Need to Know

Key findings from the *2023 State of the Phish* report

The increased risks of a hybrid workplace and increasingly advanced cyber attacks are well understood by CISOs. But have end users' security awareness and behaviours improved since last year? Unfortunately, the short answer is "no."

Attacks and the financial losses that stem from them soared in 2022 as user awareness stalled and some training metrics faltered. Here's a breakdown of our key findings.

44%

of people think an email is safe when it contains familiar branding

300K-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

76%

Increase in direct financial loss from successful phishing

30 Million

malicious messages sent in 2022 involved Microsoft branding or products

> 1 in 10

threats were blocked as a result of user reporting

ONLY 35% of organisations conduct phishing simulations

Even basic concepts are misunderstood

64% of organisations infected with ransomware paid a ransom

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

65% of organisations reported at least one incident of insider data loss

ONLY 56% of organisations with a security awareness programme train all their employees

of security professionals consider security a top priority at their company

VS.

of employees say cybersecurity is not a top priority of theirs at work

For more details, data and insight, download the *2023 State of of Phish* from Proofpoint.

proofpoint.

0704-002-02-01