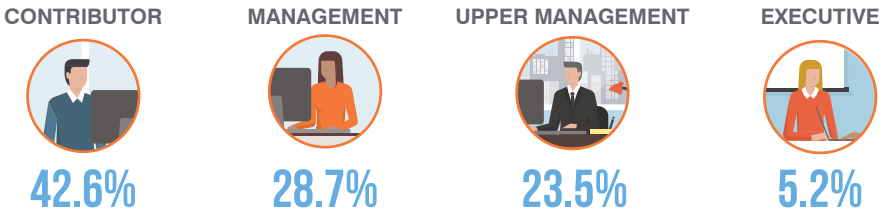
For insight into threats focused on specific people, we examined the most highly targeted attacks against Fortune Global 500 customers. We collected the most-targeted email addresses (determined by a threat score that factors in the quantity, severity and sophistication of threats received) in each company. Then we matched the recipients' title and function. To match the emails to job functions, we used social-media profiles, internet databases, news stories and other sources.

Attackers target people at all career levels. As a group, individual contributors and lower-level management account for about 60% of highly targeted malware and credential-phishing attacks. But given that upper management represents a smaller proportion of the total workforce, the figure suggests that board members, C-level executives, directors, department heads are targeted disproportionately more often.

Workers in operations and production functions, the bulk of a typical company's workforce, are the most exposed, representing 23% of highly targeted attacks. Management was the second-most exposed job function. Following closely were R&D and engineering departments.

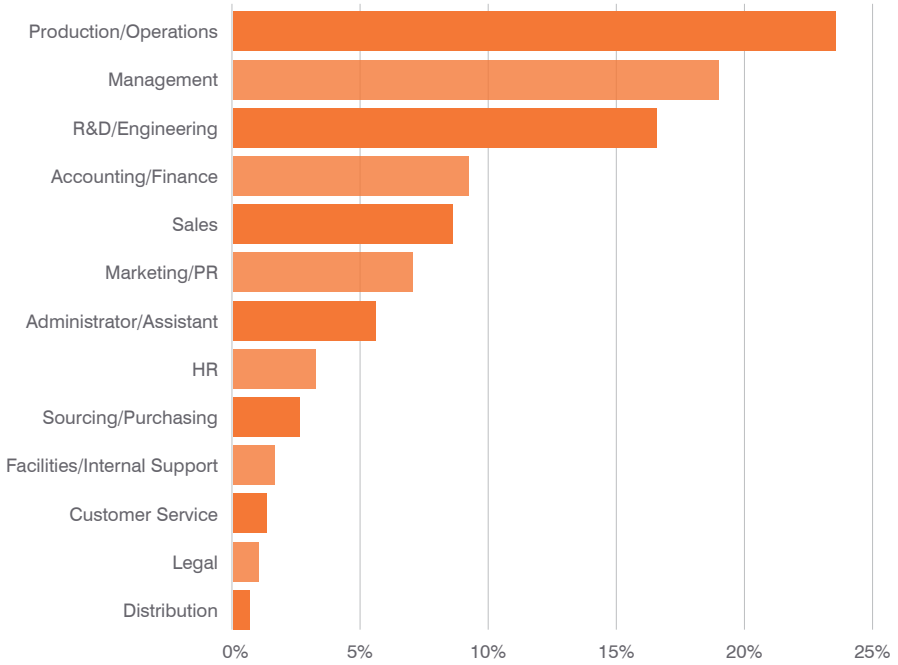
Highly Targeted Employees

As a group, lower-level employees receive 60% of highly targeted attacks. But C-level executives, directors, department heads may be targeted disproportionately more often.



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 per targeted company rose 25% from the previous quarter (to 35 on average) and 85% from the year-ago quarter. Most companies were targeted at least once.

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.

Some industries saw triple-digit increases from a year ago. The average number of email fraud attacks against automotive companies soared more than 400%. Education-related attacks jumped 250%.

We saw no correlation between an organization's size and how likely it is to see an email fraud attack—email fraudsters are an equal-opportunity attacker.

ATTACKS BY INDUSTRY

Companies across all industries are targeted with email fraud, and most saw more attacks in the second quarter than in the previous three.

For the second straight quarter, real estate firms were the most targeted, with 67 fraudulent emails sent on average. (This trend may reflect attackers trying to insert themselves in high-value, time-sensitive transactions.)

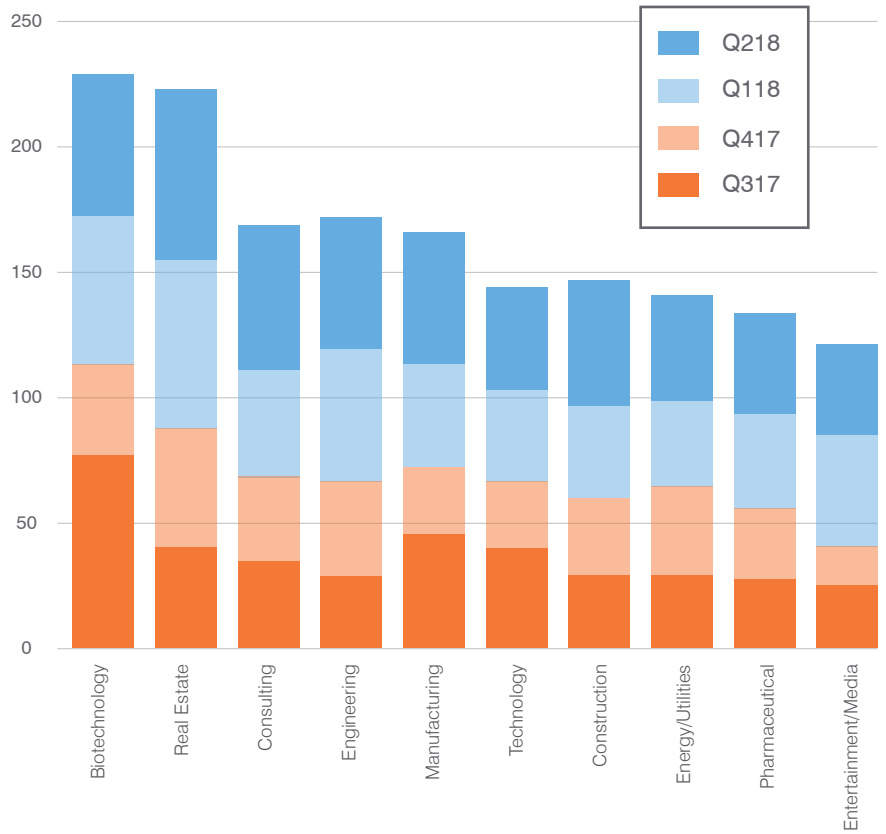
When adding up attacks over the last four quarters, biotech and medical firms were slightly more targeted as a group at 228 attacks on average.

METHODOLOGY

We compiled email fraud attempts detected by our email classification engine, which protects customers around the world. We correlated those attacks with 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

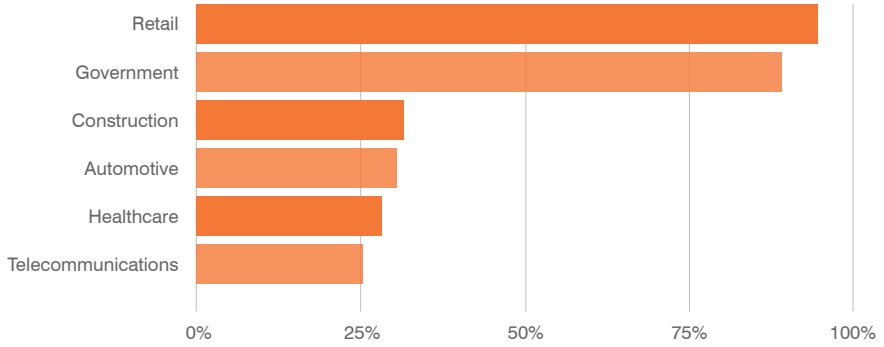
Biotech, medical device makers and real estate firms are targeted with email fraud more than other industries.



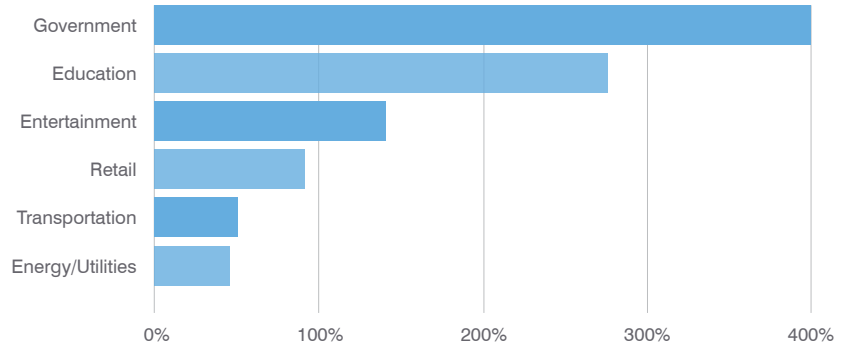
FRAUDSTERS RAMP UP ATTACKS AGAINST RETAIL, PUBLIC SECTOR, AND MEDIA

Retailers and government agencies saw huge quarter-over-quarter increases in email fraud attempts, with attacks per company soaring 91% and 84%, respectively. Year-over-year increases were even more dramatic. Attacks against government agencies more than quintupled; education, entertainment, and media companies saw triple-digit increases.

Increase vs. previous quarter



Increase vs. the year-ago quarter

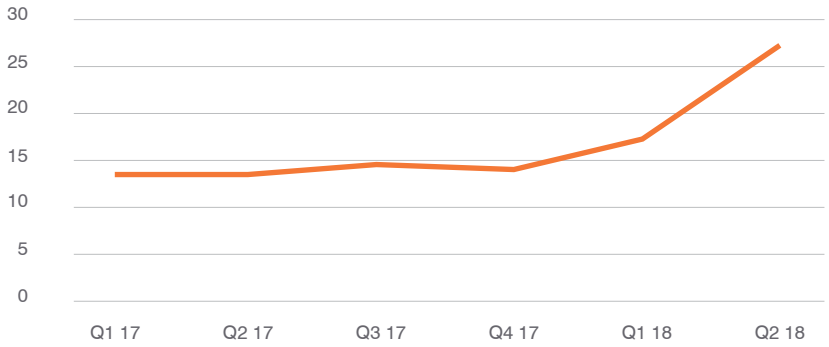


PEOPLE TARGETED

More than 65% of companies targeted by email fraud had the identities of more than five employees spoofed. That's more than triple the proportion in the year-ago quarter, suggesting that fraudsters are getting more creative and finding new ways to target. With information about employees widely and freely available, they can find multiple ways inside your environment.

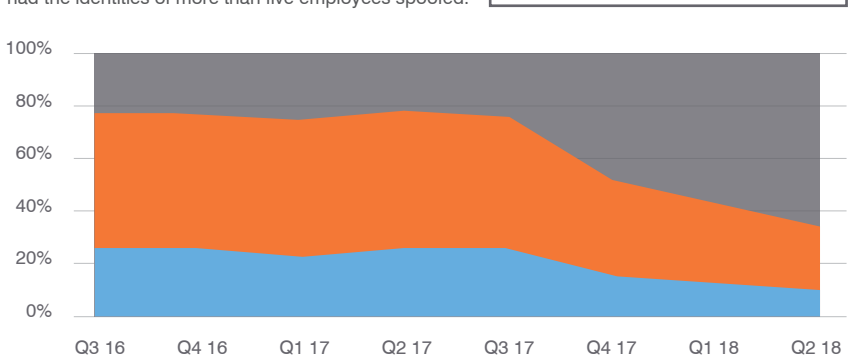
Average number targeted (mean)

The average company saw 28 people targeted, up from 17 people in the previous quarter



Total Identities Spoofed

More than 65% of companies targeted by email fraud had the identities of more than five employees spoofed.



U.S. FIRMS ARE THE BIGGEST TARGETS OF DOMAIN FRAUD

Domain fraud involves registering an internet domain that looks confusingly similar to that of a trusted company or brand. Attackers use these lookalike domains for email fraud, credential phishing, counterfeiting, and more. A lookalike email domain, for instance, may fool recipients to trust an attacker trying to steal money or sensitive information. And a lookalike web domain may look like the real thing to users entering their login credentials.

Nearly a quarter (23%) of suspicious domains that imitate top U.S. brands have active MX records, meaning they can send fraudulent emails to unsuspecting customers and employees.

English-speaking consumers and businesses are the biggest targets in attacks that use lookalike web and email domains.

METHODOLOGY

For insight into how attackers are piggybacking trusted digital brands, we used our domain monitoring and protection tool to analyze more than 350 million registrations within the global WHOIS database. We looked for any new domains that looked suspiciously like those of the top 10 global brands. We also examined how many of these domains had active mail exchange (MX) records.

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 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.

EMAIL ATTACKS SURGE

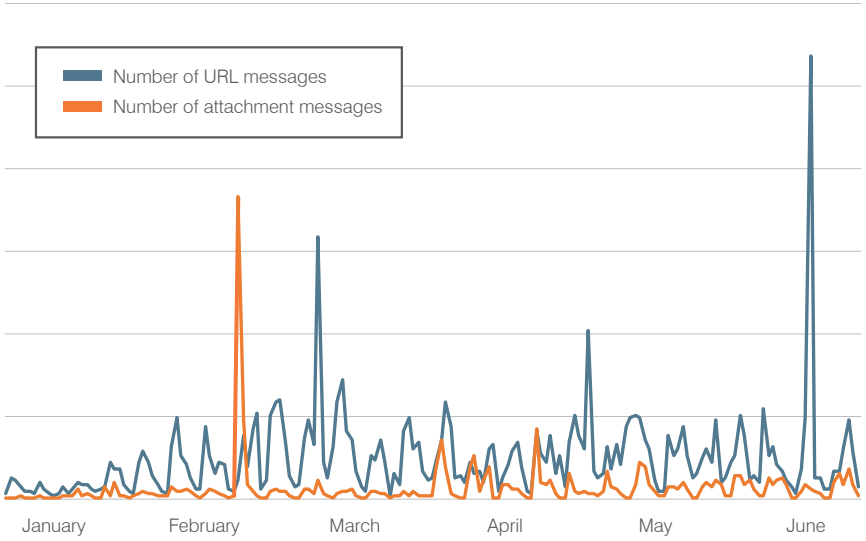
The volume of malicious email jumped 36% vs. the previous quarter buoyed by a wide range of email payloads and attackers. This diverse mix of threats is a shift from the year-ago quarter when fewer—though much larger—campaigns dominated.

Except for a large spike of attacks that used malicious attachments in February, most attacks used malicious URLs.

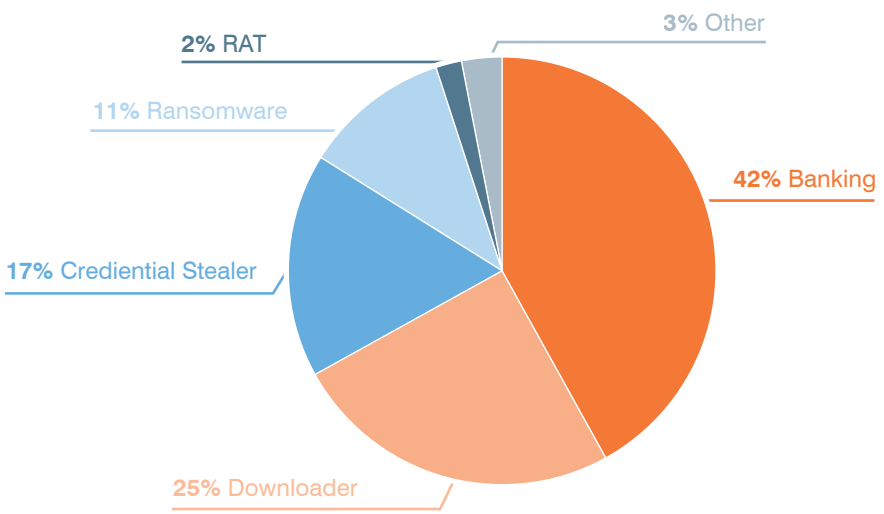
RANSOMWARE MAKES A COMEBACK

Ransomware rebounded, accounting for nearly 11% percent of the total malicious email volume. This type of malware—which locks critical data away until the victim pays a ransom to unlock it—had fallen sharply in previous quarters after dominating much of 2017.

Indexed Daily Message Volume by Attack Type
Indexed daily attack type trend



Malware by Category
Relative mix of malware payloads in email by category



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

We saw a spate of attacks in which the attacker referenced a file or document. Whether this spike is a one-time blip or the start of a trend is not yet clear.

Aside from this change, the subject lines appeared at roughly the same ratios as in previous quarters. Scams with "payment" or "request" in the subject line remain the most popular.

DOMAIN AND DISPLAY-NAME SPOOFING

Nearly two-thirds of targeted companies saw some level of abuse of their domains. This includes fraudsters sending attacks that spoofed the recipient's own employer.

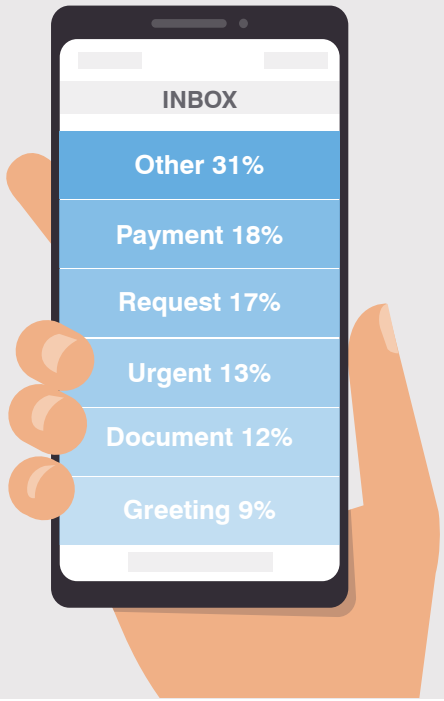
No matter what other tactics they use, most attackers spoof the sender display name in fraudulent emails.

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

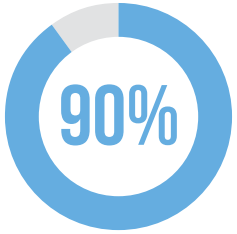
At the same time, domain spoofing appears to be falling as more companies deploy email authentication technologies such as Domain-based Message Authentication, Reporting and Conformance (DMARC).

The 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 spoof the display name, even when they're not spoofing the email domain.

Email Fraud Subject Lines
Scams with "payments or "request" in the subject line remain most popular



Display name spoofing



Most attacks use some form of display-name spoofing

Email domain spoofing

DROPPED TO **18%**

OF ALL EMAIL FRAUD ATTACKS AS MORE ORGANIZATIONS ADOPTED DMARC.

SOCIAL MEDIA ATTACKS

On social media, support fraud, also known as "angler phishing," rose sharply. Angler phishing occurs when an attacker creates a social media account designed to mimic customer support accounts of trusted brands. When a customer asks for help on social media, the attacker sweeps in using the fake customer-support account (often before the real one even has a chance to respond.) Under the guise of helping, the attacker then sends the customer to a fake login site to steal credentials or asks for the credentials directly.

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 in the first half of 2018.

The number of fake support accounts targeting our global customer base rose 37% from the previous quarter. At the same time, the number of phishing URLs sent through these accounts rose 30%.

Angler phishing accounts

Q1 2018	Q2 2018
363	499

Support fraud, also known as angler phishing rose sharply

Malicious URLs

Q1 2018	Q2 2018
364	472

SECTION 3 HOW TO PROTECT THEM

People-centric threats require a people-centric approach to keeping them safe. 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, join our webinar.

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 per cent 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.