BlackBerry. Intelligent Security. Everywhere.

SCAM I AM:

The Trouble with Modern Authentication Approaches

THE AUTHENTICATION CHALLENGE

Sensitive data is increasingly being accessed by mobile and dispersed workforces from the cloud, resulting in a marked shift away from traditional security practices that focus on network boundaries and on-premises security controls.

In response, security practitioners are beefing up password policies, implementing two-factor authentication (2FA), and deploying identity and access management (IAM) systems.

When these security improvements create undue business friction, however, users may rebel by finding workarounds to defeat them, creating opportunities for cyber criminals to steal their credentials. Credential theft is alarming, not only because it provides opportunities for identity theft, but also because it's the number one mechanism attackers utilize to steal or compromise data.[1]

280%
The rise in the number of stolen credentials since 2016[2]

81%
The percentage of confirmed data breaches that involve weak, default, or stolen passwords[3]

$148
The cost per stolen credential[4]

TRADITIONAL AUTHENTICATION APPROACHES

In recent decades, IAM efforts have focused on developing new forms of:

1. **Knowledge** — Something the user **knows** (e.g., passwords)
2. **Possession** — Something the user **has** (e.g., a smart phone)
3. **Inherence** — Something the user **is** (e.g., biometrics)

Passwords leverage only the first category, although security practitioners have attempted to buttress their effectiveness by requiring frequent updates and by requiring so-called strong passwords that include a mix of at least six numbers, symbols, and letters.

More recently, 2FA controls have been introduced that require individuals to prove who they are based on two of these three factors.

WHY TRADITIONAL APPROACHES FAIL

* * * * * * * *

Password policies can be undermined by naive workers and those who practice poor security hygiene by leaving passwords exposed on their workstations, handing them over to adversaries conducting phishing campaigns, or sharing them with co-workers.

According to a recent **Ponemon Institute** survey:[5]

69%
of respondents acknowledge they share passwords with colleagues in the workplace

51%
reuse passwords across their business and personal accounts

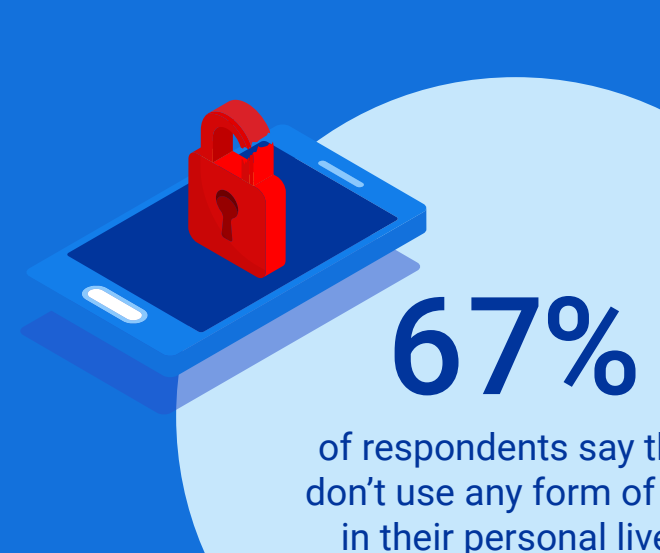
$5.2 million
Time spent entering and/or resetting passwords incurs productivity and labor loss costs of $5.2 million on average, per company surveyed

Frequent password updates are ineffective, since new passwords often resemble previous ones, and their predictability makes them easier to crack.[6]

2FA:

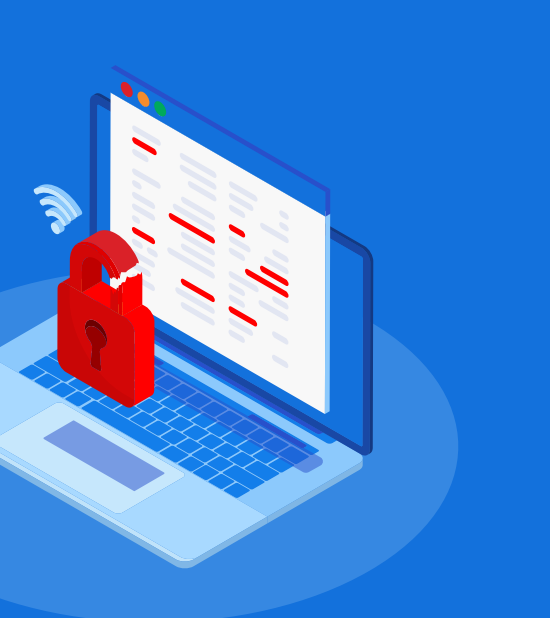
Two-factor authentication is also far from foolproof. Threat actors have introduced tactics, techniques, and procedures (TTPs) that overcome 2FA easily, ranging from bypassing it entirely (e.g., by using SMS), to directing victims to phishing sites that intercept and replay their 2FA codes.

According to the **Ponemon** survey:[5]



67%
of respondents say they don't use any form of 2FA in their personal lives

55%
say they don't use 2FA at work



And despite significant investments, 2FA adoption rates remain low.

THE WAY FORWARD

Overall, IAM approaches today are fragmented, inefficient, and a burden on users. Every new service spawns a new credential that assumes no prior knowledge of the user's identity or trustworthiness. This is expensive for the enterprise and a time-consuming deterrent for users.

At BlackBerry, we believe it's high time for practitioners to rethink their approaches to authentication while keeping the user experience in mind. In practical terms, this means transitioning to a Zero Trust security architecture that delivers a Zero Touch experience for users.

Here are three suggestions for helping security and risk management practitioners do so while guarding against the theft or compromise of enterprise credentials, improving the security of enterprise identities, and protecting sensitive systems and data.

1. USE INTELLIGENCE

Like 2FA, intelligent IAM controls utilize multiple contexts to authenticate users, including biometrics, location, and device and user characteristics. They can also spot anomalies in such measures, thereby enabling organizations to make weighted risk-based decisions on how much to trust each access attempt.

2. KEEP IT SIMPLE

There is no point in having the best security if people don't use it because it is too complicated. Use a solution that is based on public key infrastructure (PKI) that does not require passwords or additional hardware. Consider making the process smoother by implementing single sign on (SSO) authentication, which allows users to log on once to gain access to many different applications on a single device.

3. EVOLVE BEYOND JUST 2FA

Organizations need to adopt next-generation authentication tools that can provide strong protection of credentials using hardware-backed security. The toolset needs to use PKI in order to reduce the vulnerability associated with the use of codes and passwords in the authentication step; to use digital certificates, to create an unbreakable bond between users, authenticator devices, and their organizations.

Learn More

BlackBerry IAM solutions reduce friction and simplify access to your organization's critical applications, systems, and resources, streamlining the user experience while putting your security and IT team in full control. Learn more about the latest identity access management solutions from BlackBerry.

[1] Verizon 2020 Data Breach Investigations Report: https://enterprise.verizon.com/resources/reports/dbir/

[2] 2019 State of the Phish: Credential Compromise and Data Loss Have Soared Since 2016: https://www.secureworldexpo.com/industry-news/2019-sotp-credentials-and-data-loss

[3] The cybersecurity and identity gap survey: https://www.secureauth.com/resources/cybersecurity-and-identity-gap-survey

[4] Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

[5] The 2019 State of Password and Authentication Security Behaviors Report: https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf

[6] The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis: https://reitermk.github.io/papers/2010/CCS.pdf

BlackBerry.