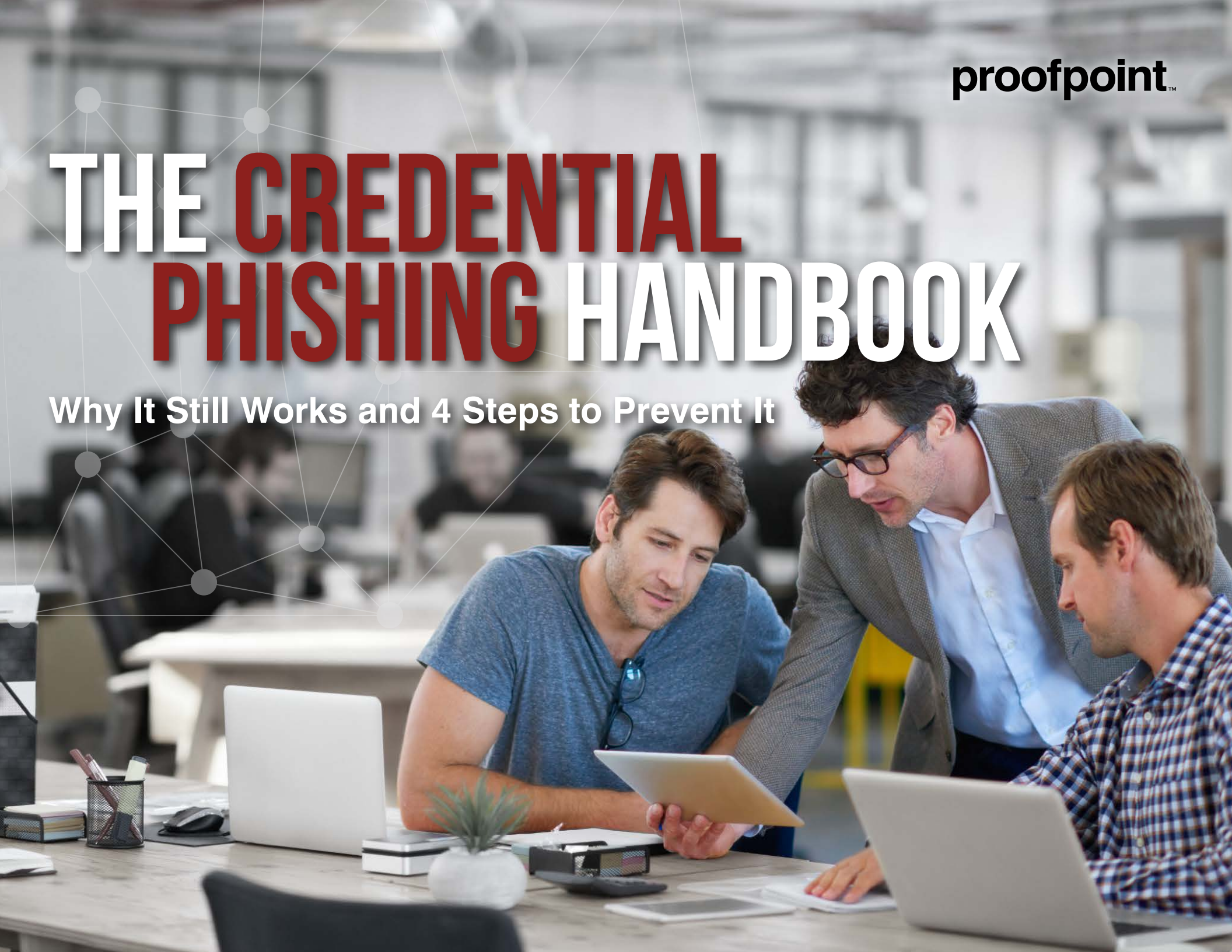
proofpoint™

# THE CREDENTIAL PHISHING HANDBOOK

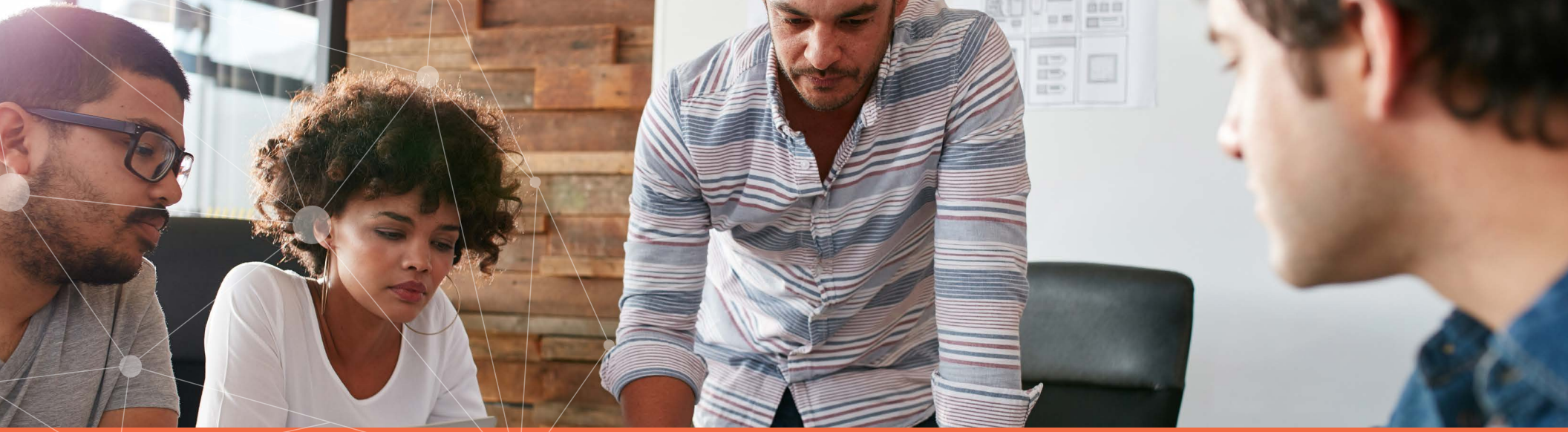
## Why It Still Works and 4 Steps to Prevent It



# INTRODUCTION

Phishing is more than 20 years old, but still represents more than 90% of targeted attacks.  The reason is simple: it works.

Nearly one in four people who receive a phishing email open it. Even more alarming: more than 10% will click on the malicious link or open the weaponized attachment that the phishing email contains.  That means an attacker has to send only 10 messages to have a 90% probability of catching and compromising a user.  The average-sized organization loses $3.7 million to phishing scams per year, according to the Ponemon Institute.  And those are just the tangible costs.



# HOW PHISHING WORKS: TRENDS AND TACTICS

While other cyber attacks have become more advanced in a technical sense, phishing has grown more advanced in terms of how it exploits human behavior. They are getting past traditional filters and into corporate inboxes. And they are being clicked, regardless of the amount of user-awareness training. Here are four techniques used in phishing attacks:

PRETENDING TO BE FROM THE TARGETED USERS' IT DEPARTMENT

TARGETING SPECIFIC USERS AND DEPARTMENTS

USING WEAPONIZED DOCUMENTS EMBEDDED WITH MALICIOUS MACROS

WORKING IN CONJUNCTION WITH WATERING-HOLE ATTACKS

# WHO ATTACKERS TARGET: FOLLOWING THE MONEY

Attackers go where the money is: payment and financial service firms make up 40% of targeted phishing attacks. Internet service firms are also popular targets because compromised domain-name and hosting services enable future attacks.

While attackers send phishing email throughout targeted organizations, click-through rates vary by department and job function. Surprisingly, some the most conscientious workers are among the most likely to click, especially when the phishing email appeals to their sense of urgency, efficiency, and order.

Phishing attacks make money in a variety of ways. Some sell stolen credentials. Others trade in confidential documents. And still others use the stolen credentials to make fraudulent financial transactions.

# WHY PHISHING ATTACKS SUCCEED: EXPLOITING HUMAN NATURE

Attackers are using all kinds of tricks to get their weaponized links and documents past the filters and firewalls that are trying to keep them out. Here are a few:

### GETTING PAST THE FILTERS WITH FAST-CHANGING URLS AND DOMAINS

and much smaller campaigns that don't trigger spam controls

### IMPERSONATING URLS AND WEBSITES

### LARGE-SCALE SOCIAL ENGINEERING RESEARCH

using public information to craft convincing email

### IMPERSONATING FRIENDS AND COLLEAGUES

# HOW TO STOP PHISHING ATTACKS: RECOMMENDATIONS

Your people are now the primary exploit target. You need to protect them the way they work and identify assets and risks before you are compromised. Here are some ways to combat phishing attacks:

### REDUCE THE ATTACK SURFACE

Deploy tools that monitor and analyze messages, URLs, attachments, and user clicks using static code and dynamic behavioral techniques.

### EXPAND YOUR DEFENSE COVERAGE

with cloud-based defenses that protect your people wherever they work.

### TAKE ADVANTAGE OF BIG DATA AND MACHINE-LEARNING TECHNIQUES

to predictively catch emerging and never-before-seen attacks before the user clicks.

### GET BETTER VISIBILITY

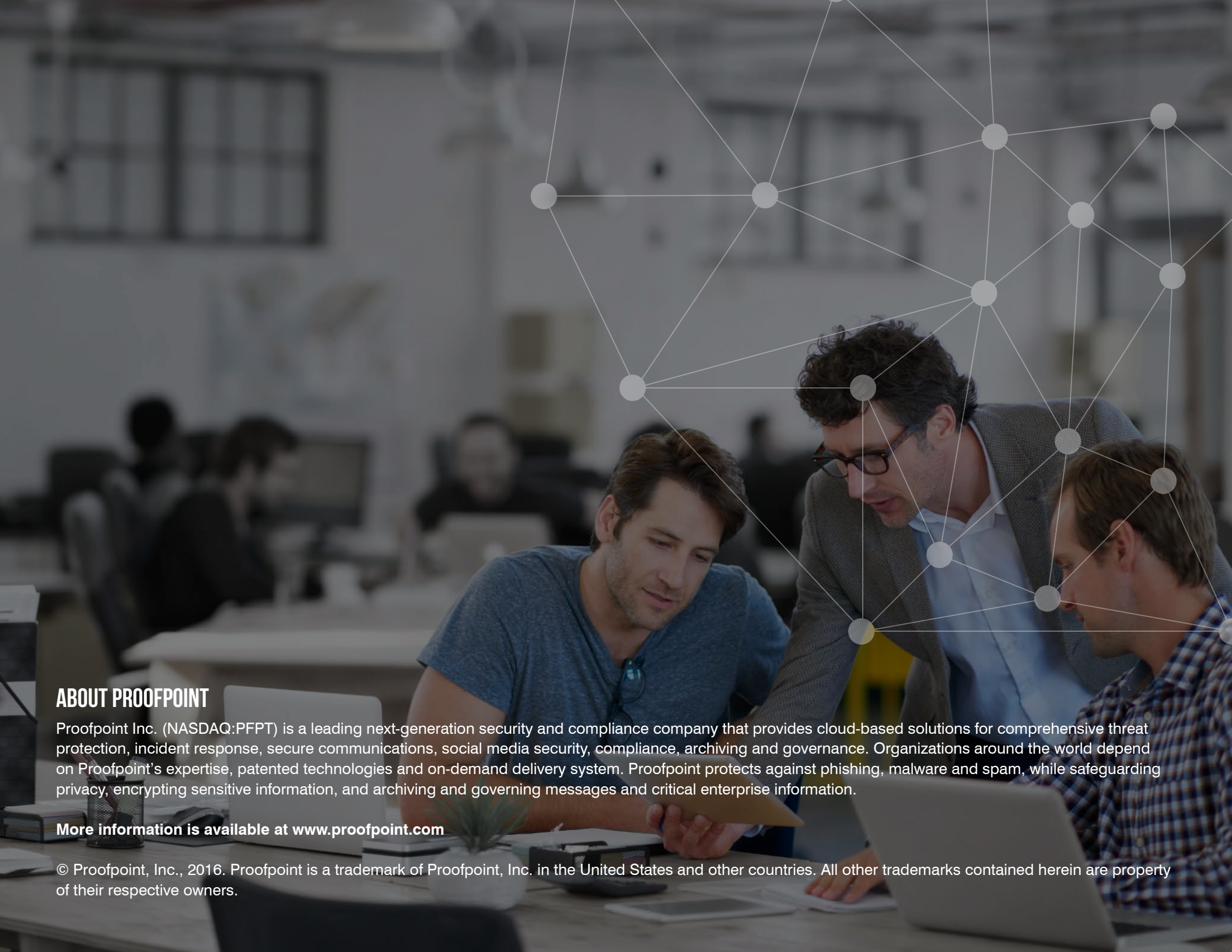
into your environment and the broader threat landscape. Real-time threat intelligence and a view of threat activity on your systems help you respond and recover faster. Deploy tools that help you understand who is being targeted by what threats, which threats made it through your defenses, and who has been hit.

# GET EMAIL PROTECTION BUILT FOR THE WAY YOU WORK

With an increasing amount of sensitive and confidential information—and an expanding attack surface of devices, cloud apps, and mobile locations—you cannot afford to rely on traditional defenses. Innovative new tools operate within the work flow, monitoring URLs and attachments, sharing real-time threat intelligence, and watching user activity on and off your corporate network.

Targeted attack protection helps you detect, mitigate, and respond to these threats before they succeed.

**To learn more about how Proofpoint can help you stop credential phishing, download our white paper, Hook, Line, and Sinker: How Credential Phishing is Changing and How to Stop It at www.proofpoint.com.**



## ABOUT PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information.

**More information is available at www.proofpoint.com**