proofpoint.

2023 State of the Phish Report

An in-depth exploration of user awareness, vulnerability and resilience

Download

proofpoint.
REPORT
2023 State of the Phish
An in-depth exploration of user awareness, vulnerability and resilience
proofpoint.com

2023 State of the Phish

Loïc Guézo

Director Cybersecurity Strategy

linkedin.com/in/lguezo

@lguezo

lguezo@proofpoint.com

Davide Canali

Threat Research Manager

linkedin.com/in/dcanali

dcanali@proofpoint.com

proofpoint.

2023 State of the Phish - 9th Annual Report

2023 Report

7500
Working adults across 15 countries

1050
IT security pros across the same 15 countries

135M
Simulated phishing attacks sent by our customers

18M
Email reported by our customers’ end users

2022 Report

3500
Working adults across 7 countries

600
IT security pros across the same 7 countries

100M
Simulated phishing attacks sent by our customers

15M
Email reported by our customers’ end users

Surveyed Across the Globe

Surveyed **8** additional countries

- United States
- **Canada**
- **Brazil**

- United Kingdom
- Spain
- France
- Germany
- **Italy**
- **Sweden**
- **The Netherlands**
- **UAE**

- Australia
- Japan
- **Singapore**
- **South Korea**

2023 State of the Phish

Threat Landscape—
TOAD, MFA phishing, brand abuse, BEC and more

User Vulnerability—
knowledge gaps, security habits, benchmarking data

Opportunities—
Security awareness education and controls

The 2022 Threat Landscape

Phishing— More Sophisticated Techniques

MFA PHISHING

Ubiquitous enough to threaten almost every organisation

TOAD

Telephone Oriented Attack Delivery— 300k-400k per day; **600k** at peak

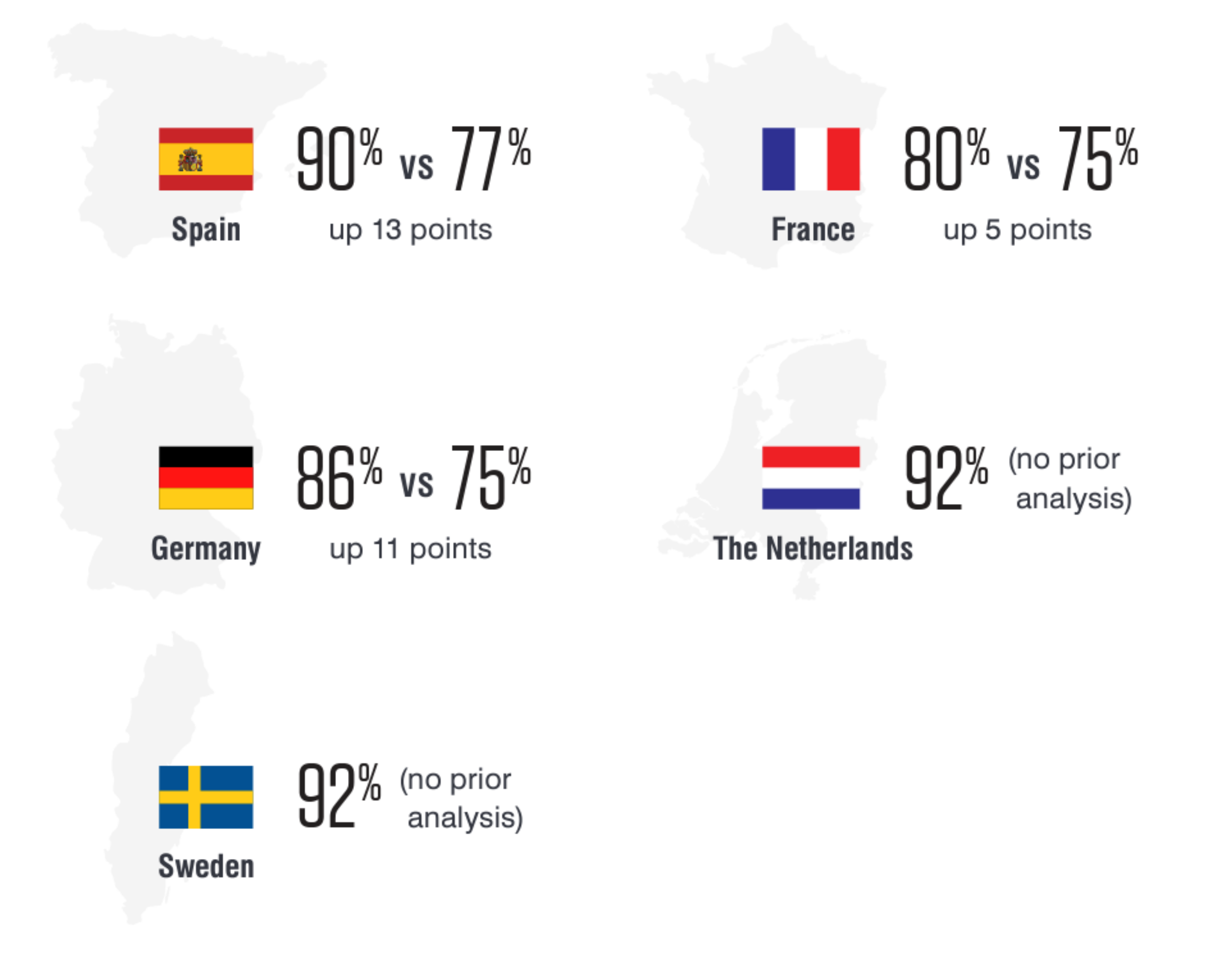
BEC

75% experienced attacks. Increase in countries where English is not the first language

BEC Goes Global

80%

French organisations reported facing BEC attacks

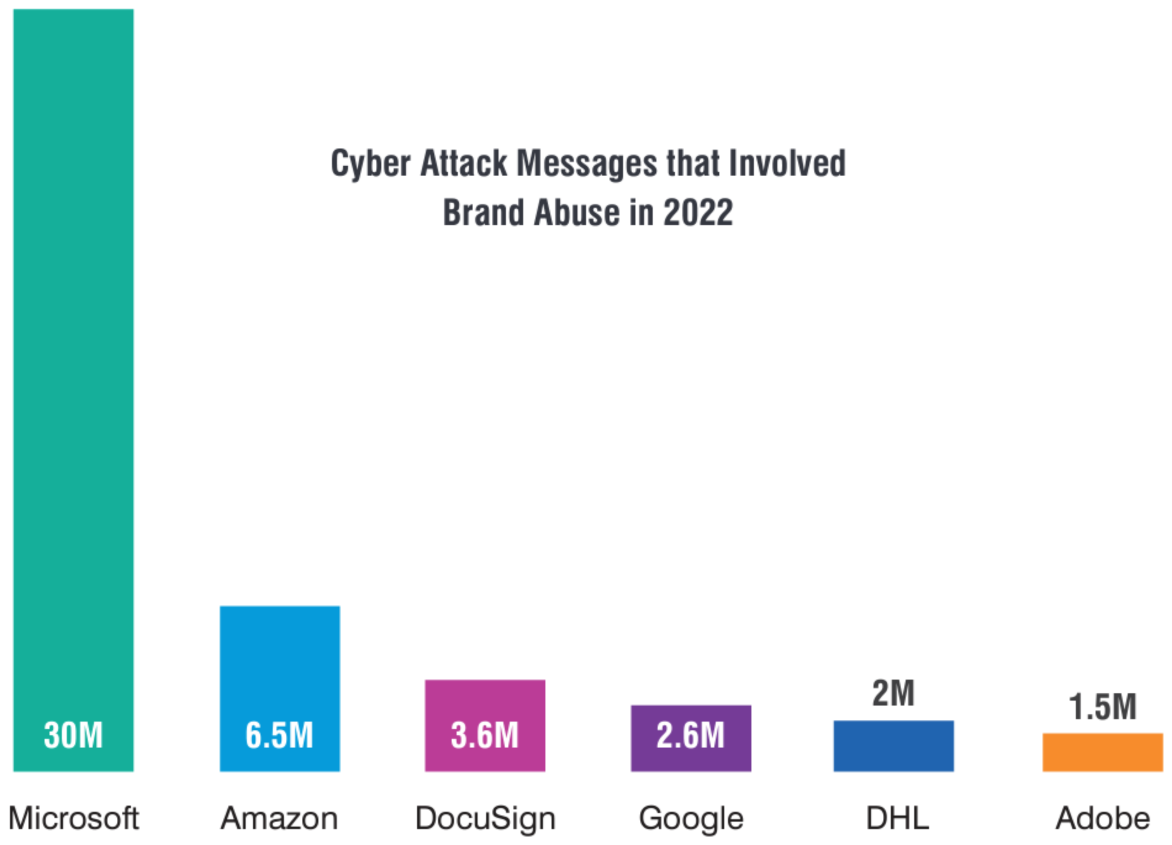


Poll #1

Quelle a été la marque la plus détournée en 2022?

A. Amazon
B. Google
C. Microsoft
D. Adobe

Microsoft, the Most Abused Brand



30M

malicious messages used **Microsoft** branding and products

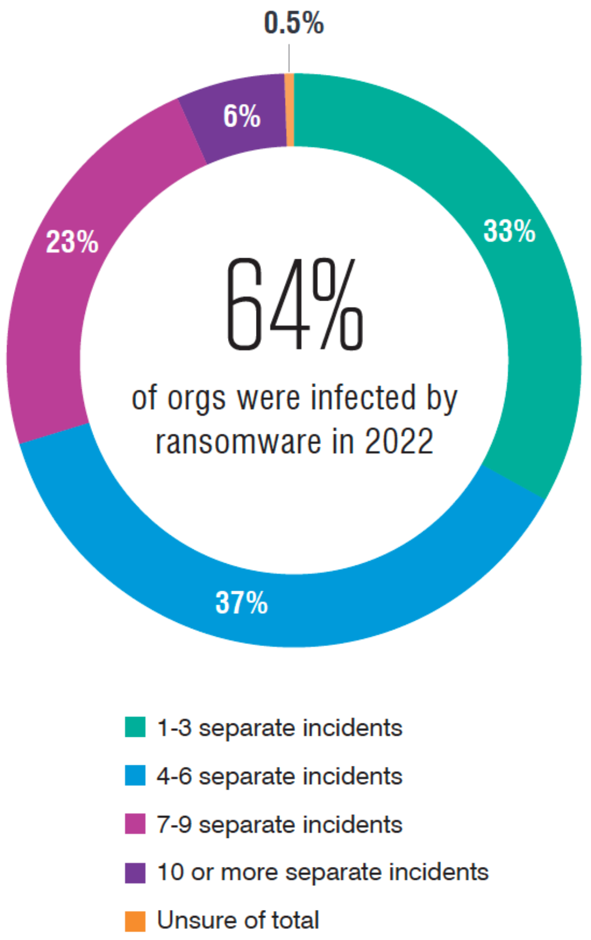
Meanwhile… 44%

of working adults think an email with a familiar brand is safe

Ransomware Remains

76%

Of orgs experienced an attempted ransomware attack in 2022



64%

of orgs were infected by ransomware in 2022

52%

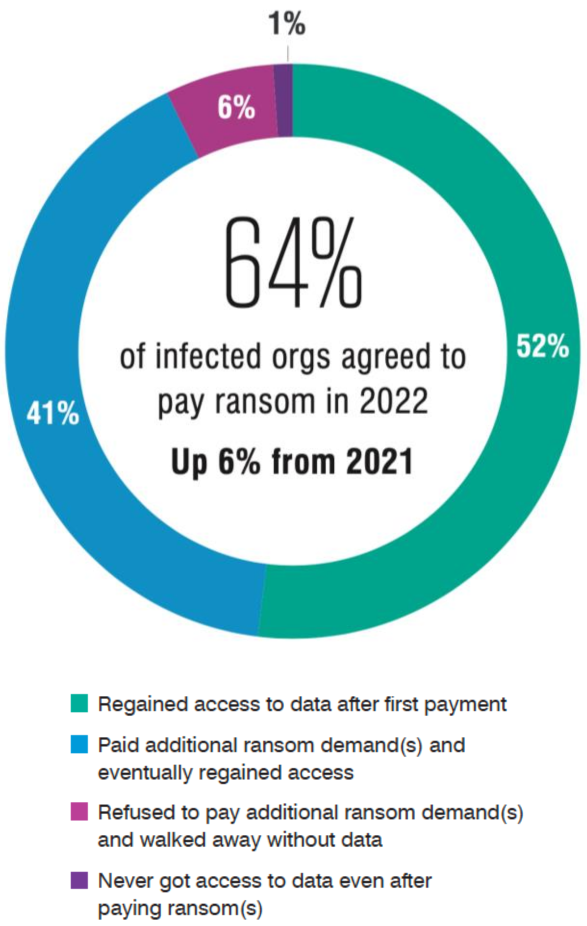
Regained access to their data after making a single ransomware payment

Poll #2

Quel pourcentage des organisations ont finalement payé la rançon?

A. 82%
B. 64%
C. 40%
D. Moins de 20%

Organizations Got Help from Cyber Insurance



90%

Of orgs infected by ransomware had cyber insurance

82%

Of insurers were willing to help

The Insider Threat

14%

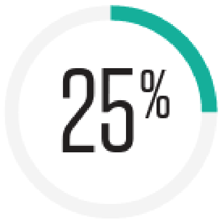
French security professionals surveyed have changed jobs within the past two years

~47%

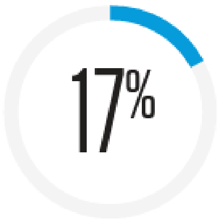
Admitted to taking data with them when they left (FR)

~70%

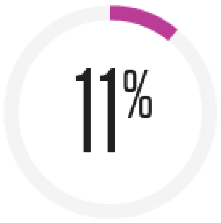
Reported data loss because of an insider (FR)



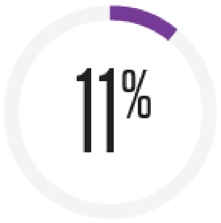
Report one to 10 data loss incident(s) via insider



Report 11 to 25 data loss incidents via insider



Report 26 to 50 data loss incidents via insider

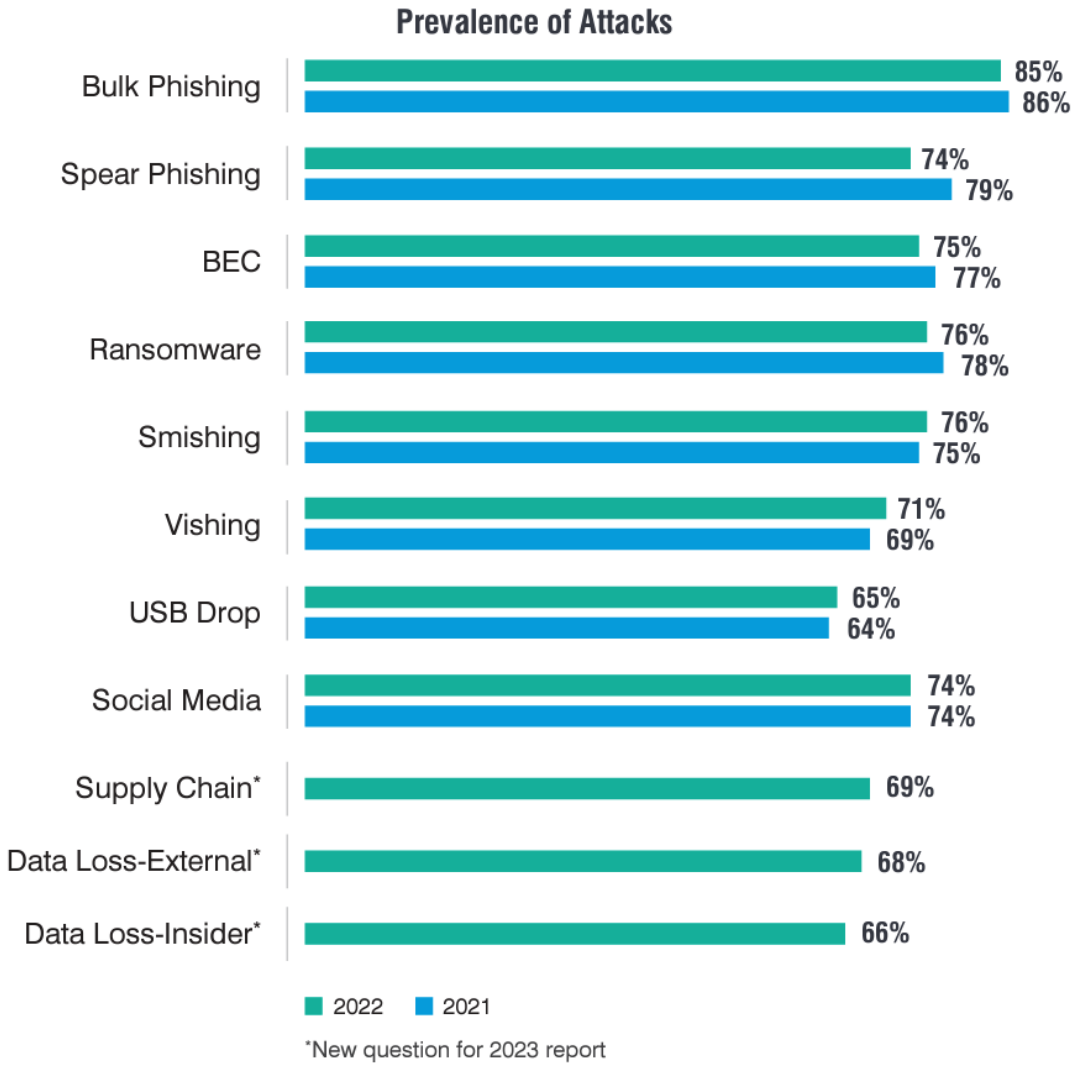


Report over 50 data loss incidents via insider

Attackers Were Just As Successful

84%

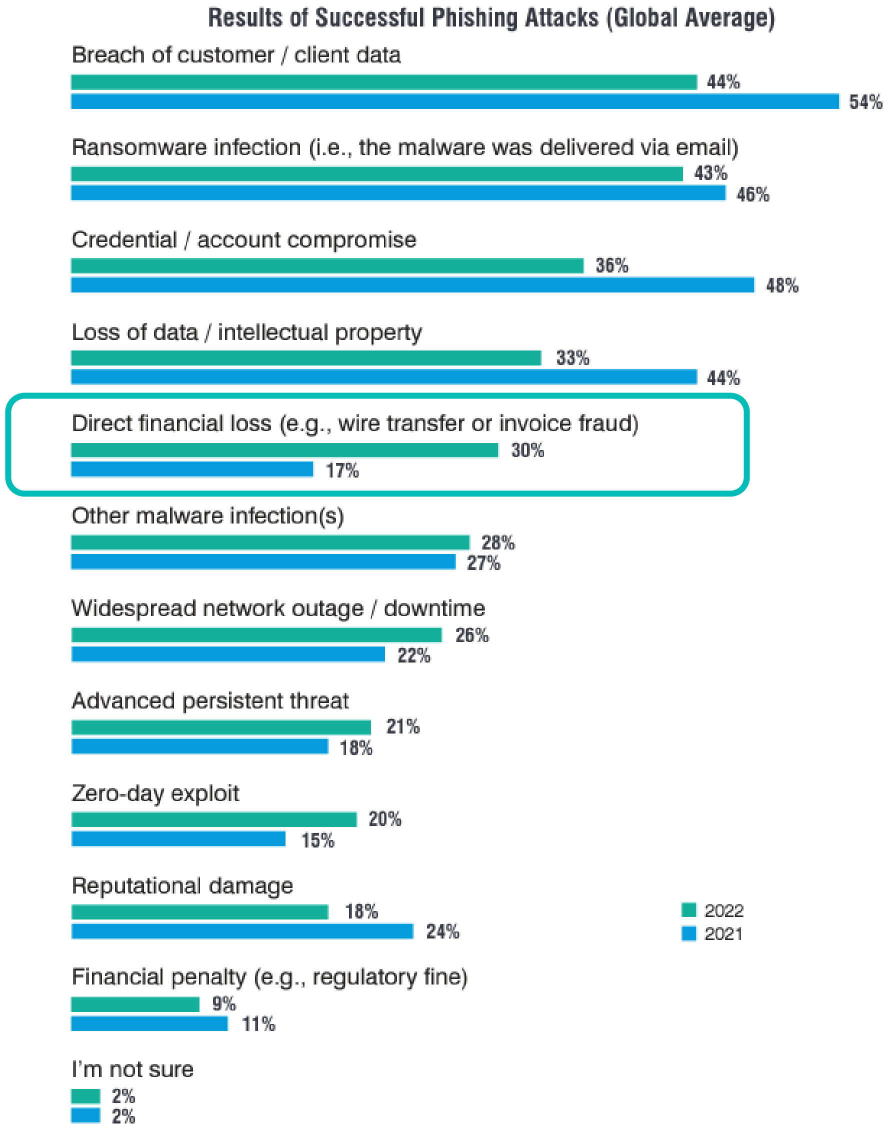
Experienced a successful email-based phishing attack in 2022, **up from 83% in 2021**



Cost of a Phish

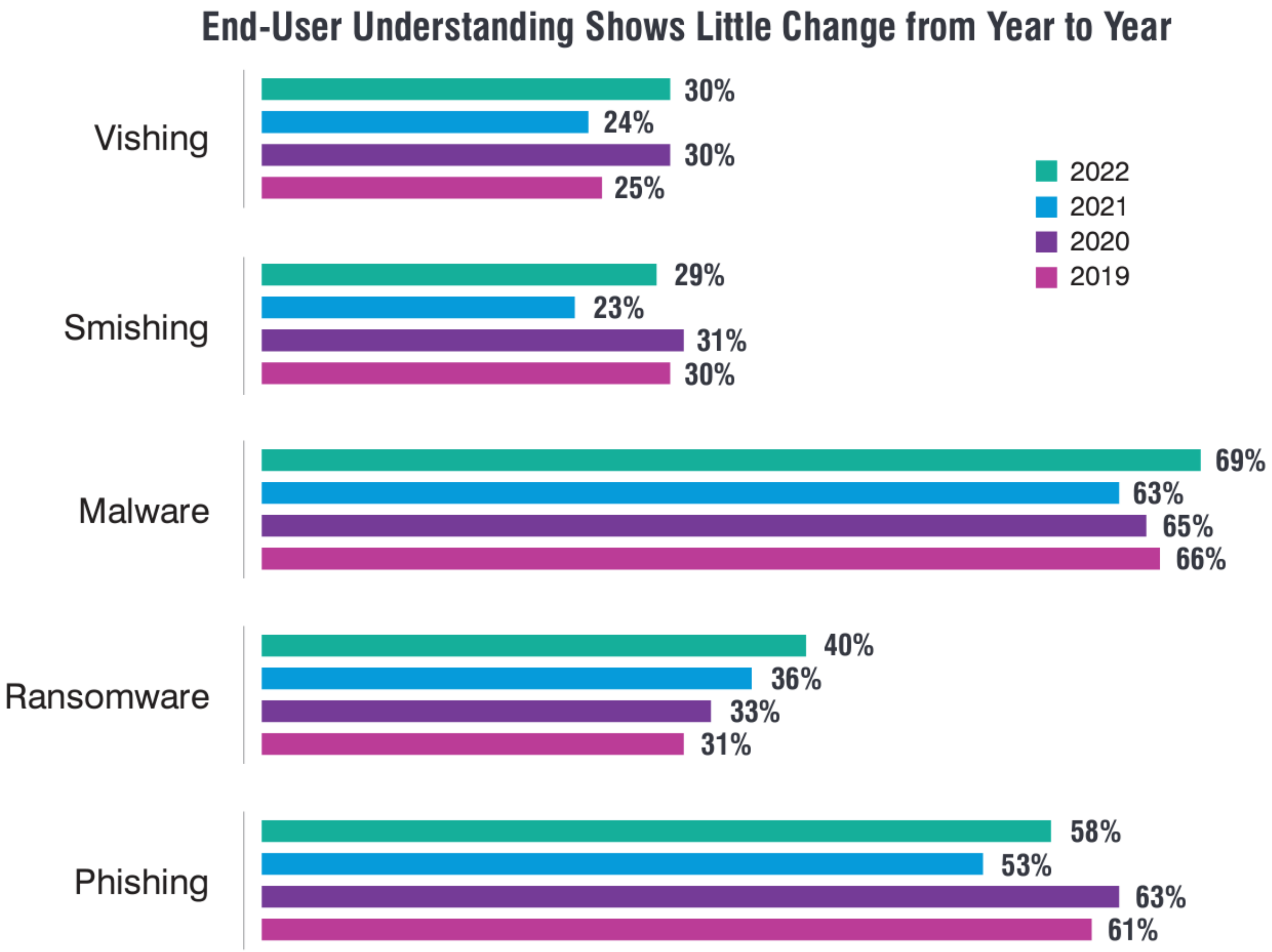
76%

Increase in **Direct financial loss** (e.g., wire transfer or invoice fraud)



User Awareness and Vulnerability

User Knowledge: The Same Gaps Remain

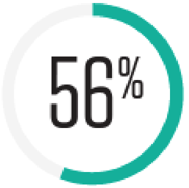


Poll #3

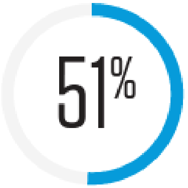
Combien de professionnels savent qu'un échange de plusieurs courriels ne signifie pas pour autant que l'expéditeur est sûr?

A. ~40%
B. ~50%
C. ~60%
D. ~70%

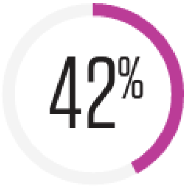
Additional Knowledge Gaps: Security Fundamentals



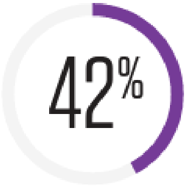
Know a familiar company brand doesn't make an email safe



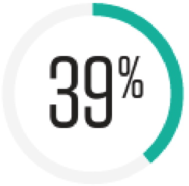
Know a link or attachment can affect computers beyond theirs



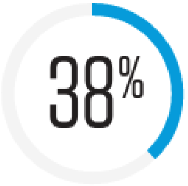
Know their email provider can't automatically block all malicious emails



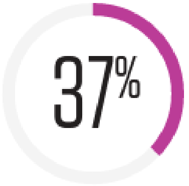
Know exchanging multiple emails doesn't mean a sender is safe



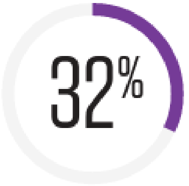
Know that files stored in the cloud are not always safe



Know internal emails at work are not always safe

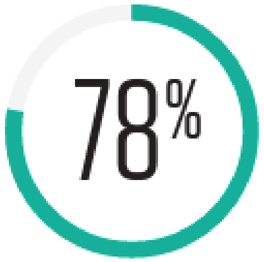


Know an email link might not match the website it goes to

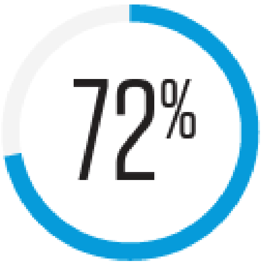


Know their company can't automatically block all malicious emails

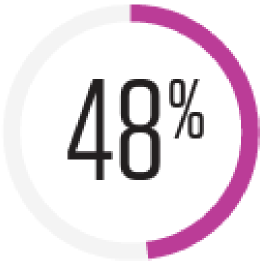
Security Habits: Blurred Lines



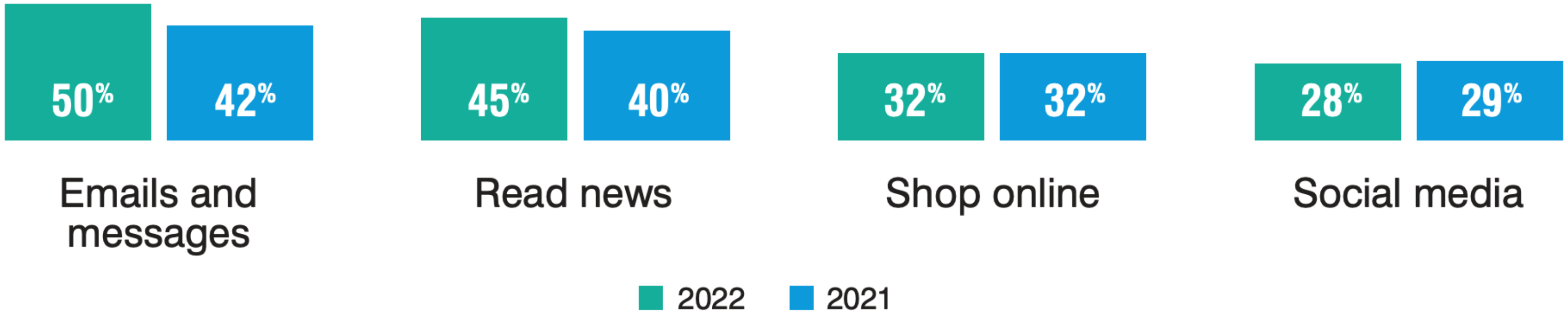
Use work devices for personal activities



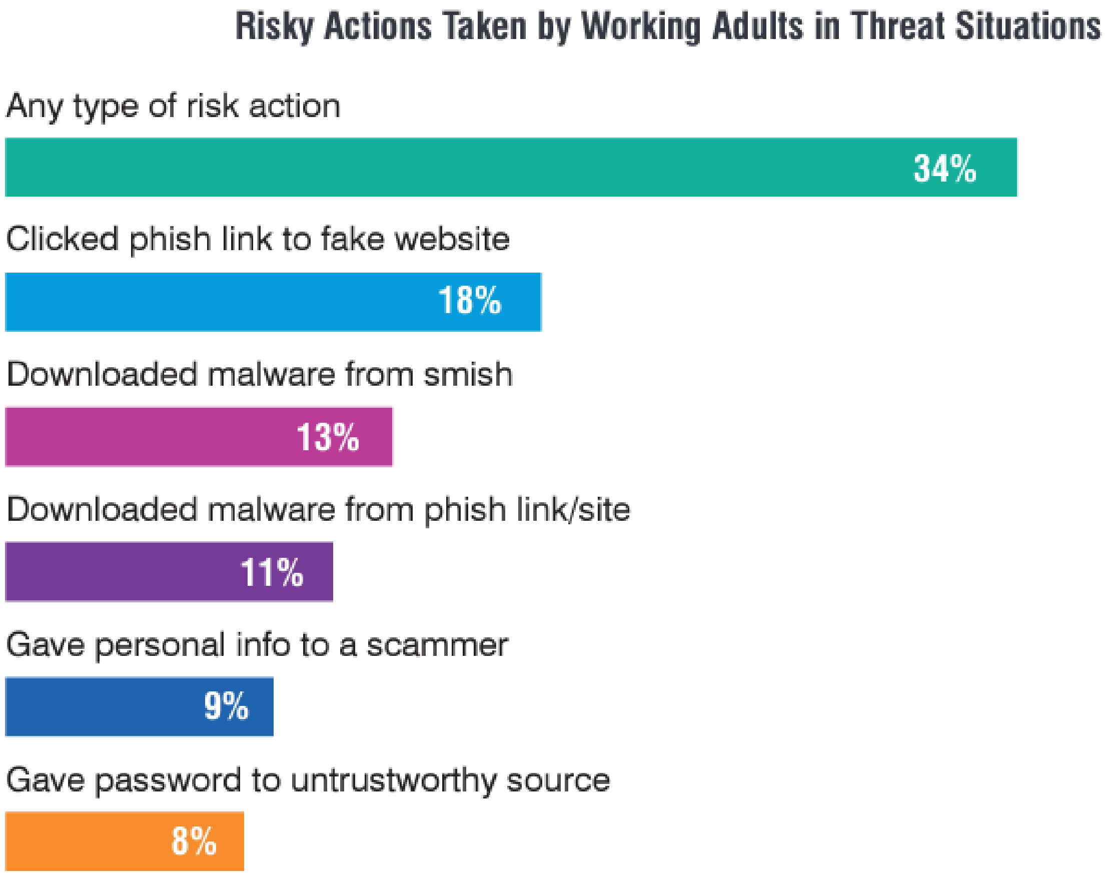
Use personal devices for work devices



Let family & friends use their work devices



Risky User Behavior



1/3+

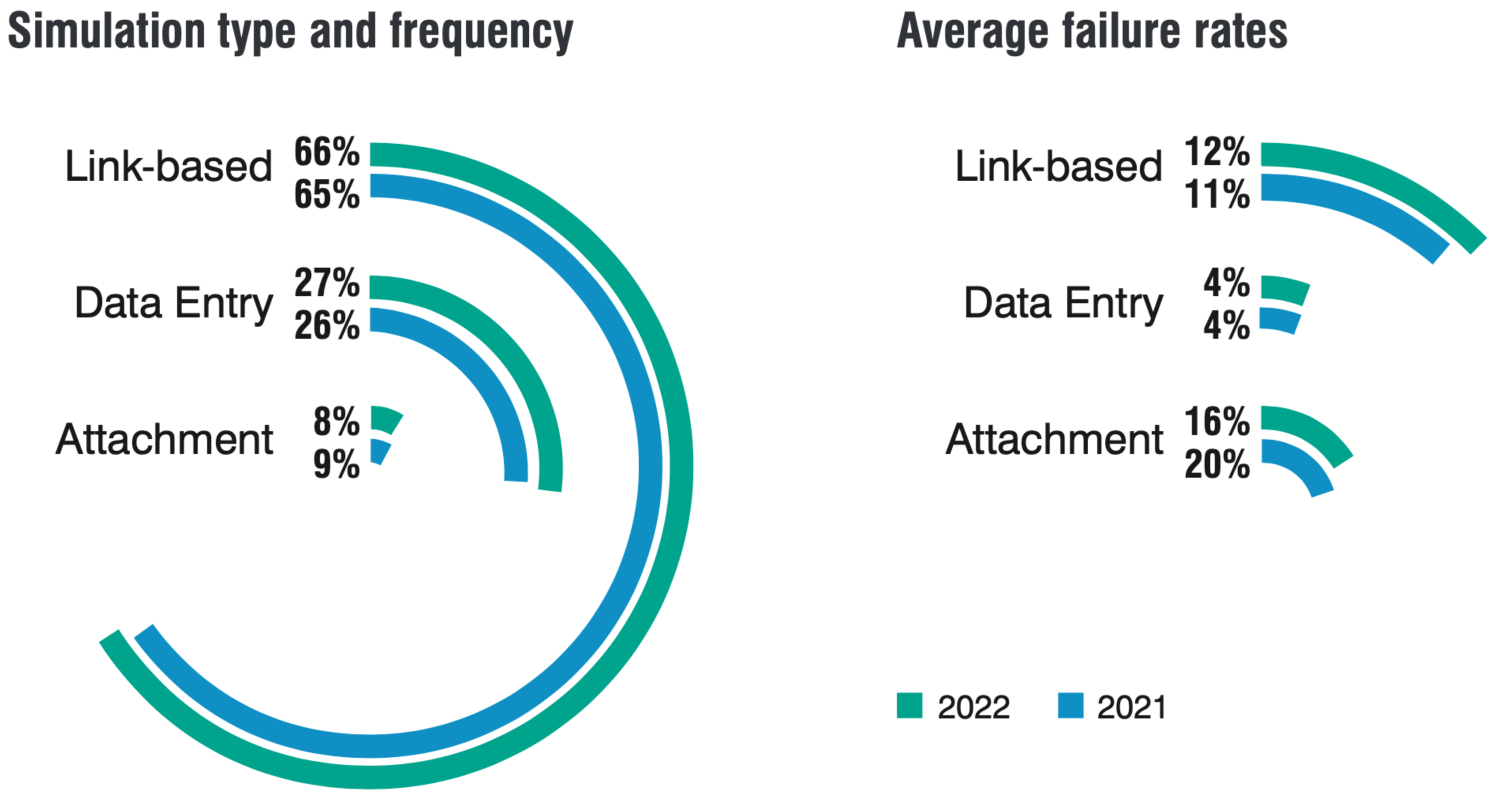
Of working adults took at least one risky action in 2022.

Failure Rates, Benchmarking, and Resilience

Simulation: Failure Rate

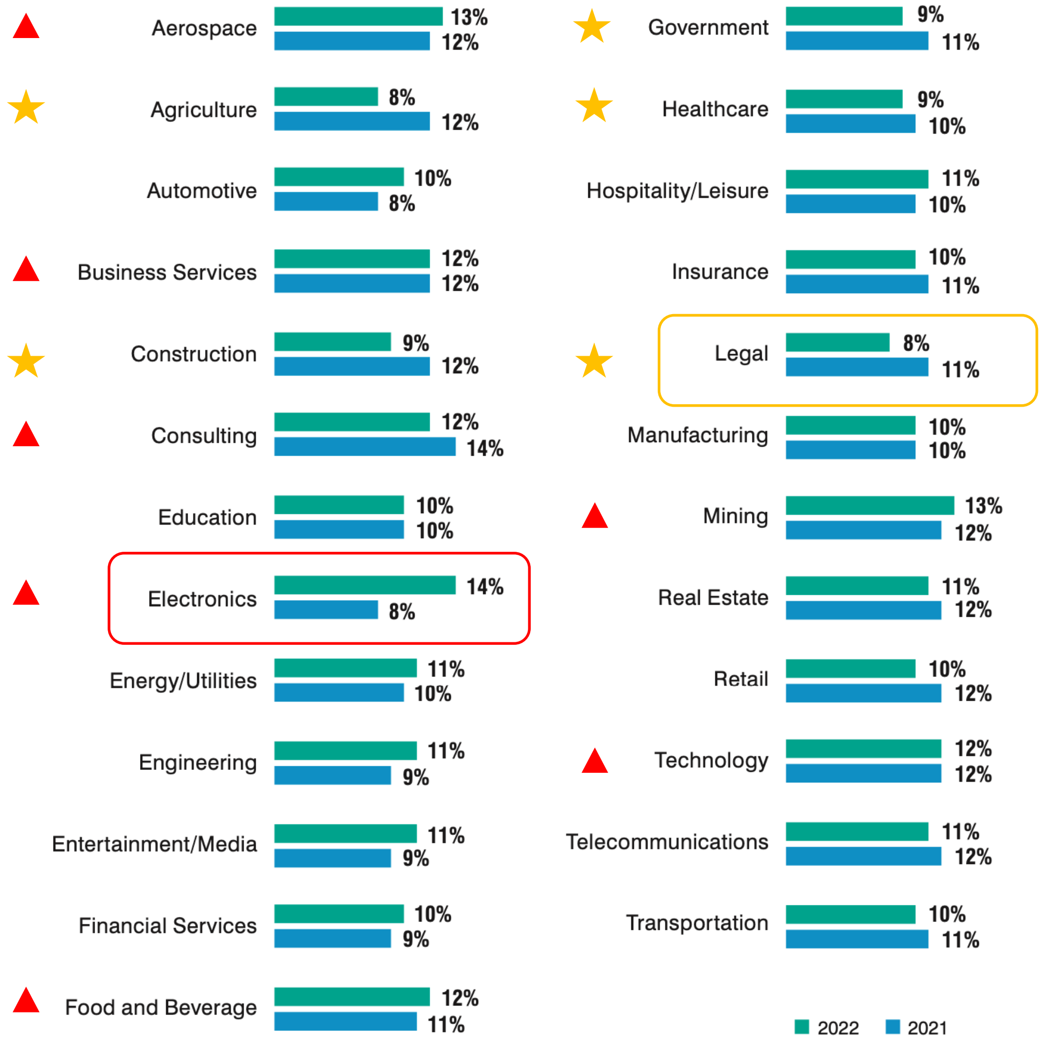
135M+

Simulated phishing tests sent by our customers in 2022



COVID-themed template has high failure rate

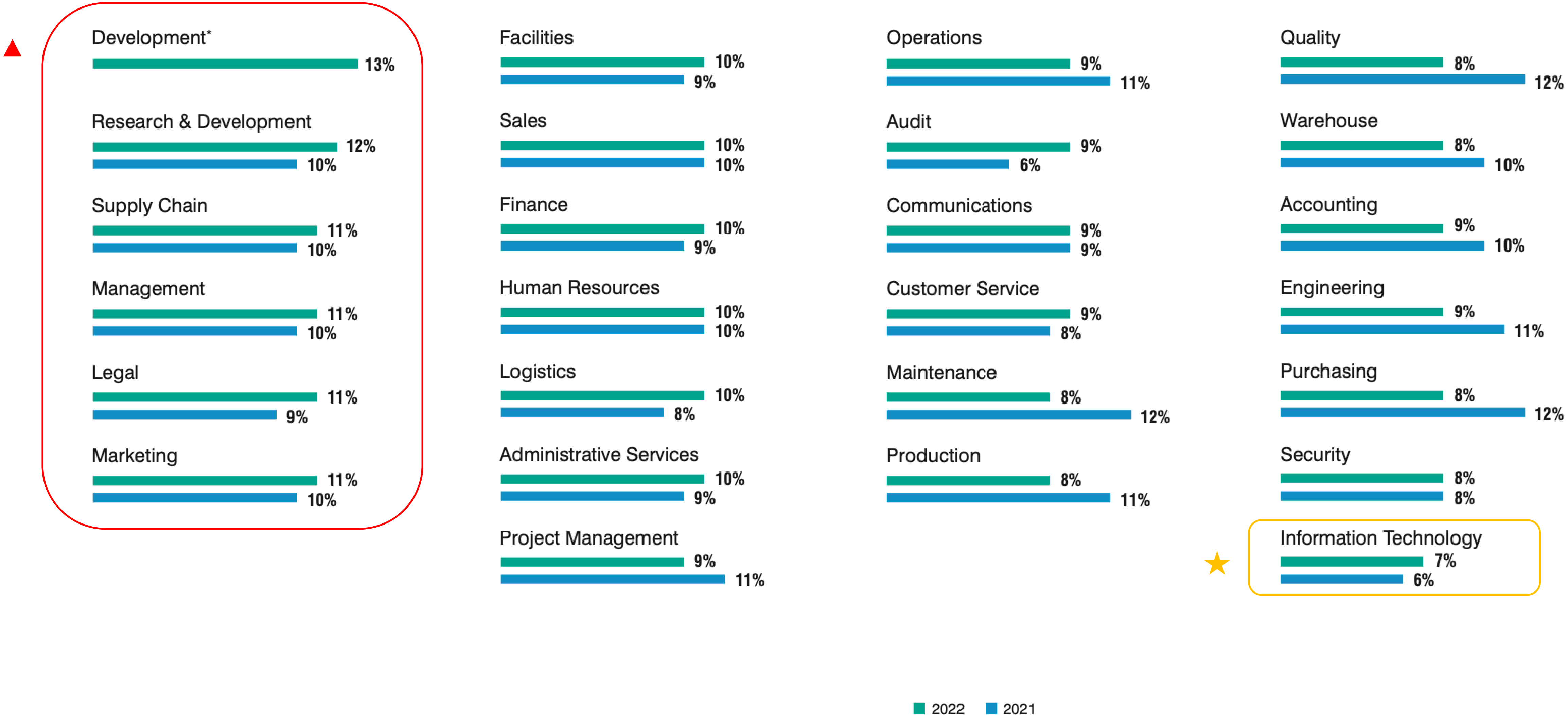
Failure Rates by Industry



11%

Overall average failure rate for phishing simulations

Failure Rates by Department



*New question for 2023 report

Reporting Rates and Resilience Factor by Industry

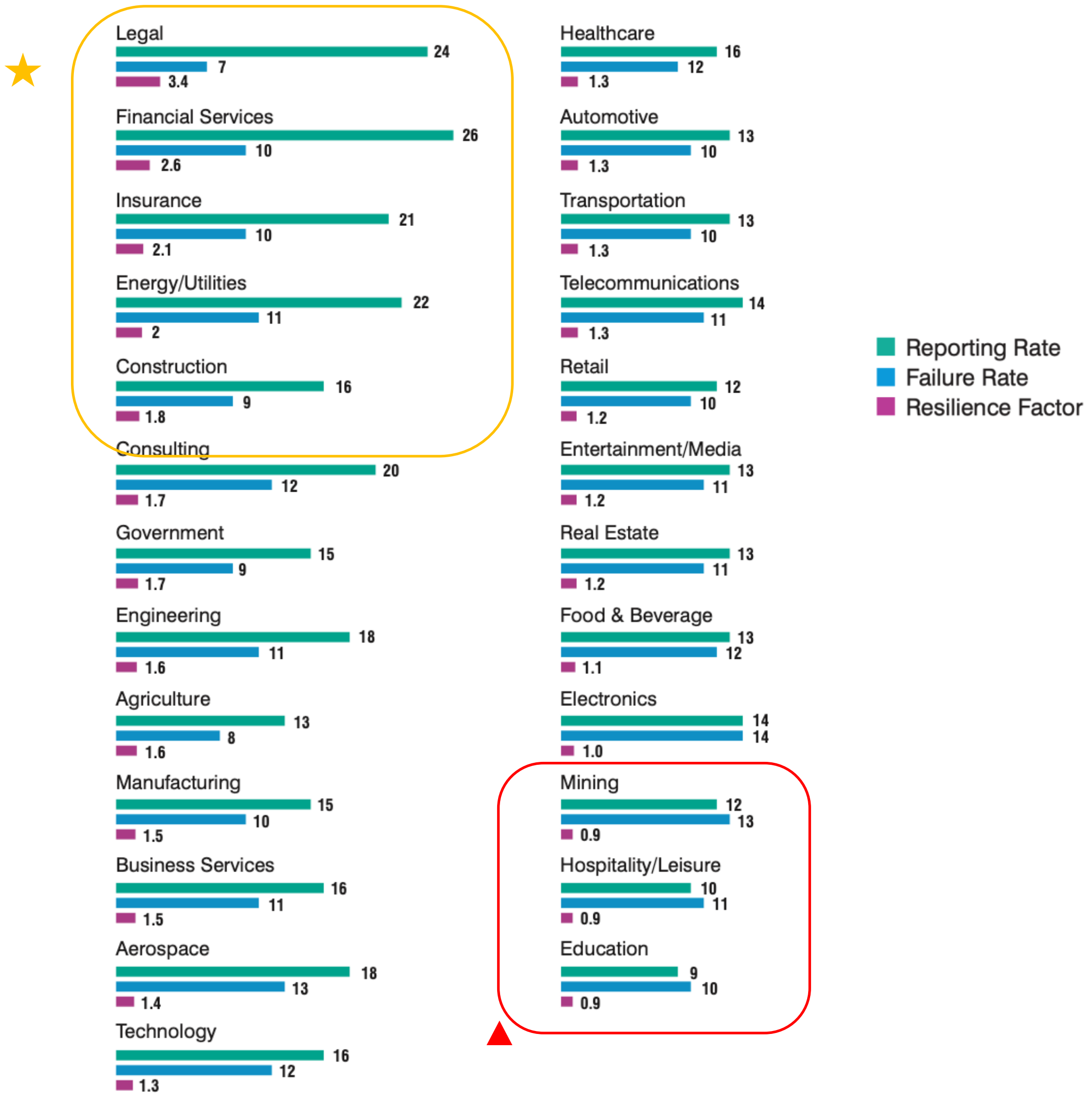
17% ÷ **10%** = **1.7**

Average reporting rate

Average failure rate

Resilience factor

(Up from **1.5**)



More Reasons You Want a Reporting Button

75M

malicious messages were blocked by Proofpoint as a result of user-reported suspicious emails

47M+
Credential Phishing

~600,000
Downloaders

1.5M+
Malware

260,000+
Keyloggers and Stealers

1.2M+
Banking Trojans

680,000+
Botnet malware

“Phishing has to be at the forefront of people’s minds. Even if we get to a point where we have an acceptable click rate, we just have to keep going.”

—Customer Security Manager & Security Awareness Lead
Financial Services (UK)

State of Security Awareness

State of Security Awareness Varies

In France 54% of respondents said their organisation runs a security awareness program. But…

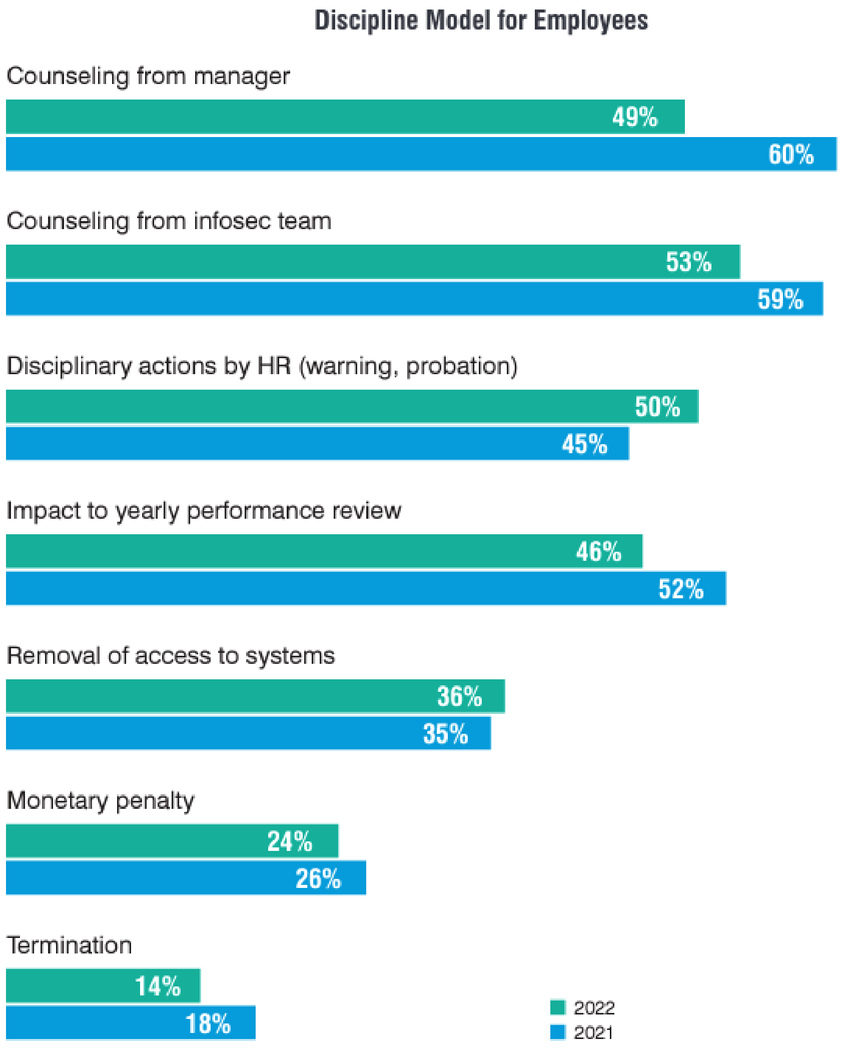
Only
74%
Of orgs with a program deliver formal training to users

Only
56%
of those train everyone in the organization

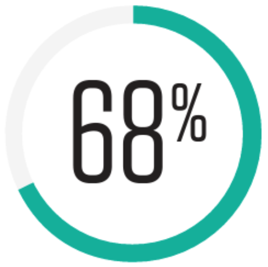
Only
30%
Conduct phishing simulations FR

27%
Said that failure rates had remained the same

To Discipline or Not to Discipline



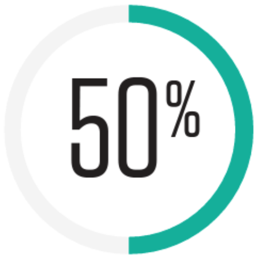
InfoSec



Said consequences had increased end users' overall phishing awareness

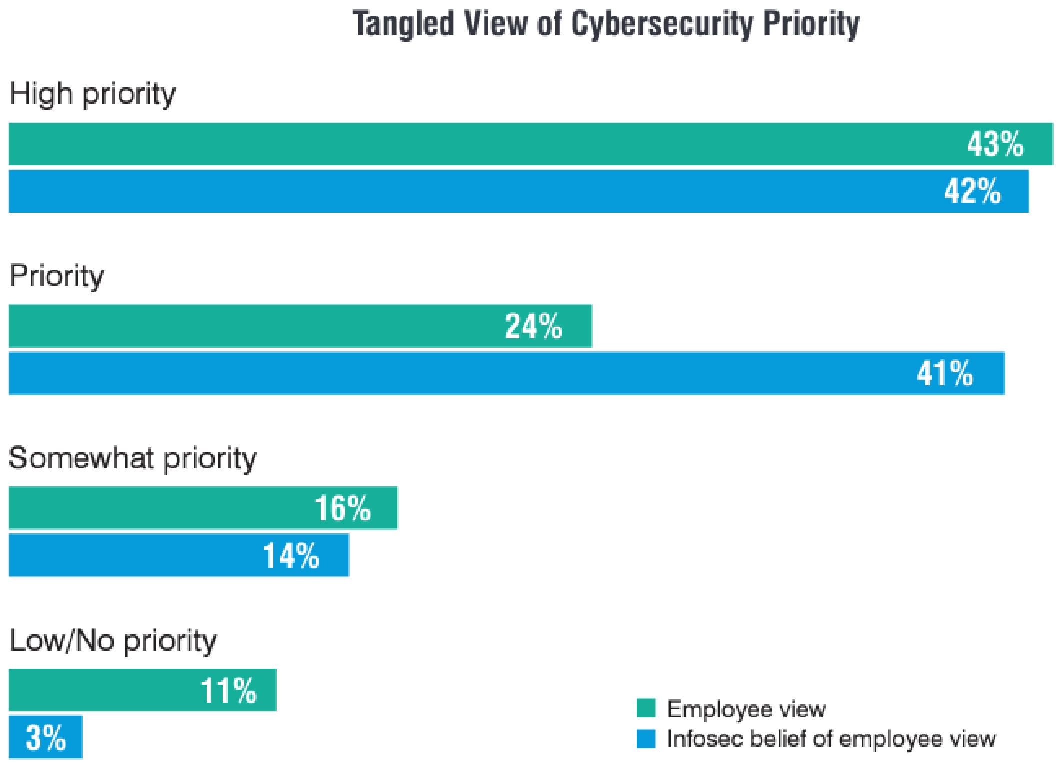
VS.

Employees



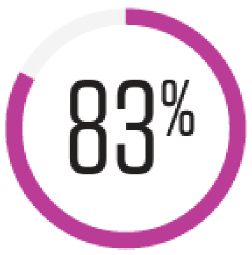
Complain about the consequence model

Security Culture is at a Crossroads



Tangled View of Cybersecurity Priority

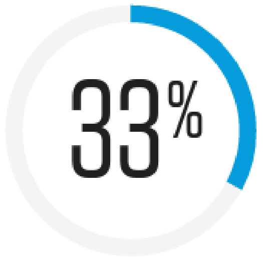
InfoSec



Feel employees think security is a top priority at work

vs.

Employees



Said cybersecurity is not a top priority of theirs at work

Key Statistics

30 Million

malicious messages sent in 2022 involved Microsoft branding or products

600K per day

$300-400K

telephone-oriented attack delivery attempts daily, with a peak of 600k per day in August 2022

1/3

of people took a risky action (such as clicking links or downloading malware) when faced with an attack

>1 in 10

threats were blocked as a result of user reporting

64% of organizations infected with ransomware paid a ransom

90% of organizations affected by ransomware held a cyber insurance policy

65% of organizations reported at least one incident of insider data-loss

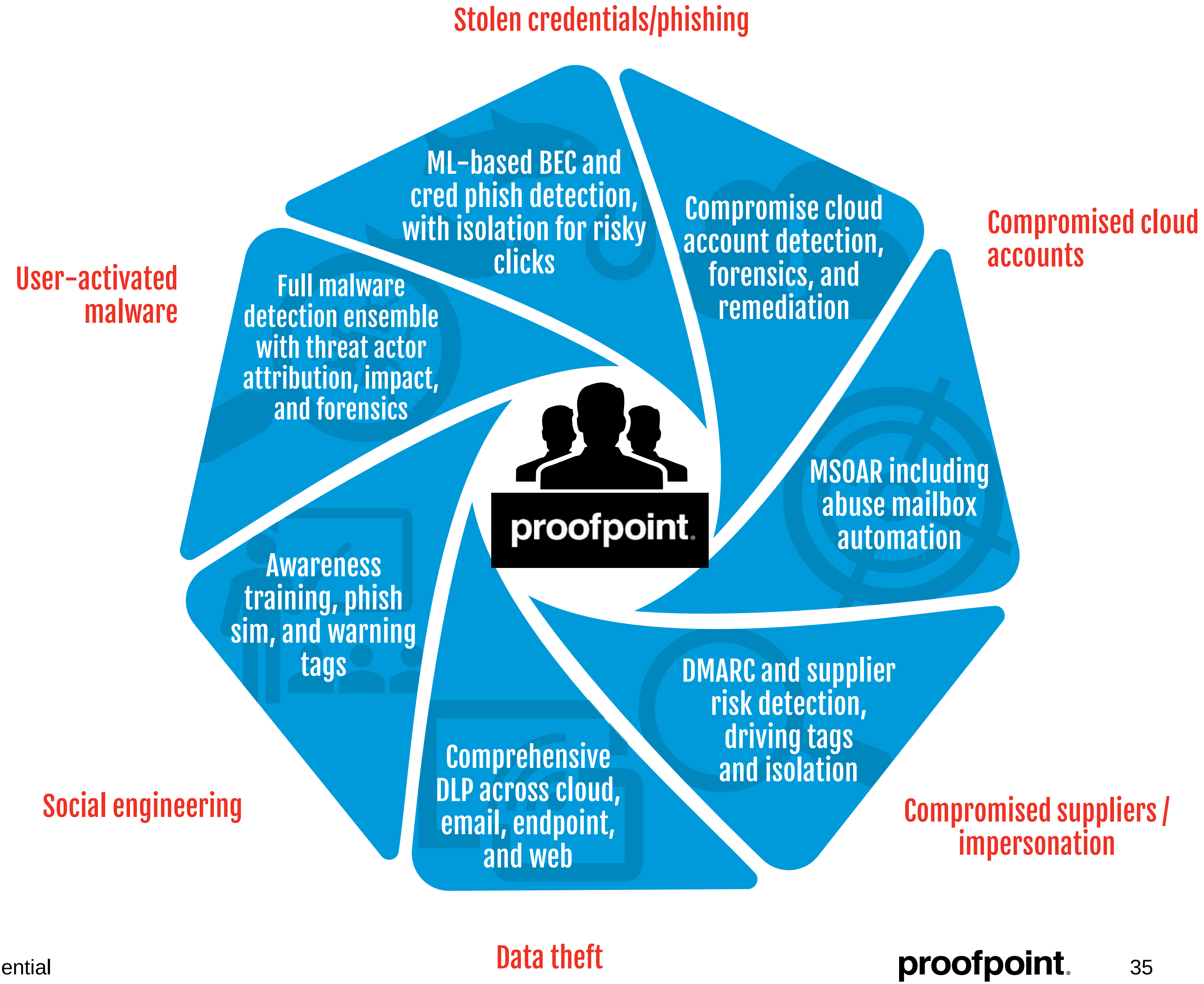
ONLY 56% of organizations with a security awareness program train all their employees

ONLY 35% of organizations conduct phishing simulations

PLATFORM APPROACH: THE RIGHT PROTECTION FOR THE RIGHT PEOPLE

"The evolution in threats has led to increased demand for other techniques and services, such as DMARC, cloud access security broker (CASB)/API integrations, continuous awareness and mail-focused security orchestration, automation and response (MSOAR)."

Gartner


Stolen credentials/phishing
ML-based BEC and cred phish detection, with isolation for risky clicks
Compromised cloud accounts
Compromise cloud account detection, forensics, and remediation
MSOAR including abuse mailbox automation
Compromised suppliers / impersonation
DMARC and supplier risk detection, driving tags and isolation
Data theft
Comprehensive DLP across cloud, email, endpoint, and web
Social engineering
Awareness training, phish sim, and warning tags
User-activated malware
Full malware detection ensemble with threat actor attribution, impact, and forensics
proofpoint.

Loïc Guézo
Director Cybersecurity Strategy
linkedin.com/in/lguezo
@lguezo
lguezo@proofpoint.com

Davide Canali
Threat Research Manager
linkedin.com/in/dcanali
dcanali@proofpoint.com

2023 State of the Phish Report

An in-depth exploration of user awareness, vulnerability and resilience

proofpoint.

Download

proofpoint®