WebGuy IT Tech Tips

Proactive, not Reactive.

# Multi-Factor Authentication (MFA)

*Protecting Your Accounts with an Extra Layer of Security*

## What is MFA?

Multi-Factor Authentication requires you to verify your identity using two or more methods before accessing an account. Even if someone steals your password, they still can't get in without your second factor. Think of it as a deadbolt on top of your normal door lock. **MFA blocks over 99% of automated account attacks. Your password alone is not enough.**

## The Three Factors of Authentication

| Something You KNOW | Something You HAVE | Something You ARE |
|---|---|---|
| Passwords, PINs, security questions | Phone, authenticator app, hardware key | Fingerprint, face ID, retina scan |

## Why SMS/TXT Codes Are NOT Secure

Text message codes are better than no MFA at all, but they have serious weaknesses:

- ✕ **SIM Swapping** — Attackers convince your carrier to transfer your number to their SIM card.
- ✕ **Interception** — SMS messages can be intercepted through network vulnerabilities because they are transmitted as plain text.
- ✕ **Phishing** — You can be tricked into entering your code on a fake website.
- ✕ **No Encryption** — Text messages travel unencrypted and can be read in transit.

## Use an Authenticator App Instead — It's the Better Choice

Authenticator apps generate time-based codes directly on your device. They work offline, can't be intercepted over a network, and are immune to SIM-swap attacks. Scan the QR codes below to download one of the two most recommended apps:

| Microsoft Authenticator | Google Authenticator |
|---|---|
| Recommended for Microsoft 365 accounts | Works with Google, Amazon, social media, and more |

### Safety Tips — Protect Yourself Every Day

- ☑ Enable MFA on every account that supports it
- ☑ Use an authenticator app over SMS whenever possible
- ☑ Never share your MFA codes with anyone
- ☑ Save your backup/recovery codes in a secure location
- ☑ If prompted unexpectedly for MFA, do NOT approve it
- ☑ Report suspicious MFA requests to IT immediately