******

***Convenient and Open Multi-Factor Authentication (MFA) Methods!***

CATIC has been a strong advocate in the MFA arena, as this technology is often successful in deterring threat actors’ unwanted advances. Cybersecurity experts have noted that most account-compromised attacks can be prevented if MFA is incorporated into a company’s environment, particularly if an authentication app is in play. We know MFA is an authentication method that requires authenticating one’s identity through two or more technological factors. In other words, MFA uses something a user knows (username/password), has (possession-based), and is (biometric). The “**two or more**” elements mentioned is crucial, because threat actors may have your credentials from a phishing endeavor. However, should they try to sign in with your credentials elsewhere, MFA should stop this attempt based on your location, IP, access to device, etc. This avoidance is critical, especially in our industry where wire fraud is rampant.

While MFA’s abilities to prevent possible attacks may seem costly, it is quite the opposite. Fortunately, there are many **free** and **reputable** applications to download for MFA. In addition to applications, there are many inexpensive tools that can promote MFA as well. Even better, should one not want to download an application or purchase a device for MFA, most providers offer a text and/or call within their platform to authenticate one’s identity. Below you will find a list of reliable MFA providers, as well as quick guides on setting up MFA via Gmail, Yahoo, etc.

***Free* MFA Apps for Android and iOS:**

* **Microsoft Authenticator:** Microsoft’s product has earned favorable reviews across the board from experts. Authenticator offers secure password generation, and this app allows you to add school/workplace accounts. With Authenticator, you can also require a PIN code before you can see the MFA codes on the screen, which only adds to the security of this software.
* **Auth0 Guardian:** Okta owned, and an MFA choice that CATIC already offers its agents when accessing catic.com. Auth0 primarily focuses on push notifications as its form of confirmation. Once a push notification is sent to your device, you have the option to approve it, and to have it remember your device for 30 days.
* **Authy:** A Twilio product, which offers password protection, cloud backups, and MFA. Authy is traditionally used with Gmail, password managers, and social media accounts.

***Physical* MFA Tool:**

* **YubiKey:** A productthat has various devices and sizes for your computers. Relatively inexpensive ($45-$85), YubiKeys can work with a plethora of accounts, such as Google, Microsoft, Amazon, Apple, etc. Its “claim to fame” is often cited within its ability to reduce account takeovers. YubiKeys are hardware-based, and its authentication secret is stored on a separate secure chip built into the YubiKey, with no connection to the internet so it cannot be copied or stolen.

*As a disclaimer, you should always validate this information with your IT Department and/or consultant, as products can have different instructions:*

**Gmail MFA Setup:**

1. Open your Google Account.
2. In the navigation panel, select Security.
3. Under “Signing into Google,” select “2-Step Verification” and then “Get started.”
4. Follow the on-screen steps.

URL: <https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3DDesktop>.

**Yahoo MFA Setup (Phone Verification):**

1. Sign into your Account Security page (login.yahoo.com).
2. Next to "2-Step Verification," click Turn on 2SV.
3. Click Get started.
4. Select Phone number for your 2-step verification method.
5. Follow the on-screen prompts to complete the process.

URL: <https://help.yahoo.com/kb/sln5013.html?guccounter=1>.

\* Statistics were derived from zdnet.com, support.google.com, help.yahoo.com, and yubikey.com.\*

**© CATIC – All Rights Reserved.**

**building partnerships together.**