TN Department of Finance & Administration | Strategic Technology Solutions

2022 NCSAM National Cybersecurity Awareness Month

#SeeYourselfInCyber

Multi-factor authentication (MFA)

We hope this year's cybersecurity awareness campaign will help you tighten cybersecurity at home and across communities and businesses. We need your help and the help of your family and friends in protecting the United States, its vast intelligence community, and your personal and professional assets. This year's campaign shares ways to increase resilience against cyber-attacks and provides several easy examples to help lock down private data and keep assets secure from criminals, terrorists and foreign entities.

What is MFA?

Multi-factor authentication (MFA) is a layered approach to securing your online accounts and the data they contain. By adding MFA to your online services (like email), you provide a combination of two or more authenticators to verify your identity when logging on. MFA provides greater protection even if someone guesses your password, those unauthorized users will be stopped at the second identifier.

MFA is also called Two Factor Authentication, Two Step Authentication, and 2FA. They all refer to using a combination of knowledge (something you know), possession (something you have) and inherence (something you are).

Your bank, your social media network, your school, your workplace all want to make sure that you're the one accessing your information, and to prevent unauthorized individuals from accessing your account and data.

Online services are also taking a step to double check, asking for something you know like a PIN number or a password, along with an authentication application or a confirmation text on your phone, or a fingerprint or face scan. Two steps are harder for a hacker to compromise.

Enabling MFA at home

Start by looking at the security settings on your most-used accounts. You may see options to enable MFA listed as "Two Factor Authentication," "Multi-Factor Authentication," or "Two Step Factor Authentication."

There are many ways you may be asked to provide a second form of authentication. Here are the most popular forms of MFA (in order of strength) from weakest to strongest:

Text Message (SMS) or Email: When you login to an account, the service will send a code to your phone or email account, which you then use to login.

Authenticator App: An authenticator app is one that generates MFA login codes on your smartphone. When prompted for your MFA code, you launch the app and type in the displayed number. These codes often expire every 30 or 60 seconds.

Push notification: Instead of using a numeric code, the service "pushes" a request to your phone to ask if it should let you in. You will see a pop-up and can approve the login request or deny it if you did not initiate the authentication request.

Any form of MFA is better than no MFA. Any MFA will raise the cost of attack and will reduce your risk.

Additional MFA Resources for at Home Consumers

Multi-Factor Authentication Fact Sheet

Learn how to set up MFA for Facebook

Learn how to set up MFA for Gmail

Learn how to set up MFA for Apple ID

Why should your organization enable MFA?

Implementing MFA makes it more difficult for a threat actor to gain access to information systems, such as remote access technology, email, and billing systems, even if passwords are compromised through phishing attacks or other means.

Adversaries are increasingly capable of phishing or harvesting passwords to gain unauthorized access. They take advantage of passwords you reused on other systems. MFA adds a strong protection against account takeover by greatly

increasing the level of difficulty for adversaries.

Additional MFA Resources for Organizations

Capacity Enhancement Guide for Organizations: Implementing Strong Authentication

Multi-Factor Authentication (MFA) - Glossary from NIST

Google: Protect your account with 2-Step Verification - Computer - Google Account Help

Apple: Two-factor authentication for Apple ID

Microsoft: How to use two-step verification with your Microsoft account

Yahoo: Add two-step verification for extra security | Yahoo Help - SLN5013

Remember: always trust your instincts. If an email, phone call or an attachment seem suspicious, don't let your curiosity put your computer at risk! If you see or hear something cyber suspicious, please contact the STS Customer Care Center at 615-741-1001.

Best regards to all,

Curtis Clan | Chief Information Security Officer, CISSP

You May Also Be Interested In:

CyberSafeTN

NCSAM Tips and Advice

Security & Risk Mitigation Resources

STS Security Services Policy Documentation