What Is Two Factor Authentication, and Why Does It Matter?

2024-03-28 - Richard Woolf - General

You've likely seen security updates on your phone or computer asking you to set up 2FA or MFA to increase the security of your accounts. But what is two-factor authentication (2FA), and why does it matter?

What Is Authentication?

In the simplest terms, authentication is the process of providing proof of identity. There are three authentication factors.

- **Something you know.** Knowledge that only you possess such as a password, PIN, passphrase or the answer to a security question (e.g., What is your mother's maiden name?).

- **Something you have.** Something you possess such as a smartphone, hardware key or smartcard. As part of the authentication process, a user must provide a one-time passcode (OTP) sent to a smartphone, a unique code generated by a physical token or insert a smartcard into a device.

- **Something you are.** Biometrics information such as a fingerprint, iris or retina, voice or facial recognition, heartbeat or gait. Using biometric information as an additional authentication factor requires organizations to ensure the necessary scanning equipment is available during authentication.

Single Factor Authentication Is No Longer Sufficient

Most traditional systems still rely on single-factor authentication. With this approach, a user is only required to provide valid credentials (username and password) to prove their identity.

Due to weak passwords, data breaches, leaks of sensitive user data and password cracking tools, relying solely on user-supplied credentials is no longer sufficient to secure accounts.

Enter two factor authentication!

What Is Two Factor Authentication?

2FA is an authentication method that requires two forms of valid identification before access is granted to an account. It is a powerful tool that helps organizations protect their systems.

Benefits of 2FA

Businesses use 2FA to block unauthorized access to resources, preventing cybercriminals from accessing, stealing or destroying systems and data.

Some key benefits include:

- Increased security.
- Affordable implementation.
- Manageability and user-friendliness.

2FA Authentication Methods

Various authentication methods exist for 2FA, catering to different preferences and security needs. These include:

- **Voice-based authentication.** The user provides identity confirmation through automated voice prompts. Thanks to AI-driven deepfake voice-cloning, this method is increasingly at risk.

- **SMS verification.** A time-sensitive, one-time password (OTP) is sent via text message to a trusted phone number. Text messages are sent in plain text. Unfortunately, SIM swapping (aka SIM jacking) attacks make this method increasingly less secure.

- **Authenticator app.** An encrypted, time-sensitive OTP is sent to an authenticator app like Authy on your phone. This is a convenient, user-friendly approach that works well for most people.

- **Hardware tokens.** A hardware device is used that produces OTPs at regular intervals. Possession of the device is required to log in.

2FA vs. MFA: What's the Difference?

While these terms are often used interchangeably, there is a difference between 2FA and multi-factor authentication (MFA), which is the number of factors required to authenticate. Two factor authentication typically requires a password and an OTP. In contrast, MFA involves two or more factors presented during authentication to verify the identity of a user. It could be a password, an OTP and a fingerprint scan, for example.

While 2FA adds an essential layer of security for any account, organizations that require very high security such as healthcare facilities, government agencies or financial services, often opt for the increased security of MFA despite the increased costs and friction.

The term 2FA has fallen out of favor over time and most people now use MFA when referring to two or more factors required for authentication. For the remainder of this blog post, we use the term MFA.

MFA Implementation

Microsoft, Google and many other organizations have repeatedly

stressed the importance of using MFA to protect accounts. Here are some tips for a smooth implementation of MFA, from an expert IT support company:

- Any MFA method is better than none. Enable MFA on all accounts.

- SMS (text) based MFA is the most common and convenient method but is not secure as an authenticator app or a hardware key.

- Authenticator apps like Authy or Microsoft Authenticator are convenient and more secure than SMS-based MFA.

- Hardware tokens like a YubiKey are the most secure but least convenient option. For highly sensitive accounts or systems, it's wise to require hardware keys for MFA.

Risks of Not Adopting MFA

MFA is a relatively simple and inexpensive way to improve your security posture, especially if you require an authenticator app or hardware key for authentication. Lack of MFA during authentication exposes organizations to significant company-wide risks. Without this added layer of security, sensitive data becomes much more susceptible to unauthorized access and potential breaches.

Cybercriminals can exploit the absence of MFA to compromise employee accounts, leading to data theft, financial losses, downtime and damage to the company's reputation. Beyond

financial implications, a security breach may result in legal consequences, with potential regulatory fines for failing to protect confidential information adequately.

Is your organization vulnerable? Are you aware of security gaps? Consider getting a no-cost, no-obligation vulnerability assessment to locate any problem areas your business may have.

But this isn't just an issue for corporations, it extends to you as an individual. Without MFA, your personal accounts become prime targets for cybercriminals seeking unauthorized access to sensitive information.

The bottom line?

The absence of MFA leaves accounts exposed to cybercriminals, and it's only a matter of time before they are compromised with potentially catastrophic effects.

Why MFA Matters

Single factor, password-only protection simply isn't enough anymore.

Are your passwords strong enough? Check out InTrust's password management guide.

MFA matters immensely due to the increasing frequency and increasing impact of cybercrime. Personal and business information is becoming increasingly vulnerable, and MFA adds an extra layer of security. In many if not most cases, bad actors will move on to a softer target when they encounter MFA.

MFA mitigates risk by requiring additional verification step(s), which means that even if your login credentials are compromised, unauthorized access won't be granted. This enhanced security tool is particularly crucial for businesses safeguarding sensitive data, preventing potential breaches that could have severe consequences.

You should see adding MFA as a simple but effective step towards fortifying your defenses, both at work and at home for all your accounts.

If you want to learn more about cyber security and protecting your company from cyber threats, contact us or schedule a quick meeting with one of our certified cybersecurity experts.

Source: IntrustIT: What Is Two Factor Authentication, and Why Does It Matter? [February 28, 2024]