proofpoint.

2019 THREAT REPORT

EMAIL FRAUD IN FINANCIAL SERVICES

INTRODUCTION

Email fraud, already one of today's biggest cyber threats, shows no signs of letting up. That's the sobering conclusion our latest research into this growing category of cyber attacks. Attackers are sending more fraudulent emails. They're impersonating more people. And they're targeting more recipients.

Email fraud is a broad category. It includes business email compromise (BEC), a type of wire fraud, and other threats in which the attacker uses some form of identity deception. According to the FBI, BEC alone has cost organizations around the globe a potential $12.5 billion since the end of 2013.[1]

Email fraud preys on human nature—fear, trust and the desire to please—to steal money and valuable information. These are highly targeted, socially engineered attacks that seek to exploit people rather than technology. They use a wide range of methods and tools. But they all involve impersonation tactics (such as spoofing) to pose as trusted colleagues and business partners.

Email fraud affects organizations of every size, across every industry, and in every country around the world. The financial services industry, for obvious reasons, is an especially attractive target.

Every day, Proofpoint analyzes more than 5 billion email messages, hundreds of millions of social media posts and more than 250 million malware samples to protect organizations around the world from advanced threats. That gives us a unique vantage point from which to identify, analyze and reveal the tactics, tools and targets of today's cyber attacks.

For this study, we anlyzed a subset of more than 160 billion emails sent across 150 countries in 2017 and 2018. We focused on email fraud attacks targeting more than 100 financial services organizations.

This report is designed to serve as actionable intelligence. Our goal is to help you better combat today's attacks, anticipate emerging threats, and manage your security posture. Along with our findings, we recommend steps you can take to protect your people, data and brand.

1 FBI. "Business E-Mail Compromise: The 12 Billion Dollar Scam." July 2018.

TABLE OF CONTENTS

EMAIL FRAUD CONTINUES TO RISE

Financial services firms were targeted by impostor attacks 60% more frequently in Q4 2018 vs. the year-ago quarter. Already a significant threat to the financial services sector in 2017, email fraud continued to grow throughout 2018. We saw more frequent of attacks, more people targeted per attack, and more identities spoofed.
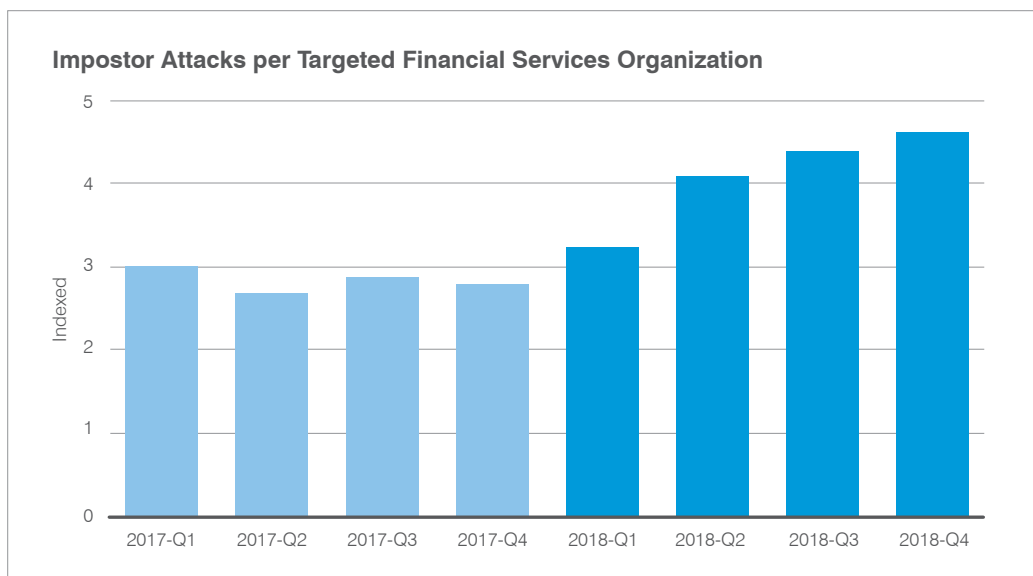
Impostor Attacks per Targeted Financial Services Organization

FINANCIAL SERVICES FIRMS WERE **TARGETED BY IMPOSTOR ATTACKS 60% MORE FREQUENTLY** IN Q4 2018 VS. THE YEAR-AGO QUARTER.

FRAUDSTERS IMPERSONATE AND TARGET MORE PEOPLE

As criminals grow more sophisticated, they are spoofing (or impersonating) more identities and targeting more people within organizations.

In Q4 2018, 38% of financial services firms were targeted using at least five spoofed identities. In other words, the identities of at least five of the companies' employees were weaponized to target other employees within that organization. About 37% of companies were targeted using two to five spoofed employee identities.

More than half (56%) of firms had more than five of their employees targeted by impostor attacks. Just 17% had only one person targeted.

SOCIALLY ENGINEERED FOR SUCCESS

WITHIN TARGETED FINANCIAL SERVICES FIRMS, 56% SAW MORE THAN FIVE EMPLOYEES TARGETED BY IMPOSTOR ATTACKS IN Q4 2018.

Impostor Email Attacks Against Financial Services Companies by Subject Category

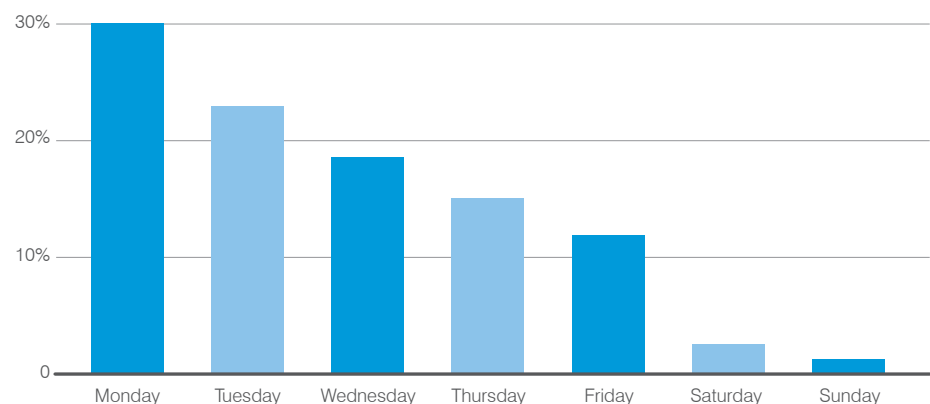Payment — Request — Urgent — Greeting — FYI — Others
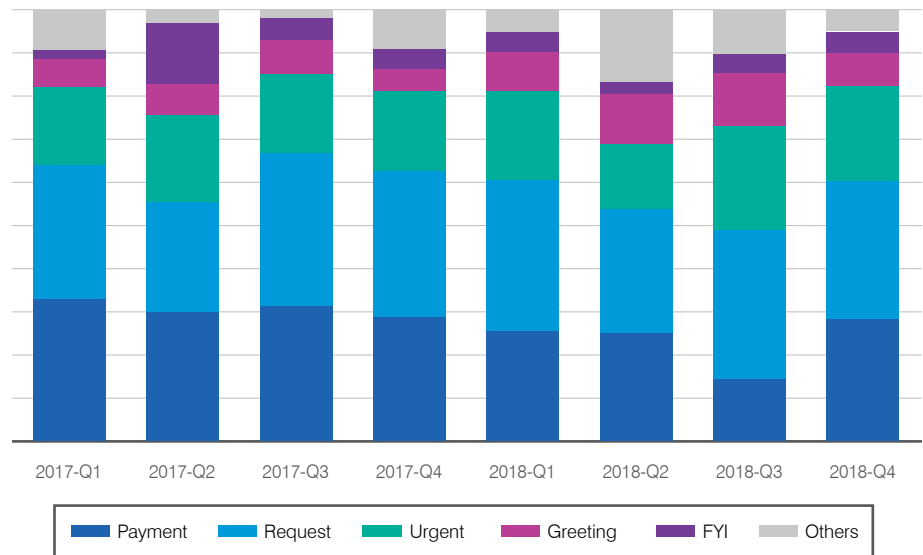
Wire-transfer scams are a large component of email fraud in the financial services industry. Over the past two years, the top subject categories used to target financial services firms have included "payment," "request" and "urgent."

Payment-related subject lines such as "payment status," "payment request" and "swift transfer" were twice as common among financial services firms. They accounted for 10% of total messages vs. just 5% across all industries.

Shipment-related subject categories, such as "UPS shipment notification" and "your tracking notification," were far more common in financial services organizations. They represented 8% of impostor attacks, compared to 1% across all industries. And messages that included "account change request" in the subject made up 7% of attacks targeting financial services companies vs. just 2% overall.
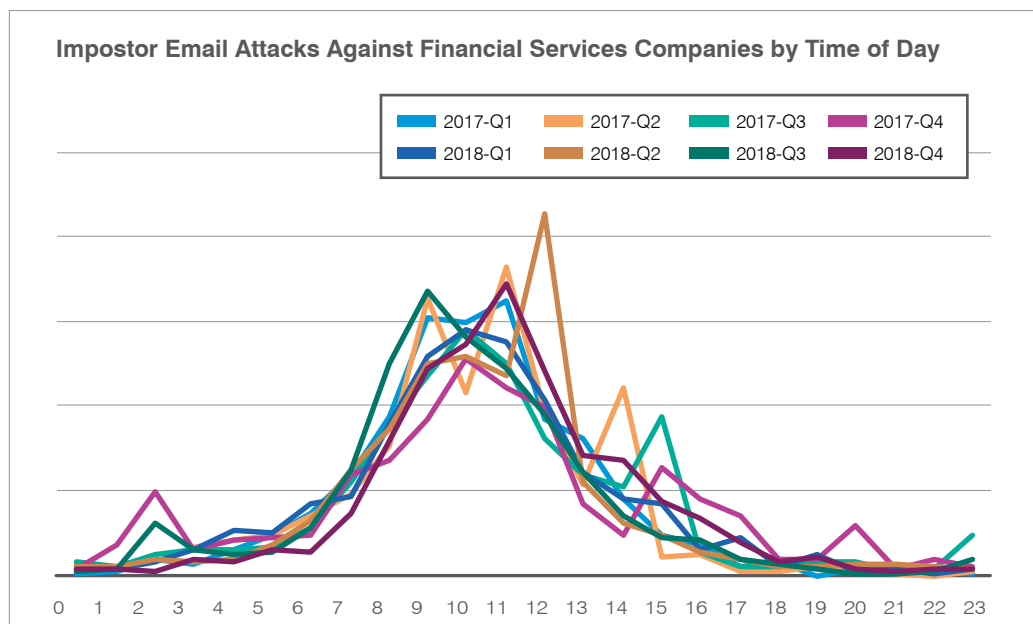
THE LARGEST VOLUME OF IMPOSTOR EMAIL ATTACKS TARGETING FINANCIAL SERVICES ARRIVED ON WEEKDAYS BETWEEN 7 A.M. AND 2 P.M. IN THE TARGETS' TIME ZONE.

Impostor Email Attacks Against Financial Services Companies by Day of the Week

Email fraud attacks are socially engineered to target specific people who, due to their job roles, can carry out criminals' wishes. For that reason, fraudsters target financial services companies mostly on weekdays. Most attacks are sent on Monday through Thursday. Volume dips on Friday before falling sharply for the weekend.

IN Q4 2018, **39% OF EMAIL SENT FROM DOMAINS** OWNED BY FINANCIAL SERVICES COMPANIES **APPEARED SUSPICIOUS OR WERE UNVERIFIED.** THAT FIGURE INCLUDES **68% SENT TO EMPLOYEES, 36% SENT TO CUSTOMERS,** AND **19% SENT TO BUSINESS PARTNERS.**

Impostor Email Attacks Against Financial Services Companies by Time of Day

| 2017-Q1 | 2017-Q2 | 2017-Q3 | 2017-Q4 |
| 2018-Q1 | 2018-Q2 | 2018-Q3 | 2018-Q4 |

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

More than 74% of all impostor email attacks against financial services organizations are sent between 7 a.m. and 1 p.m. in their targets' local time zone. The largest percentage arrives around 10 a.m., early in the workday.

TACTICS USED TO TARGET FINANCIAL SERVICES ORGANIZATIONS

Email fraudsters use a variety of techniques, often in tandem, to pose as someone the victim trusts or does business with. Here are the most common:

DISPLAY-NAME SPOOFING

DISPLAY-NAME SPOOFING
Display-name spoofing is when an attacker simply changes the name that shows up at the top of the email as the sender, which may not reflect the actual sending email address.
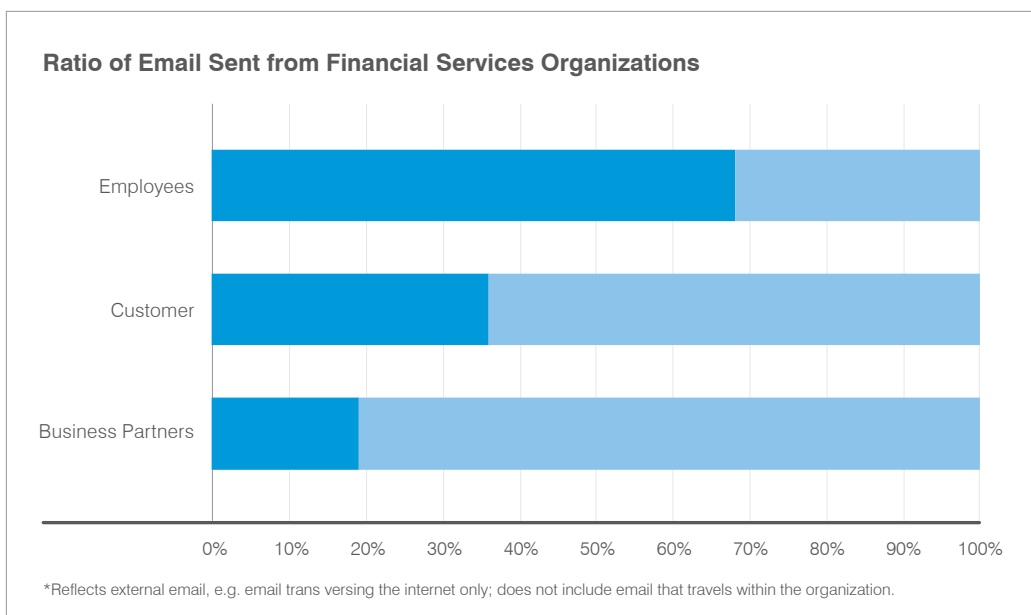
Webmail services such as Gmail are the preferred vehicle for email fraud because they're free and easy to use. In email fraud, the attacker simply changes the display name. (Email display names are unrelated to the actual email address being used—they can be anything the sender wants it to be.) Over the course of 2017 and 2018, nearly 39.5% of email fraud across financial services used Gmail.com, Comcast.net, AOL.com, Inbox.lv, or RR.com.

DOMAIN SPOOFING
Domain spoofing is sending fraudulent emails that appear to come from an organization's own trusted domain.

DOMAIN SPOOFING

Another common tactic is sending fraudulent email from the organization's own trusted domain. This is called domain spoofing. Criminals spoof domains owned by financial services companies to target its employees, customers and business partners.

Ratio of Email Sent from Financial Services Organizations

*Reflects external email, e.g. email trans versing the internet only; does not include email that travels within the organization.

Overall, 39% of emails sent from financial services domains in Q4 appeared suspicious or were categorized as unverified. The percentage was even higher for emails sent to employees, at 68%. Roughly 36% of the emails sent to customers from financial services-owned domains was suspicious or unverified. The same was true of 19% of emails sent to business partners.

The good news: you can prevent criminals from hijacking your trusted domains for email fraud attacks by fully deploying **DMARC** email authentication. With DMARC authentication, you can ensure that all email sent from your trusted domains is verified and legitimate. DMARC adoption is on the rise for financial services firms seeking to protect their domains.

In a study of 119 financial service organization's primary domains, 64% had published a DMARC policy. About 28% of these organizations have implemented a "reject" policy, the most effective way to protect domains against email fraud.

LOOKALIKE DOMAINS

Attackers often register lookalike domains to trick people into believing an email is sent from someone they trust. They create new, deceptively similar domains a variety of ways. They may swap characters, such as replacing the letter "o" with the numeral "0," for example. Or they might insert an additional character, such as an "s" or a hyphen. In 2017 and 2018, 24% of financial services organizations were targeted by attacks launched from lookalike domains.

DMARC
DMARC stands for Domain-based Message Authentication, Reporting, and Conformance.

PROOFPOINT RECOMMENDATIONS

Email fraud continues to rise, and financial services organizations are being targeted more than ever. Cyber criminals are growing more advanced. They are targeting more people within companies. And they use a wide range of tactics to trick people into sending money or valuable information.

These fraud tactics are always shifting. That's why you need a multi-layered defense.

To protect your employees, customers and business partners from email fraud, consider the following:
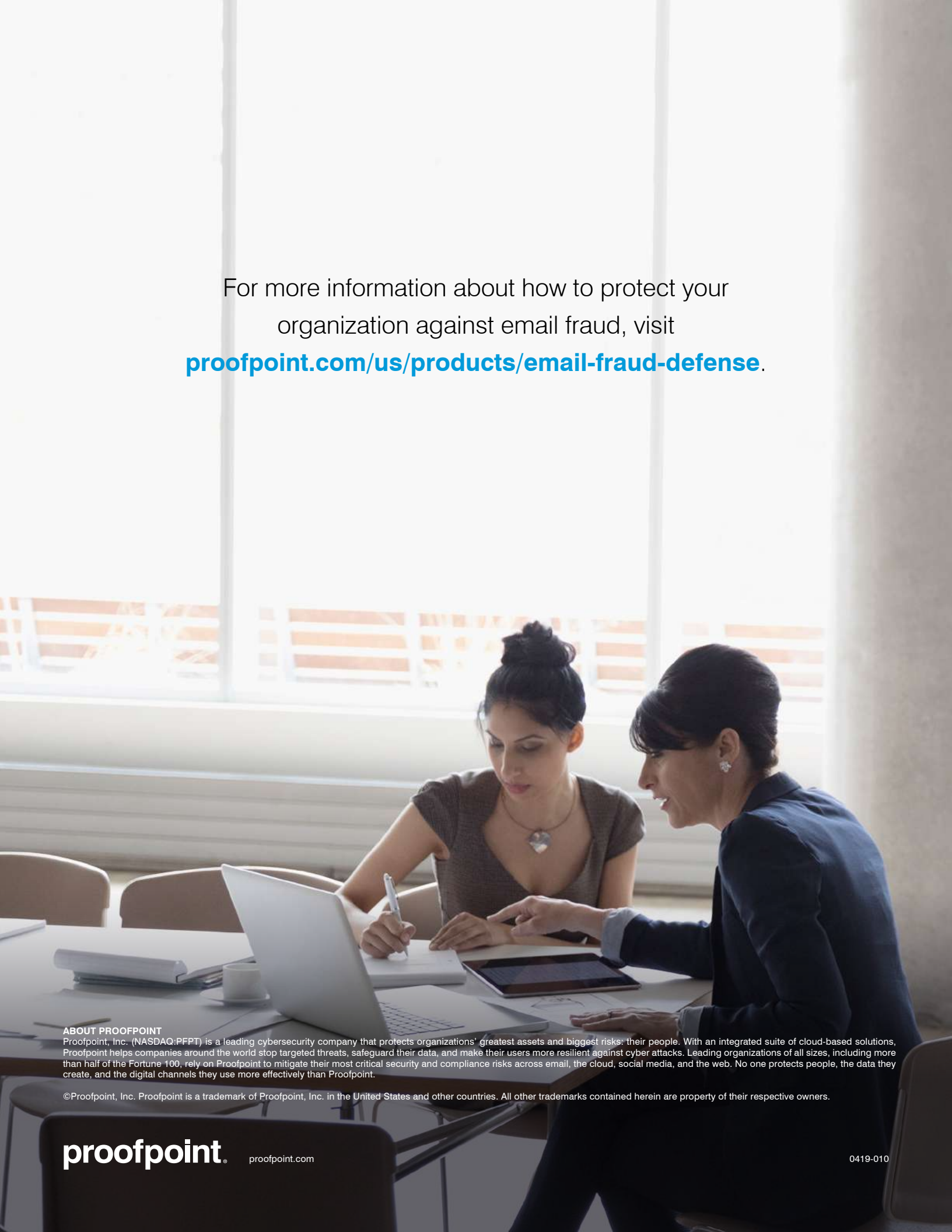
People-centric security. Build protection for—and gain visibility into—your greatest security risk: your people.

Email authentication (DMARC). Block all impostor attacks that spoof your trusted domains.

Machine learning and policy enforcement. Analyze the contents and context of email to stop display-name spoofing and lookalike domains at the email gateway.

Domain monitoring. Automatically identify and flag potentially risky domains registered by fraudsters.

Security awareness training. Turn your users into a strong last line of defense against phishing and other cyber attacks.

For more information about how to protect your organization against email fraud, visit **proofpoint.com/us/products/email-fraud-defense**.