



T. Daniels Consulting



Weak and Stolen Passwords: The Gateway to Data Breaches

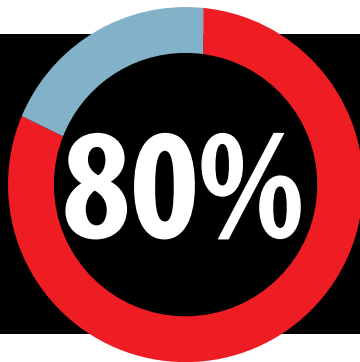
INTRODUCTION

Password security is one of the most important security issues that business owners face today. According to the 2021 Verizon Data Breach Report, 80 percent of data breaches involve weak or stolen passwords.

Every day, cyber criminals use stolen credentials to access and infect systems or steal data. What's most needed to reverse this trend is for authentication (known as multi-factor authentication or MFA) to require additional proof of identity beyond simple username and password, and to be widely deployed by all companies – no matter their size.

So, what is MFA? It is something you are already doing in your everyday life. Think about your bank. You go to login to their website and enter your username and password. Once confirmed, your bank will send a one-time code to your mobile phone or device. You then input that code to access your banking data. You need both your password and one-time code to get in-multiple factors of login credentials. **That is MFA.**

To better understand the current state of password security and MFA usage, WatchGuard commissioned a survey of small and midsize business owners and IT decision-makers at companies with less than 1,000 employees in the United States, the UK and Australia. Here's what was found.



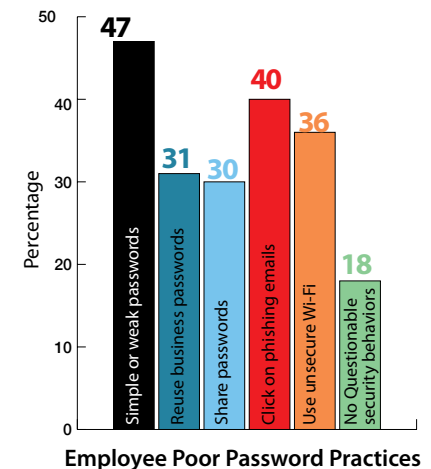
80 percent of data breaches involve
weak or stolen passwords.

THE CURRENT STATE OF PASSWORD SECURITY

Weak passwords are a serious problem, and the survey shows that 83 percent of business owners and IT decision-makers say their employees know that password best practices are important. Despite the fact that employers perceive a need for password security amongst their staff, they still have serious concerns about relying on passwords alone to protect company, employee, and customer data. In fact, 84 percent of respondents believe that weak passwords are responsible for up to 60 percent of all cyber attacks, which is actually low considering the Verizon report data mentioned above.

So, despite a general awareness of password best practices and security, proper execution of this knowledge falls short. Nearly half (46 percent) of respondents believe they can't force employees to keep strong passwords. Most of the businesses surveyed offer some form of password training or have policies in place to encourage best practices. This includes requiring employees to use long, complex passwords and change them periodically. But, they still believe their employees regularly engage in the following poor password practices:

- **47%** of respondents believe their employees use **simple or weak passwords**
- **40%** believe employees **click on phishing emails**
- **36%** believe employees use **unsecure Wi-Fi**
- **31%** believe employees **reuse business passwords for personal applications**
- **30%** believe employees **share passwords**
- **18%** believe their employees have **no questionable security behaviors**



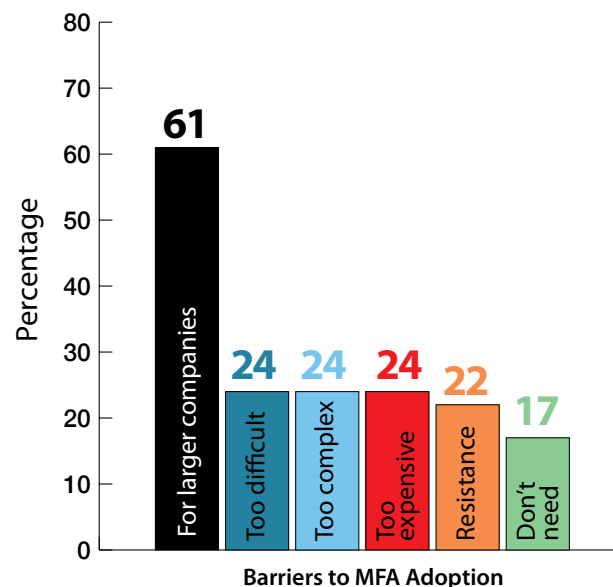
To address these issues, **84 percent of IT decision makers** at businesses with less than 1,000 employees said they would rather have **technology in place than rely on policies to enforce strong passwords**.

BARRIERS TO MFA ADOPTION

If IT decision-makers want technological solutions, and don't trust their employees to follow good password practices, why are more small businesses and mid-market enterprises not adopting MFA solutions?

Here's what businesses had to say about adopting MFA:

- **61%** feel MFA solutions are designed for **larger companies**
- **24%** say MFA is **too difficult** to maintain and support
- **24%** believe MFA is **too complex to implement**
- **24%** think MFA solutions are **too expensive**
- **22%** believe there is **inter-company resistance** to MFA
- **17%** say they **JUST DON'T NEED MFA SOLUTIONS**



These are all valid concerns (except for the last bullet point – our research clearly shows a need for MFA at companies of any size). **Businesses with limited IT resources need an MFA solution, like SecureFactor from T. Daniels Consulting, that falls within their price range and is easy to deploy and support.**

HOW COMMON IS MFA?

Of companies that don't have MFA, 83 percent are interested in using it, and 65 percent have plans to purchase in the future. There is clear momentum toward MFA solutions, even among companies with less than 1,000 employees. 67 percent of companies surveyed currently use some sort of MFA for at least some portion of their user population, and 29 percent do not use MFA at all. 29 percent is a significant number of businesses because it only takes a mistake from one employee to cause a data breach. Also, the 67 percent stat is deceptive, so let's dig into it.

Of companies that already use MFA:

- **56%** use **desktop authenticators**
- **47%** use **SMS (text messages)**
- **44%** use **mobile tokens**
- **40%** **don't know** the type
- **61%** use **Cloud-based authentication servers**



While it is good to see businesses using MFA, not all MFA methods are created equal. If businesses have MFA solutions that don't use advanced security methods, they're likely running an additional risk. SMS messages (such as text messages) for example, have been deemed an insecure method of authentication because they can be spoofed or intercepted by an attacker. Also, physical hardware tokens (such as a key FOB) pose a threat because they can be lost or stolen, resulting in a security gap that could lead to a breach.

CONCLUSION

MFA is no longer just for large enterprises. This survey found that although the majority of IT decision-makers at sub-1,000 employee companies have password policies and training in place, more than three-fourths believe their employees still engage in poor security behaviors. Also, nearly all respondents agree that a technology solution is needed to augment passwords.

SecureFactor from T. Daniels Consulting is a MFA solution that's affordable and addresses the perceived difficulties that keep businesses owners and IT decision-makers from embracing MFA. Ultimately, modern MFA is no longer an optional precaution; it is a business requirement.



Survey Details:

This survey was conducted by CITE Research on behalf of WatchGuard Technologies. It collected responses from 650 small business owners and IT decision-makers at companies with less than 1,000 employees in the United States, the UK and Australia.

PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

Minimize the risk of being one weak or stolen password away
from a data breach.

Enable SecureFactor today and safeguard your business.

To learn more or see a demo visit:
<https://www.tdaniels.com/secure-factor/>

T. Daniels Consulting
107 S. Walnut
Fenton, MI 48430
Phone: 810-629-0131