Sent: Thursday, October 20, 2022 at 7:30 AM
Subject: National Cybersecurity Awareness Month: Passwords

CITY OF **MADISON**
INFORMATION TECHNOLOGY

National Cybersecurity Awareness Month

CYBERSECURITY AWARENESS MONTH 2022

In honor of National Cybersecurity Awareness Month, we are sharing cybersecurity tips each week in October! We're proud to be part of National Cybersecurity Awareness Month to help us all understand the latest ways to protect our City online.

Passwords & Password Management

Creating long, random, and unique passwords is a critical step to protecting yourself online. Using long passwords is one of the easiest ways to defend yourself from cybercrime! The most secure way to store all your unique passwords is by using a password manager. *Sticky notes under your keyboard is **not** an appropriate password management strategy.*

Stronger Passwords, Stronger Security

12+ Characters

Use the longest password or passphrase permissible. For example, you can use a password manager or passphrase such as a news headline or even the title of the last book you read. **Passwords should be at least 12 characters long.**

Make Passwords Difficult to Guess

Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.

Keep Your Passwords Private

Do not tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or by phone. Every time you share or reuse a password, it chips away at your security by opening more ways with which it could be misused or stolen. **Passwords should never be shared over email**!! At the City, if a password must be shared, please share it over the phone or using Skype for Business.

Use Unique Passwords

Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protects you in the event of a breach.

Additional Cyber Basics for Password Management

These basics can apply at home, work, school, or wherever you engage in online interaction.

Strengthen Your Login Protection

Use multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other password-required service. Enable MFA by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

Layer Authentication Tools

Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics (biological measurements—or physical characteristics—that can be used to identify individuals, such as fingerprint mapping, facial recognition, and retinal scans), and/or security keys. Your usernames and passwords are not enough to protect key accounts like email, banking, and social media.

Each of you are our first line of defense against cybersecurity threats. That's why we will continue to share more cybersecurity resources from the Cybersecurity and Infrastructure Security Agency (CISA) throughout October to make us all more aware of these best practices.

Cybersecurity Awareness

Our Madison – Inclusive, Innovative & Thriving Through Technology

Previous NCSAM newsletters: https://www.cityofmadison.com/employeenet/information-technology/training-support/it-monthly-newsletters

Information Technology

210 Martin Luther King Jr Blvd

Madison, WI 53703

Help Desk: (608) 266-4193

https://www.cityofmadison.com/employeenet/information-technology