proofpoint.

State of the Phish: At a Glance

INTRODUCTION

Cybersecurity can be tricky in normal times. In not-so-normal times—such as a global pandemic that leads to dramatic changes in work environments—it can seem downright overwhelming. Over the last year, information security professionals have faced a deluge of coronavirus-themed phishing scams and a continuing surge in ransomware attacks. At the same time, they have struggled to keep their users secure amid an abrupt shift to remote work.

Our 2021 *State of the Phish* report explores the effects of these trends and more. Analysing simulated phishing exercises, surveys and real-world cyber attacks, it explores today's biggest threats. It examines users' greatest vulnerabilities. And most important, it offers insights into what you can do about them.

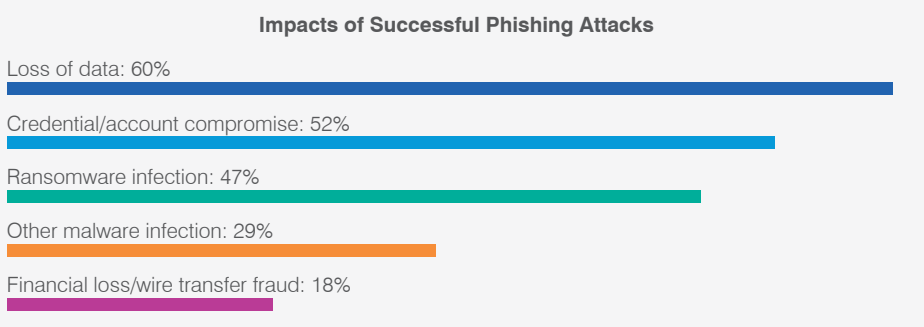
Here's an overview of this year's key findings.

THE THREATS ARE GROWING

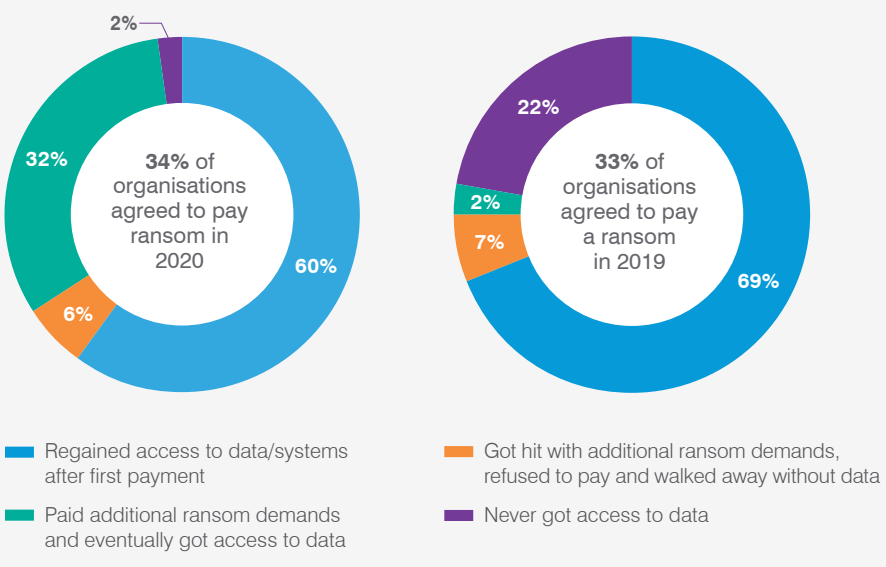
2020 was a banner year for phishing attacks, hitting victims in a multitude of ways.

57%

of respondents in a third-party survey said their organisation experienced a successful phishing attack in 2020, up from **55%** in 2019



A slightly higher percentage of ransomware victims paid attackers to regain access to their data and systems. But fewer got what they were promised, and nearly a third ended up paying additional ransom.



INTERNATIONAL

68% of US organisations said they paid a ransom in 2020, twice the global average

41% of Spanish organisations refused to pay a ransom after being infected, making them the least likely to negotiate with attackers

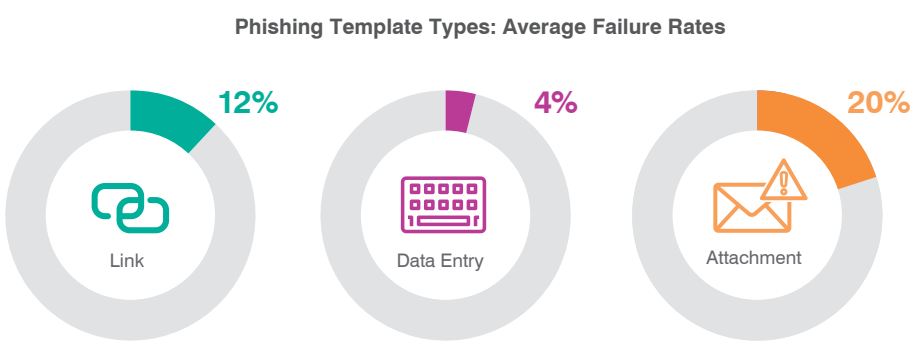
78% of French organisations were lucky enough to regain access to their data and systems after paying a single ransom, the highest of any region surveyed (the US was the second highest at **76%**)

14% of German organisations refused to pay a follow-up ransom, the highest among the regions surveyed

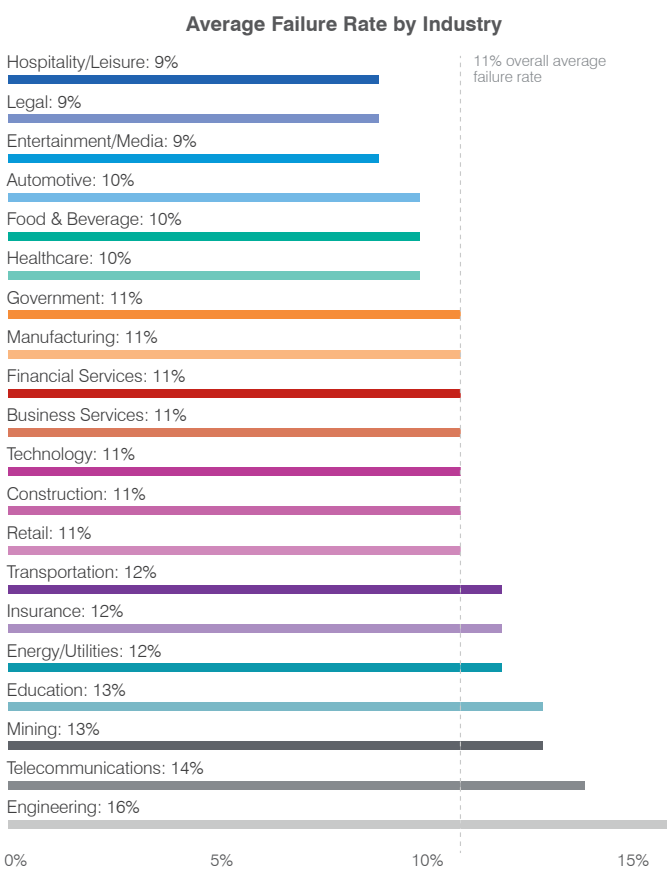
WHERE USERS ARE MOST VULNERABLE

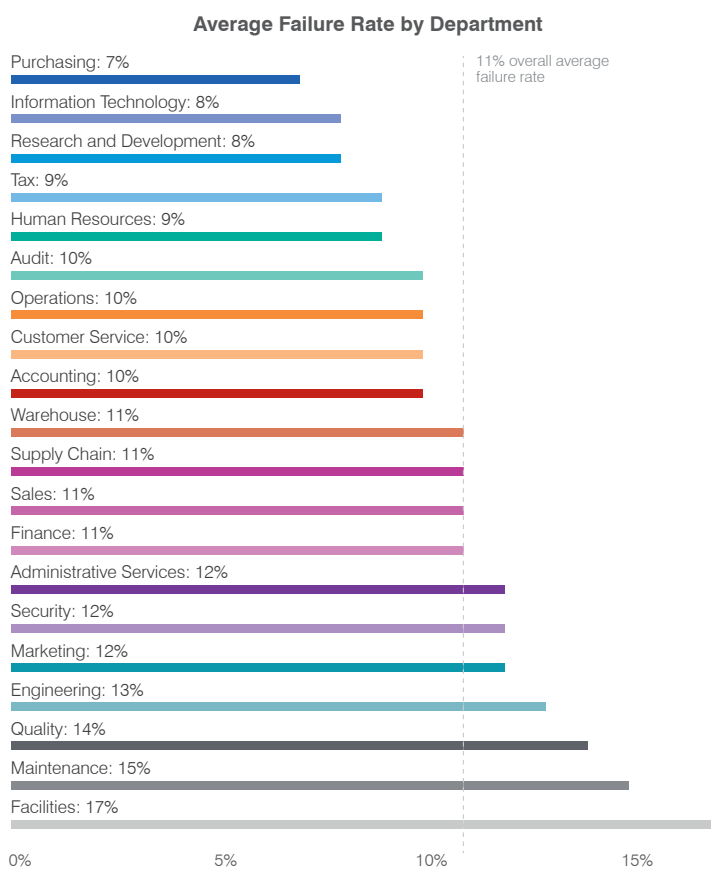
Today's attacks target people, not just technology. Knowing where users are most vulnerable is a critical part of equipping them to be more resilient.

More than 1 in 10 users clicked on a simulated phishing email. For phishing tests with attachments, that figure was 1 in 5.



Users in some industries are more vulnerable than others. The same goes for users in different departments.





Common cybersecurity terms may seem second nature to IT leaders, but many users don't know them.

Our "what is" survey questions offered three multiple choice answers and an "I don't know" option. Users who don't know an answer may pose as much risk as those who answer incorrectly.

What is **PHISHING?**

Correct	Incorrect	I Don't Know
63%	22%	15%

US workers scored lowest (52% correct)

UK workers scored highest (69% correct)

What is **RANSOMWARE?**

Correct	Incorrect	I Don't Know
33%	36%	31%

Just 26% of German workers were correct

42% of Australian workers were correct

What is **MALWARE?**

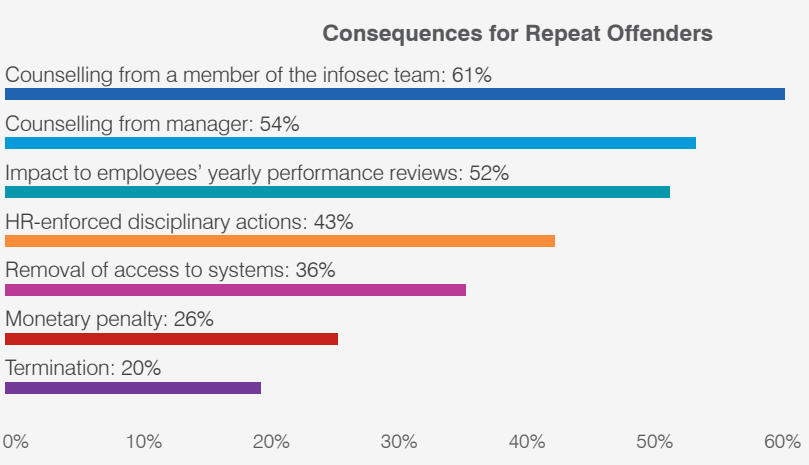
Correct	Incorrect	I Don't Know
65%	21%	14%

Spanish workers scored highest (75%)

US workers underperformed (54%)

HOW ORGANISATIONS ARE RESPONDING

While we don't recommend punishing users for honest mistakes, some organisations use a consequence model for "repeat offenders."



INTERNATIONAL

82% of US organisations use a consequence model, the most of all regions surveyed

72% of Australian organisations involve HR in disciplining repeat offenders

35% of Spanish organisations use a consequence model, the fewest of all regions surveyed

32% of UK organisations said their consequence model has not made a difference in employee awareness

30% of US organisations include termination as a consequence, the most of any region surveyed

GET THE FULL REPORT

Want to learn more? The 2021 *State of the Phish* report includes data from:

A third-party survey of	A third-party survey of	More than	About
3,500 working adults across seven countries (Australia, France, Germany, Japan, Spain, the United Kingdom, and the United States)	**600** IT security professionals across the same seven countries	**60M** simulated phishing attacks sent by our customers over a 12-month period	**15M** emails reported by our customers' end users

Get the report for a detailed picture of today's phishing threat and steps you can take to build a people-centric cybersecurity strategy that helps enhance user awareness, reduce risk and make your people more resilient.

www.proofpoint.com/uk/resources/threat-reports/state-of-phish

proofpoint.