



## Cybersecurity Awareness Month Theme

### See Yourself in Cyber

This year's campaign theme — *"See Yourself in Cyber"* — demonstrates that while cybersecurity may seem like a complex subject, ultimately, it's really all about people. This October will focus on the "people" part of cybersecurity, providing information and resources to help educate CISA (Cybersecurity & Infrastructure Security Agency) partners and the public, and ensure all individuals and organizations make smart decisions whether on the job, at home or at school – now and in the future. We encourage each of you to engage in this year's efforts by sharing this messaging with your peers.

- For individuals and families, we encourage you to **See Yourself taking action to stay safe online**. That means enabling basic cyber hygiene practices: update your software, think before you click, have good strong passwords or a password keeper, and enable multi-factor authentication (meaning you need "More Than A Password!") on all your sensitive accounts.
- For those considering joining the cyber community, we encourage you to **See Yourself joining the cyber workforce**. We'll be talking with leaders from across the country about how we can build a cybersecurity workforce that is bigger, more diverse and dedicated to solving the problems that will help keep the American people safe.
- For our partners in industry, we encourage you to **See Yourself as part of the solution**. That means putting operational collaboration into practice, working together to share information in real-time, and reducing risk and build resilience from the start to protect America's critical infrastructure and the systems that Americans rely on every day.

### 4 Things You Can Do

Throughout October, CISA and NCA will highlight key action steps that everyone should take:

- **Think Before You Click: Recognize and Report Phishing:** If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software:** Don't delay -- If you see a software update notification, act promptly. Better yet, turn on automatic updates.
- **Use Strong Passwords:** Use passwords that are long, unique, and randomly generated. Use password managers to generate and remember different, complex passwords for each of your accounts. A passwords manager will encrypt passwords securing them for you!
- **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and **enabling MFA makes you significantly less likely to get hacked**.

For additional information on any HIPAA-related topics, please refer to the URMS intranet site at <http://sites.mc.rochester.edu/departments/hipaa/>. For any questions regarding HIPAA, please contact your Privacy Officer or HIPAA Security Official.