

# Secure Your Business with Strong Passwords and Multi-factor Authentication



In the 1983 movie *WarGames*, Matthew Broderick's character hacks into a powerful military supercomputer by correctly guessing a single password. Computers, hackers and cyber security have come a long way since the *WarGames* days. Now, savvy organizations use a combination of strong passwords and multi-factor authentication to secure sensitive data and processes.

## Password Evolution

Think of your early passwords. Perhaps you used a pet's name or your last name, followed by the month and year of your birth. (Perhaps you still use those passwords. If you do, change them. Now.)

Then, experts told users to add a mix of uppercase and lowercase characters, numbers, and special characters. Your password changed to *Snoopy42#*, and some services forced you to choose a new password every 90 days. As a result, you cycled through the same five passwords, occasionally changing the number.

Then, in 2017, the National Institute of Science and Technology (NIST) released updated [password guidelines](#). These guidelines emphasize password length over complexity. Specifically, they advocate using passphrases instead of passwords (for instance, *SnoopyLove\$P3anuts*). And they no longer advise frequent password changes.

## Passwords No Longer Enough

While the new guidelines help, passwords remain a problem. The average user needs to remember dozens, if not hundreds, of passwords. As a result, users develop bad habits, such as reusing passwords or writing them down. Additionally, when a hacker learns a password through [phishing](#) or keylogging, the complexity of the password makes no difference.



## Enter Multi-factor Authentication

Consequently, organizations increasingly turn to a combination of passwords and multi-factor authentication to keep the business and its data safe. Multi-factor authentication, sometimes referred to as two-factor identification, adds a layer of security by requiring multiple pieces of evidence to prove identity. This typically includes at least two of the following:

- Something you know – generally a password or PIN
- Something you have – this could include a bank card, a one-time passcode or a verification text or email
- Something you are – such as fingerprints, face or voice recognition

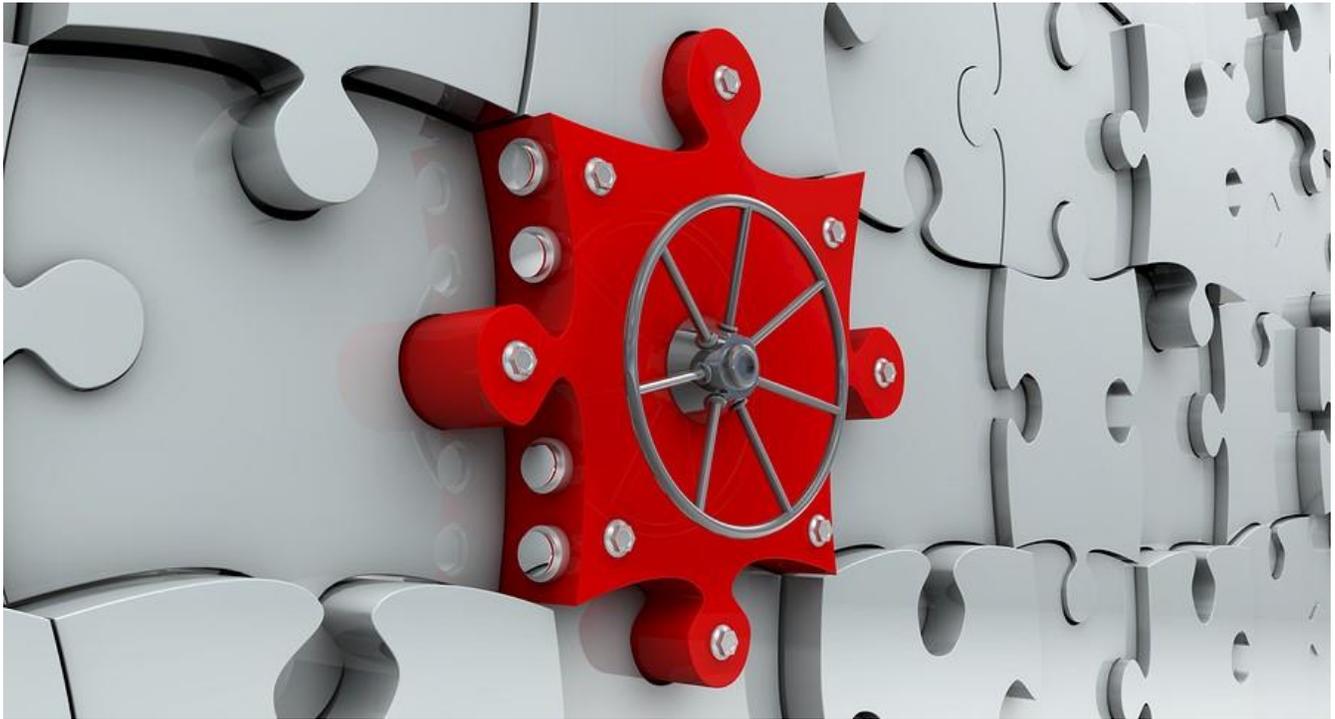
For example, when banking on a new computer, you might have to enter a code sent to your cell phone, in addition to your login and password.

## Moving Past the Barriers to Adopting Multi-factor Authentication

Recent studies indicate that use of multi-factor authentication has nearly doubled since 2017. While that research demonstrates a positive trend, additional studies show that small businesses have been slow to adopt multi-factor authentication.

Some users resist the added steps required to access necessary applications and networks. Additionally, multi-factor authentication solutions can prove complex and costly to implement.

However, organizations can no longer afford to choose convenience over security. Hackers see small to medium businesses as prime targets for attack. And companies can easily spend many times more recovering from an attack than they spend deploying multi-factor authentication.



Fortunately, multi-factor authentication offers a number of benefits to small businesses. Most important, it brings an extra layer of protection to critical assets. This added security strengthens regulatory compliance. Additionally, it demonstrates to customers that the business places a priority on the security of sensitive data.

## Strengthen Security by Combining Passwords and Multi-factor Authentication

Make the commitment now to secure sensitive data for your business and your customers with a layered solution that includes both passwords and multi-factor authentication. With decades of experience customizing [cyber security solutions](#) for businesses of all sizes, eMazzanti will help you find the right solution that balances security with usability.

2015 | 2013 | 2012 Microsoft  
Partner of the Year



**Inc. 500** || **5000**  
2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010



**ShoreTel Sky**  
Partner of the Year