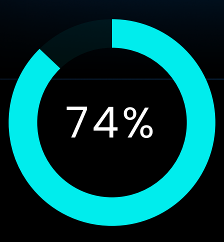
Are Your Identity Security Practices Keeping Up?

The CISA (Cybersecurity and Infrastructure Security Agency) includes single-factor authentication in their list of Cybersecurity Bad Practices.[1]

WHY?

74% of 2022 breaches involved the human element, including stolen credentials, according to the 2023 Verizon Data Breach Investigations Report.[2]



HOW SHOULD YOU RESPOND?

Cybersecurity authorities from the US, New Zealand, Canada, the Netherlands and UK say that "hardening credentials" with the use of MFA and strong password policies are best practices against the growth of cyberattacks.[3]

★ Bonus point – implementing strong identity security helps you qualify for the best cybersecurity insurance rates!

[1] https://www.cisa.gov/BadPractices
[2] https://www.verizon.com/business/resources/reports/dbir/
[3] https://www.cisa.gov/uscert/ncas/alerts/aa22-137a

Five Questions That Help You Choose the Right Identity Security Solution

1

Does the MFA solution use SMS-based verification as the primary or default authentication option?

SMS-based verification is less secure than other methods because it is vulnerable to hijacking.

2

Does it support offline authentication?

Employees need to access their laptops without an Internet connection - while on airplanes and when connecting to hotel or public Wi-Fi or when an Internet connection is spotty – and offline authentication is required.

3

Does it provide secure web single sign-on (SSO)?

Web single sign-on not only makes the solution easier, but also makes it more secure. Web SSO enables your company to deploy many different Cloud applications, while users only sign in once to access them, for fewer passwords, resets, helpdesk calls and happier employees.

4

Does it include credentials management tools, like a password manager and dark web monitoring?

With wide adoption of passwords rooted in 20+ years of systems and application development, passwords are here to stay…and they are one of the factors in MFA. Credentials management services enhance security with tools to boost protection against the inherent risks from poor password handling.

5

How much does the solution cost?

Free and low-cost consumer-grade products can be tempting, and pricing can be obscured in large software OS packages, so it's important to evaluate direct and indirect costs to see the full picture. Is support included – both technical support and subscription management support? Is there extra software you will need to license? Do you have a management interface that allows for corporate administration, reporting and visibility, or are you burdening your IT security team with added steps and costs? Are helpdesk costs increasing with usability shortfalls?

Get Started Today withAuthPoint Total Identity Security from WatchGuard

- Corporate Password Manager
- Dark Web Monitor
- Multi-Factor Authentication

One Answer to Keep Identity Real

To find out more, talk to your authorized WatchGuard reseller or visit https://www.watchguard.com/authpoint

ABOUT WATCHGUARD

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.