State of Global Enterprise Authentication

How modern enterprises are embracing phishing-resistant MFA
Executive Summary

The inaugural State of Global Enterprise Authentication Survey 2022, by Yubico, highlights the critical importance of using modern phishing-resistant MFA to protect your organization against cyber attacks. The new research also finds that while employees and enterprises across the globe are increasingly aware of the risks of cyber crime, many still leave themselves vulnerable by using legacy authentication methods and by failing to follow cybersecurity best practices.

In this exclusive preview, Yubico can reveal:

- **59% of employees** still rely on username and password as their primary method to authenticate into their accounts.
- **79% of VP-level staff** think their organization needs to upgrade to modern phishing-resistant MFA (like hardware security keys).
- **More than 54% of employees** are not required to go through cybersecurity training on a frequent basis.
- **54% of employees** admit to writing down or sharing a password in the past 12 months.
- **61% of employees** think their organization needs to upgrade to modern phishing-resistant MFA (like hardware security keys).
- **Nearly 40% of survey respondents** admit to have broken their phone over the last 2 years and **29% have lost it** (a device organizations commonly use to authenticate).

Yubico partnered with industry experts Censuswide to capture insights from employees across organizations in eight countries: the UK, the USA, Australia, New Zealand, Singapore, France, Germany and Sweden. Those surveyed ranged from entry-level employees to VPs, from sole traders to 2000+ employee enterprises.
The extensive report explores many facets of modern enterprise authentication, highlighting the severe consequences of cyber attacks. The survey finds that the majority of employees log into four or more accounts per day, yet most aren’t losing sleep about cybersecurity. However, almost half of C-suite executives and VPs admit to being kept up at night by concerns about getting hacked on private accounts and cyber attacks causing severe impacts to their organization.

Leaders are right to be worried. Yubico’s 2022 survey reveals concerning security failures globally. In the past 12 months, 61% of employees had an account reset due to lost or forgotten credentials, 54% had written down or shared a password and 40% of the respondents admitted to ignoring or not following a security protocol.

In the wake of a data breach, 15% of affected companies experienced severe damage to profits, 15% suffered severe reputational damage and 20% had to temporarily suspend operations.

To make the internet safer for everyone, leadership is required, and this is most visible in the US. Following President Biden’s executive order on cybersecurity, US enterprises lead all nations’ surveyed for discussion of cybersecurity at board meetings, security training and for leaders regularly discussing cybersecurity issues with employees.

The majority of respondents agreed that having credentials stolen was more concerning than missing out on their morning cup of coffee. The good news is, with YubiEnterprise Subscription Service, you can modernize your security and prevent account takeovers for less than the cost of a cup of coffee per employee per month. For more information, visit yubico.com.

59% of employees still rely on username and password as a primary method to authenticate into their accounts.

**Primary way(s) businesses authenticate into their accounts**

- **1%** Other
- **4%** None
- **7%** Don’t know
- **20%** Hardware security keys (eg. YubiKeys)
- **29%** Mobile TOTP/Push Authenticator apps
- **30%** Password manager
- **33%** Mobile SMS based authentication
- **59%** Username and password

*Multiple answers allowed*
More than 54% of employees are not required to go through cybersecurity training on a frequent basis.

61% of employees and 79% of VP level staff think their organization needs to upgrade to modern phishing-resistant MFA (like hardware security keys).

The majority of respondents agreed that having credentials stolen was more concerning than missing out on their morning cup of coffee.
Nearly 40% of the survey respondents admit to have broken their phone over the last 2 years.

Length of time since employees last broke their phones

- **40%** Within the last 2 years
- **15%** Within the last 5 years
- **36%** Never
- **9%** More than 5 years ago

29% of the survey respondents admit to have lost their phone over the last 2 years (a device organizations commonly use to authenticate).

Length of time since employees last lost their phones

- **29%** Within the last 2 years
- **10%** Within the last 5 years
- **53%** Never
- **8%** More than 5 years ago
Have you written down or shared your password in the last 12 months?

- 54% At least once
- 43% Never
- 3% N/A / Prefer not to say

54% of employees admit to writing down or sharing a password in the last 12 months.