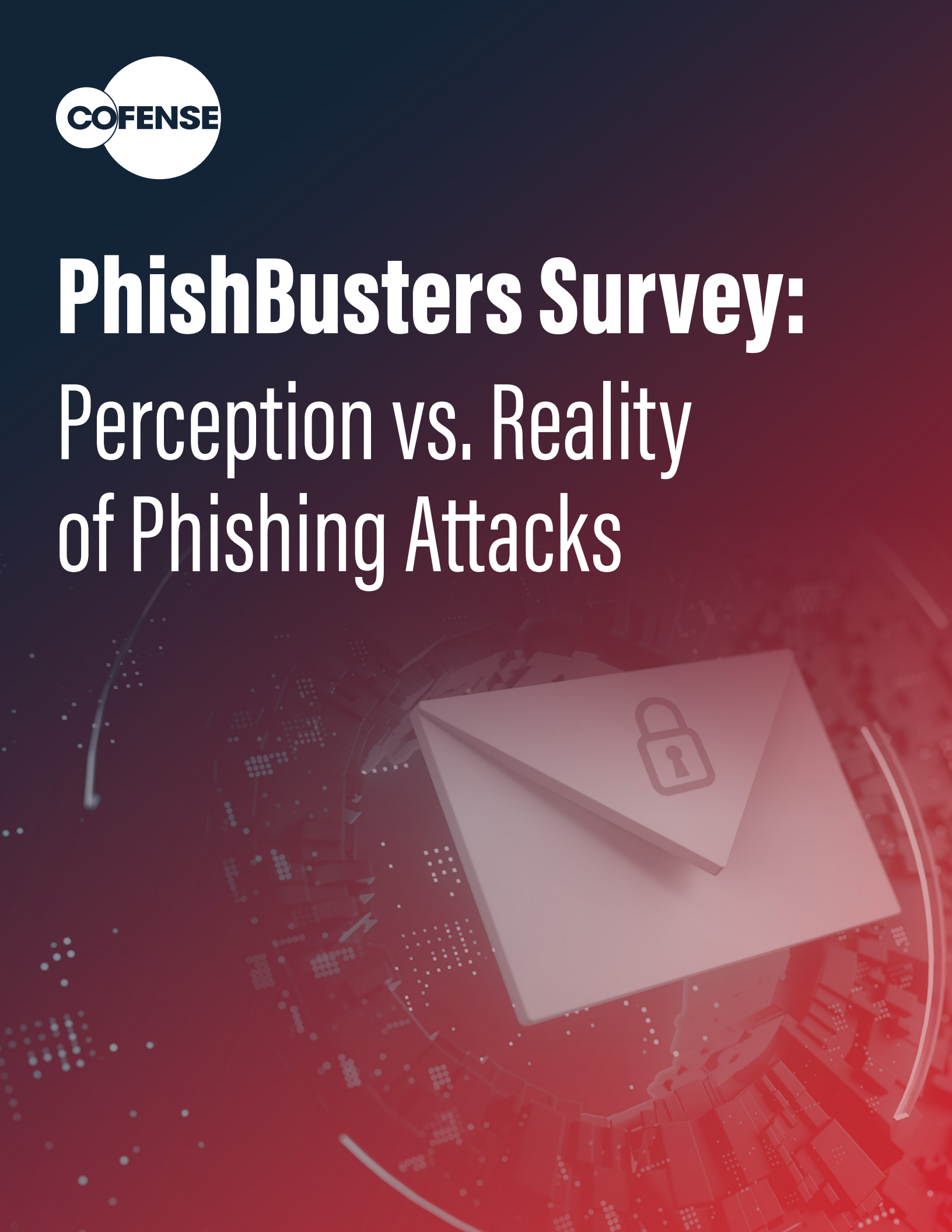
COFENSE

PhishBusters Survey:

Perception vs. Reality of Phishing Attacks



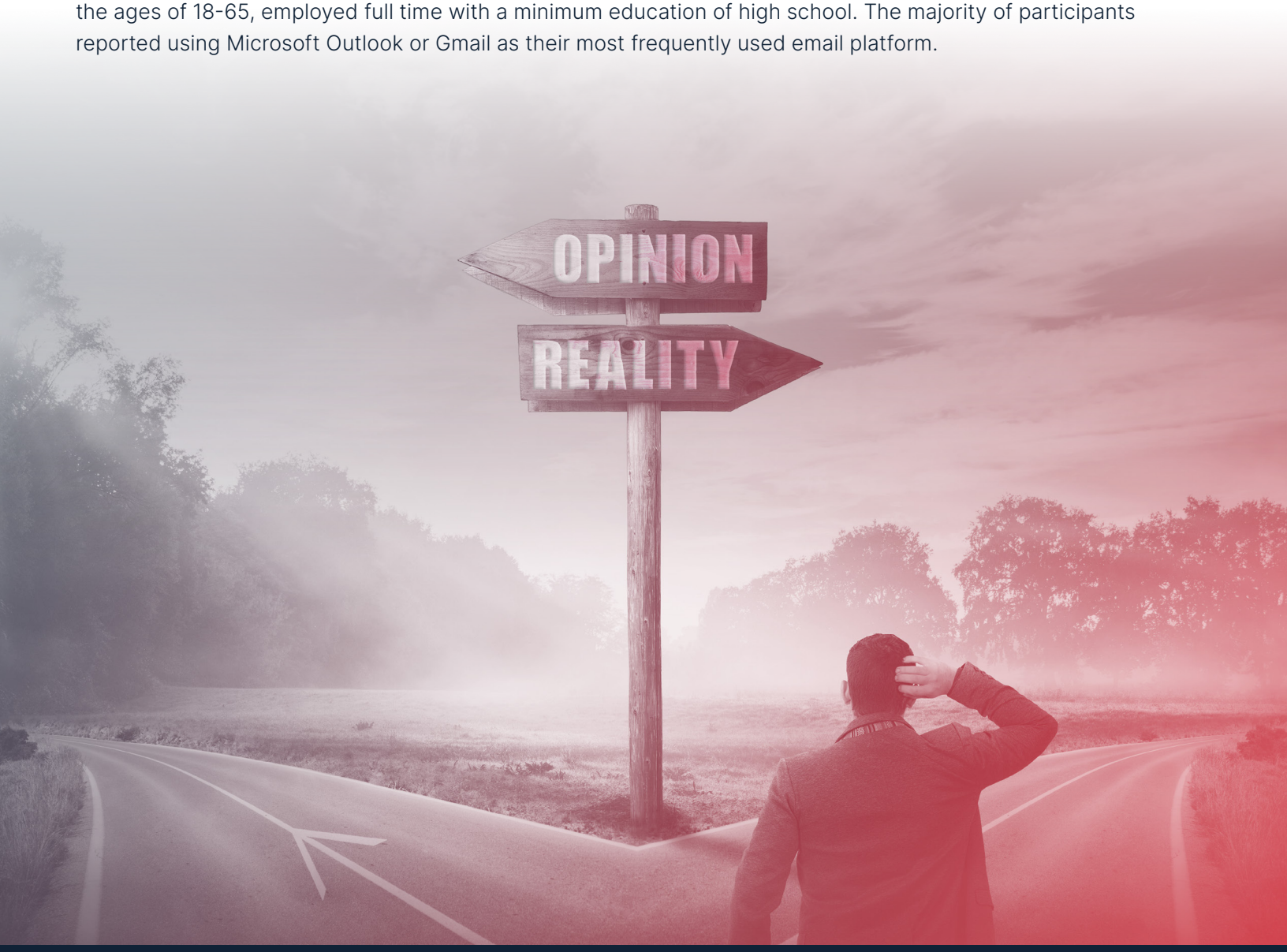
Introduction

What does the general population know about phishing attacks?

How do these beliefs, and the behaviors of individuals, impact the security of their employers?

To answer these questions and more, Cofense conducted a survey to examine the general public's perceptions of phishing attacks, including what they believe to be the top types of attacks, motives of attackers and who is most at risk.

The PhishBusters Survey was conducted in October 2021, and included 557 respondents from the U.S. The participants were representative of the general population, diverse in the industries they work in, their job functions, company size, household incomes, etc. Responses were narrowed down to participants between the ages of 18-65, employed full time with a minimum education of high school. The majority of participants reported using Microsoft Outlook or Gmail as their most frequently used email platform.



Key Findings – PERCEPTION VS. REALITY

Which employees at an organization are most likely to be targets of phishing attacks?

PERCEPTION

Entry level or middle management are most likely to be targeted by a phishing attack.

- A majority of respondents (nearly 34%) felt entry level employees were targeted most by phishing emails. Almost 40% of respondents also feel Finance is the most targeted industry, followed by Defense/Government (15.8%) and Healthcare (15.26%).

REALITY

Everyone is a target, no matter what their level is in the organization or their industry.

- Cofense observes phishing attacks across all job levels and all industries. But attackers see executives as high-level targets because they have access to sensitive information that can be damaging to an organization. It's not uncommon to find a phishing campaign targeting one industry also showing up in another industry.

Who is most likely to fall for a phishing email?

PERCEPTION

Entry level, or "front-line" employees, are most susceptible to falling for a phishing attack.

- 60% of respondents feel entry level workers are more likely to fall for phishing attacks.
- Nearly 66% of respondents held roles in middle management or higher, indicating they believe they are savvier than entry level employees.

REALITY

Everyone, regardless of level in an organization, is susceptible to falling for a phishing attack.

- Phishing campaigns typically cast as wide a net as possible to catch as many employees as possible in an attack.
- Cofense observes attackers becoming increasingly clever at disguising phish. Everyone, at every level, is vulnerable.

How do attackers carry out phishing campaigns?

PERCEPTION

Phishing emails usually have a malicious link or attachment included for users to open that will deploy malware to the computer.

- More than 60% of respondents believe phishing emails are used to deploy malware to a computer, through malicious attachments or links.

REALITY

Emails that request users to input credentials via links to fraudulent web pages are the most common types of phish.

- Very few phishing emails use attachments or links to deploy malware. According to Cofense research, 60% of phishing emails in 2021 were designed to steal credentials and used links to do so.

Phishing Threats are Here to Stay

At Cofense, our mission is to stop phishing attacks in their tracks. One of the biggest hurdles to preventing individuals and organizations from becoming a victim is awareness. While we are having some fun with "survey says..." results, the reality of phishing attacks is bleak. Millions of ransomware, business email compromise (BEC) and credential harvesting attacks bypass expensive email security solutions every year. In fact, Cofense observes SEGs missing about 50% of email-based attacks employing malicious URLs. Meanwhile, the average cost of a data breach is nearing $4 million, and the average ransomware payment is over $100k.

Additional Survey Findings

- 71% of respondents identified stealing login credentials as the top motivation for phishing attacks (spoiler alert: that's correct)! However, only 29% of people are concerned about password or account compromise as the result of falling victim to an attack.
  - *Cofense notes that one of the prominent ways threat actors commit fraud, or drain bank accounts, is via credential reuse. It is evident that there is confusion about how passwords can be used against individuals and organizations.*
- Well known brands, including Microsoft, DropBox and Federal Express are among those spoofed in enterprise phishing, as seen by Cofense. A majority of respondents (62%) correctly identified these brands as most commonly spoofed in phishing emails.
- When asked about protections against phishing attacks, users reported understanding the need for two-factor authentication.
  - *Cofense notes that two-factor authentication provides strong protection, but not complete protection. You also need powerful email security that combines artificial intelligence, human reporting and automation tools to stop attacks quickly.*

This survey provided an opportunity to gain a broader understanding of public perceptions relating to phishing. It is evident that among the general population, those who do not work in security for a living, there is a gap to close when it comes to better understanding of the motives and techniques of cyber criminals deploying phishing attacks.

Cofense is the only company that combines a global network of 30 million people reporting phish with advanced AI-based automation to stop phishing attacks fast. That's why over half of the Fortune 500 and thousands of other organizations trust us. **To learn more about Cofense, please visit: www.cofense.com**