How to implement Multi-Factor Authentication Cheat Sheet

Step 1: Choose Your MFA Method

You'll typically need two forms of verification:

- **Something You Know:** Your password or PIN.
- **Something You Have:** A device like your phone or an authentication app.
- **Something You Are:** Biometrics like a fingerprint or face scan.

Most platforms allow you to pick the method that suits you best.

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring multiple methods to verify your identity. It's like locking your front door and needing a key and a fingerprint to get in.

Step 2: Set up MFA on your device

Email Account (Google and Outlook)

Google (Gmail):
1. Go to your Google Account settings.
2. Click on "Security" in the left-hand menu.
3. Under "Signing in to Google," find "2-Step Verification" and click "Get Started."
4. Choose your method: Google prompts, text messages, or authenticator apps.
5. Follow the on-screen steps to verify your choice, and you're done!

Outlook (Microsoft):
1. Go to your Microsoft Account.
2. Click on "Security" then "Advanced Security Options."
3. Under "Two-step verification," click "Set up."
4. Follow the steps to choose your second factor: email, phone, or app.

For Work or Personal Computers

Windows 10/11:
1. Go to "Settings" > "Accounts" > "Sign-in options."
2. Under "Windows Hello," set up facial recognition, fingerprint, or PIN.
3. Add a second factor like a security key or app if prompted.

Mac (macOS):
1. Go to "System Preferences" > "Apple ID" > "Password & Security."
2. Click "Turn on Two-Factor Authentication."
3. Follow the steps to confirm and set up the second layer.

The Truth is in the Details

Cyber Security Awareness Month 2024
Look Closer. Think Smarter.

How to implement Multi-Factor Authentication Cheat Sheet

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring multiple methods to verify your identity. It's like locking your front door and needing a key and a fingerprint to get in.

For Social Media (Facebook, Instagram, X)

Facebook:
1. Go to "Settings & Privacy" then "Settings."
2. Click on "Security and Login."
3. Scroll to "Use two-factor authentication" and click "Edit."
4. Choose your security method: app, text, or key, then follow the instructions.

Instagram:
1. Go to your profile and tap the menu in the top right.
2. Select "Settings" > "Security" > "Two-Factor Authentication."
3. Tap "Get Started" and choose between an authentication app or text message.

X (formally Twitter):
1. Click "More" on the side menu, then "Settings and privacy."
2. Go to "Security" then "Two-factor authentication."
3. Select your preferred method, follow the instructions to verify it, and you're set!

Authenticator Application

Authenticator apps are fast and convenient, perfect for generating temporary codes.

Recommended Apps:
- Google Authenticator
- Microsoft Authenticator
- Authy

To Install:
1. Download the app from your app store.
2. Open the app and add an account by scanning the QR code from the service you're securing (like Google or Facebook).
3. Enter the code generated by the app on your service's website to verify.

Cyber Security Awareness Month 2024
Look Closer. Think Smarter.

The Truth is in the Details