Content Brief	
Title	What Is MFA?
Article Type	Article
Category	Cyber-Tips
URL	/Cyber-Tips/what-is-mfa/
Title Tag	What Is MFA? | 2Secure Corp (64 chars)
Meta Description	What is MFA? Learn how it works and why it's essential to bolster your online security. Take the necessary steps today. (120 chars)
Keyword	what is mfa (4.4K), what is mfa in cyber security (590), how to do mfa authentication (20), what does mfa protect against (10)
Word Count	500 -1,000 words
User Intent	Informational: Users aim to find an answer to a specific question.
User Journey	Users start with learning about MFA and exploring how it enhances security by adding extra steps to protect against unauthorized access. They would also understand its effectiveness in reducing the risk of breaches.

Relevant Notes	Key internal link targets: ● Email security ● Blog/podcast - phishing emails ● Tech news roundup - mentions about MFA ● Podcast ● Cybersecurity consulting services Key external link targets: ● Microsoft Featured image: [insert image: alt text =”What is MFA”] For Chuck: any image/design ideas

H1: What Is MFA?

Protecting your online accounts is more important than ever. One of the most effective ways to improve security is through Multi-Factor Authentication (MFA).

According to Microsoft, MFA reduces the risk of account breaches by 99.22% and cuts down the risk by 98.56% even if your login details are leaked.[1] Impressive.

So, how does MFA work and how can you enable it to protect your accounts?

[*add call-to-action banner here*]

H2: What Is MFA In Cybersecurity

MFA is a security measure used to protect online accounts and systems. Instead of just asking for a single password, MFA requires users to provide more than one type of information to verify their identity.

Here’s how MFA works:

- **Something You Know**: This is usually a password or PIN. It’s the most common form of authentication, but on its own, it’s not very secure because passwords can be guessed or stolen.

- **Something You Have**: This is additional information that only you should have. It could be a smartphone, a special card, or a security token. For example, you might receive a code on your phone that you need to enter to log in.

- **Something You Are**: This involves biometric data like fingerprints, facial recognition, voice recognition, or iris scans, which depend on your distinctive physical characteristics.

MFA is commonly used for:

- E-wallets, email providers, and social media platforms use MFA to protect user accounts.
- Businesses, such as banks and online retailers, use MFA to secure sensitive data and systems.
- Healthcare systems use MFA to safeguard patient information.

Since MFA requires multiple forms of verification before granting access, it makes it much harder for unauthorized people to access your account.

H2: MFA vs 2FA

Two-Factor Authentication (2FA) is actually a type of MFA. The key difference is that 2FA specifically involves exactly two factors for verification. These two factors are usually:

- **Something You Know**: This is often your password.
- **Something You Have**: This could be a code sent to your phone or a security app.

For example, when you log into your email account, you first enter your password (something you know). Then, you receive a code on your phone that you need to enter (something you have). So, while 2FA is a simpler version of MFA that uses just two factors, MFA can involve more than two.

H2: How To Do MFA Authentication?

To use MFA authentication, you can simply follow these simple steps:

1. **Set Up Your Account**: Start by logging into the account or system you want to secure. Look for the security settings or options to enable MFA.
2. **Choose Your Methods**: You will need to select which types of verification you want to use. Common methods include:
   - **Password**: The first factor is your regular password.
   - **Phone Code**: You might get a code sent to your phone via SMS or an app.
   - **Authentication App**: You can use an app like Google Authenticator, Microsoft Authenticator, or Authy to generate codes.
   - **Biometrics**: This could involve using your fingerprint or face recognition.
3. **Add Your Phone or App**: If you choose to use a phone code or authentication app, you'll need to link your phone number or install the app. Follow the prompts to complete this setup.

4. **Verify Your Setup**: Once you've set up MFA, you may need to test it by logging out and then logging back in. You'll be asked to provide the second factor of authentication, like the code from your phone or authentication app, and then the next factor of authentication, like facial recognition.

If someone tries to log in using your stolen password, they would still need the code sent to your phone or generated by an authentication app to gain access. The extra steps help keep your account secure and your information safe.

Some systems allow you to set up backup methods, like a secondary phone number or email address, in case you lose access to your primary method.

[*add call-to-action banner here*]

H2: What Does MFA Protect Against

Seth Melendez, president of IT company WareGeeks Solutions and frequent guest on The Cybersecurity Insider podcast, likens MFA to taking medicine—it's not enjoyable, but it's necessary for security.

Here's what MFA guards you against:

Password Theft

If someone steals your password, they still need the second factor to access your account. For example, if your password is stolen but you have MFA set up with a code sent to your phone, the thief won't be able to get into your account without that code.

Phishing Attacks

In phishing attacks, scammers trick you into giving away your login details. Even if you accidentally give your password to a scammer, they can't get into your account if MFA is enabled, because they won't have the second factor.

Account Hijacking

This occurs when someone steals your password to access your account. Once they're in, they can change your settings, get your information, or impersonate you. MFA makes it harder for them as they need both your password and the second factor, such as a code sent to your phone or an authentication app.

Brute Force Attacks

These attacks involve trying many passwords until finding the right one. MFA stops these attacks because even if the attacker finds your password, they still need the second factor to access your account.

Man-In-The-Middle (MITM) Attacks

In an MITM attack, hackers intercept and alter communications between you and a website. MFA makes it harder for attackers to access your accounts because they need more than just intercepted information—they also need the second verification factor, like a code sent to your phone.

Both individuals and businesses benefit from using MFA, as it adds an extra layer of security that helps protect sensitive information and reduce the risk of unauthorized access.

[*add call-to-action banner here*]

H2: FAQ

H3: What Does MFA Mean?

Multi-Factor Authentication (MFA) means you need to provide two or more types of information to log in, like a password and a code sent to your phone. This extra step makes your accounts more secure by making it harder for someone to access them without your permission.

H3: How Do I Check My MFA Authentication?

To check your MFA authentication, log in to your account and go to the security settings. Look for options to review or manage MFA settings. You can see which methods are enabled and update them if needed. If you're unsure, follow the prompts for checking MFA or contact support for help.

H3: Why Is MFA So Important?

MFA is important because it adds extra security to your accounts. Instead of just using a password, MFA requires a second type of verification, like a code sent to your phone. This extra step makes it much harder for hackers to get into your account, keeping your information safer.

H3: How Effective Is Multifactor Authentication At Deterring Cyberattacks?

MFA adds extra layers of security; even if a hacker gets your password, they still need the second factor, like a code sent to your phone. 2Secure can help users and businesses keep their accounts and systems well-protected and reduce the risk of attacks.

[*add call-to-action banner here - maybe Contact Form?*]

Source:

1. Meyer, L., Burt, T., Romero, S., Weinert, A., Bertoli, G., & Ferres, J. (n.d.). How effective is multifactor authentication at deterring cyberattacks? https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW166lD