German/US Expert Meeting

IT Security Association Germany (TeleTrusT) in cooperation with FIDO Alliance

San Francisco, 25.03.2026

Structural Phishing Risk and the Empirical Case for Cryptographic Authentication

Jan Hörnemann, AWARE7

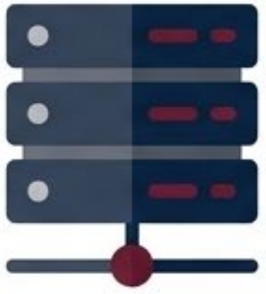
The Unprecedented Scale of the Empirical Baseline

3 Years

A definitive longitudinal analysis of human cybersecurity behavior.

36

Distinct enterprise organizations measured across three economic sectors.



96

Isolated phishing campaigns executed with controlled variables.

68,742

Total emails delivered, opened, and tracked for interactions.

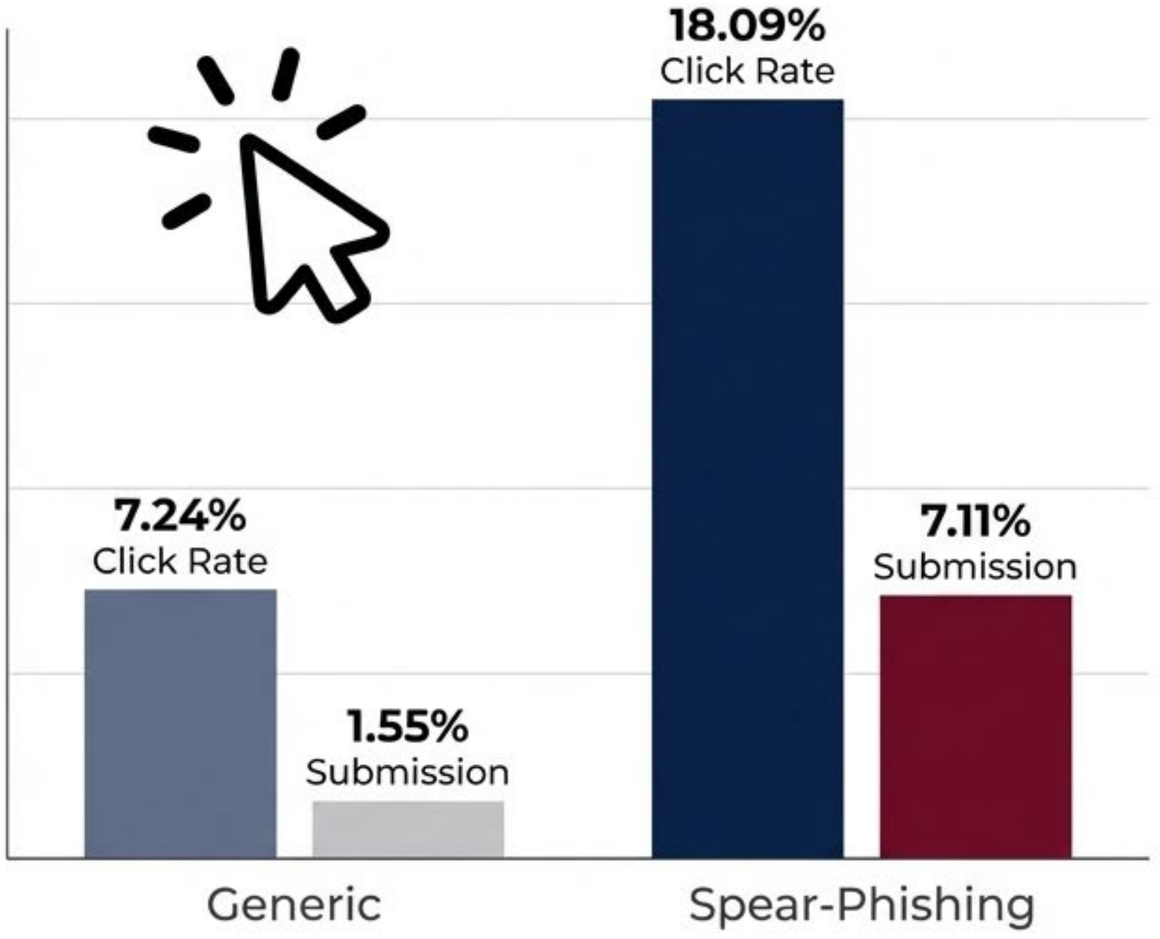
Targeted Intelligence Doubles the Baseline Human Failure Rate

Generic campaigns yield a 7.24% interaction rate and a 1.55% data submission rate.

Spear-phishing utilizes organizational intelligence to increase interaction to 18.09%.

When targeted, data submission escalates to 7.11%—a nearly five-fold increase in compromise risk.

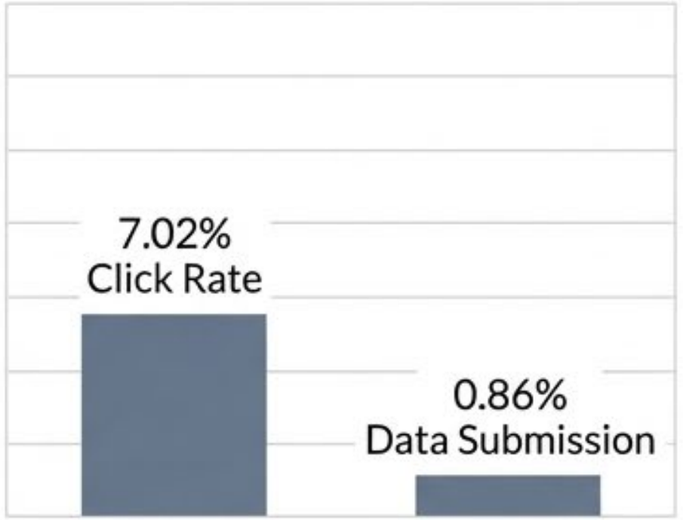
Half of all users who interact with a spear-phishing link proceed to submit sensitive data.



Systemic Variance Across Economic Sectors

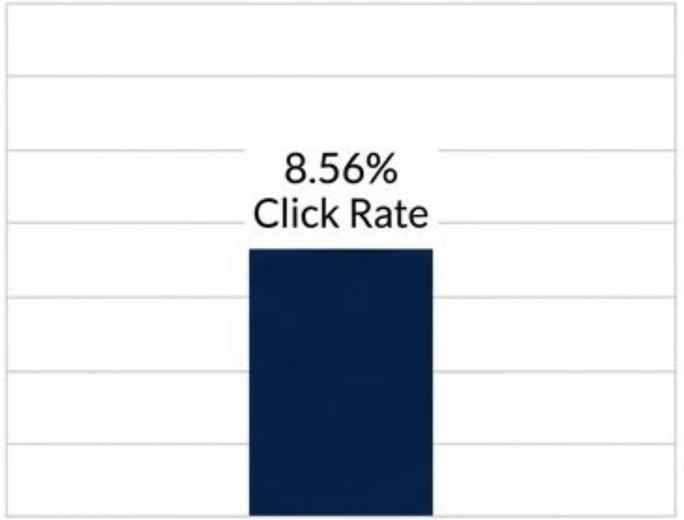
Vulnerability is not a uniform employee failing; it is a structural reality tied to the economic function of the organization.

Secondary Sector
(Manufacturing & Industry)



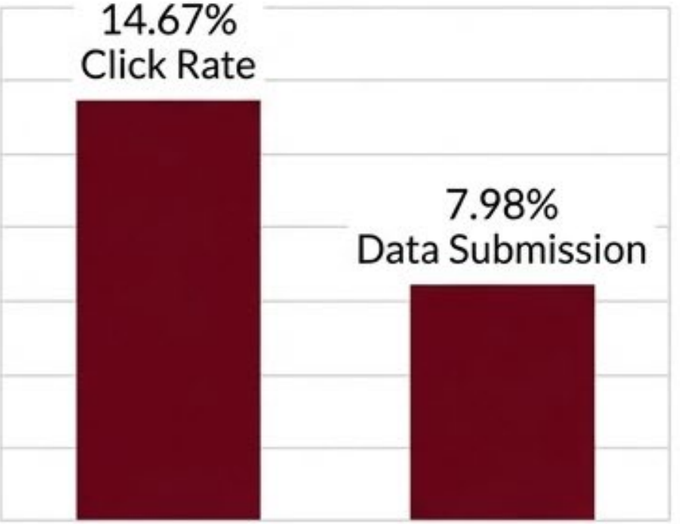
Exhibits the lowest vulnerability profile.

Tertiary Sector
(Services)



Demonstrates moderate baseline risk.

Quaternary Sector
(Knowledge-Based Services)



Represents the highest structural risk. Highly digitized environments maximize exposure.

Operational Necessity Drives Departmental Risk Profiles

Finance & Administration

Consistently exhibits the highest caution. **Lowest click rates at 8.25%.**

Sales & Marketing

Profound vulnerability driven by operational necessity.
53.2% Open Rate.
13.7% Click Rate.

External-facing roles require employees to engage with unknown communications and external links to execute their primary duties, driving inherent variance.

Moving Beyond Behavioral Vulnerability

Security Awareness Campaigns are necessary for baseline compliance (NIS2, ISO 27001).

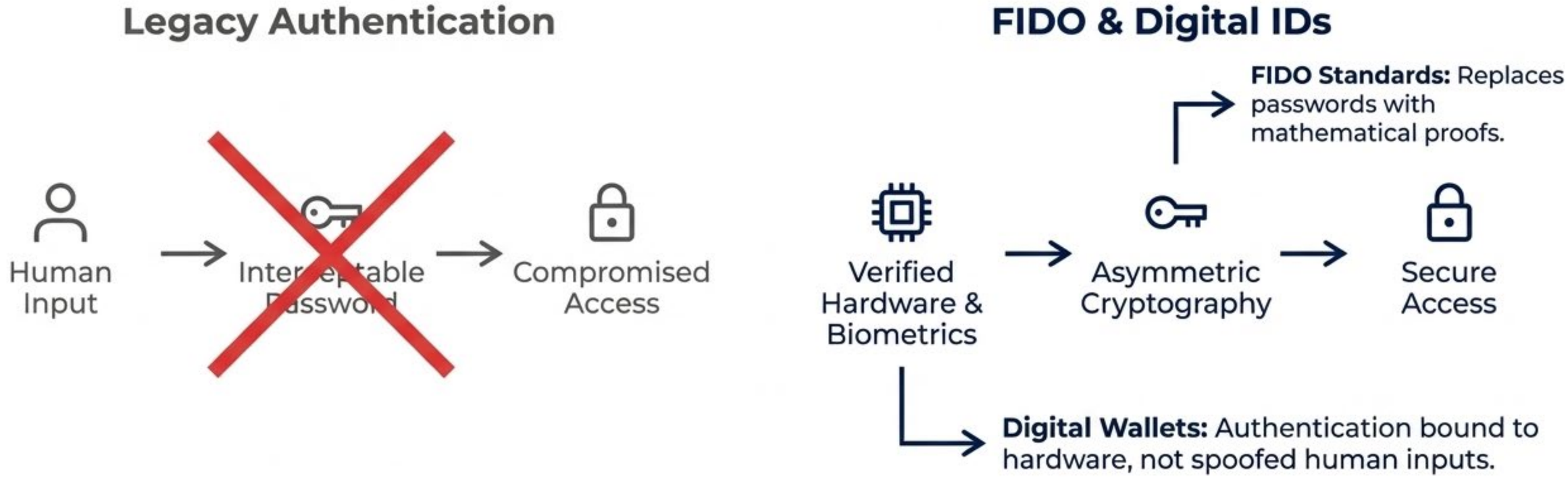
However, relying on human detection as a primary defense against credential harvesting is structurally flawed.

A minority of users will continually submit credentials, constituting a persistent, unsolvable risk.

The authentication loop must be re-architected to remove the human decision-making element.

The Strategic Imperative for Phishing-Resistant Architecture

Organizations must transition to cryptographic, phishing-resistant credentials. This architectural shift renders the established 18% spear-phishing click rates and 7% data submission rates strategically irrelevant.



Cryptographic Defense is the Definitive Response to Human Variance

The 68,000-email dataset proves that human susceptibility to phishing is a dynamic, persistent, and unpatchable baseline risk.

Vulnerability varies deeply by economic sector, departmental role, and attack scenario, making behavioral defense inherently inconsistent.

Securing the modern enterprise requires rendering credential harvesting obsolete through the immediate adoption of FIDO standards and Digital Identities.

AWARE