MULTI-FACTOR AUTHENTICATION APPS

USING AN AUTHENTICATOR APP IS SAFE, PRIVATE, AND SECURE.

Many people worry that installing an Authentication (MFA) app on their personal phone might give their company access to their device. Rest assured, this isn't the case.

MFA apps are specifically designed to add a layer of security when logging into accounts—they do not access, view, or interact with any personal information, apps, or data on your phone. When you use an MFA app, its only function is to generate a unique code that verifies your identity.

NO BUSINESS TIES TO YOUR PERSONAL DEVICE.

The authenticator app you use for work or personal accounts does not grant your employer (or anyone else) access to your device or personal data.

- **Independent of Company Networks:** Authenticator apps function separately from your company's network, operating solely on your device to generate secure login codes.
- **Flexible for Personal and Business Use:** If your organization requires an authenticator app, you can also use it for personal accounts without any conflict or repercussions.

Note: *An authenticator app never stores passwords or account details, meaning it only serves as a secure method to generate login codes, not as a gateway to your personal device or information.*

Key Benefits + How to Get Started

Its simple to use and setup is straightforward—install an app, scan a QR code, and you're ready to start generating secure codes.

One app can handle MFA for multiple services, streamlining security for both personal and business accounts. Your smartphone is all you need to add this extra layer of security.

1. **Download an Authenticator App:** Popular options include Google Authenticator + Microsoft Authenticator.
2. **Enable MFA in Account Settings:** Find the option to turn on MFA for each account—banking, email, social media, and work platforms.
3. **Scan the QR Code:** Link the account by scanning the QR code provided when enabling MFA.
4. **Store Backup Codes:** Securely save backup codes for account recovery if you lose access to your phone.

WHY MFA IS CRITICAL FOR BOTH PERSONAL AND BUSINESS SECURITY

Enhanced Security for Personal Data

- **Prevent Identity Theft:** MFA helps to prevent unauthorized access, protecting your identity and personal information if your password is compromised.
- **Protect Financial Information:** Accounts connected to financial services or sensitive data are especially vulnerable. MFA offers an additional barrier to deter cybercriminals.

Safeguard Business Resources

- **Keep Work Accounts Secure:** Businesses face daily threats from hackers seeking access to corporate networks. MFA limits potential breaches, keeping company data safe.
- **Meet Compliance Requirements:** Many industries now require MFA as part of cybersecurity compliance. This safeguard helps your organization stay compliant while protecting proprietary data.

STAY SECURE – PROTECT ALL OF YOUR ACCOUNTS

MFA is a simple but powerful tool to protect yourself and your business from potential cyber threats. Embrace the additional security without concerns about privacy and enjoy peace of mind knowing your personal and professional accounts are safeguarded.