Hello,

October is Cyber Security Month and I'm sharing this PDF from:

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

If you have any questions or need any information regarding security. Please call the IT help desk at 320-308-6445

Tim Furr
Interim CIO
320-308-5177
St. Cloud Technical & Community College
1540 Northway Drive, St Cloud, MN 56303-1240

ST. CLOUD
TECHNICAL & COMMUNITY
COLLEGE
A member of Minnesota State

SEE YOURSELF IN CYBER

CYBERSECURITY AWARENESS
MONTH 2022

Cybersecurity Awareness Month

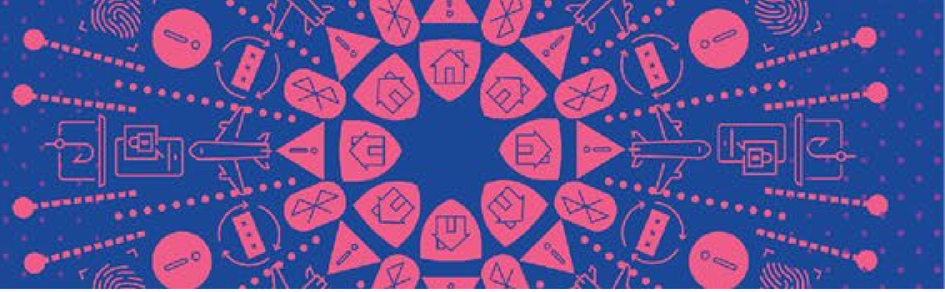
Since 2004, October is celebrated as Cybersecurity Awareness Month, previously called National Cybersecurity Awareness Month. Now in its 19th year, Cybersecurity Awareness Month is a collaborative effort between government and industry to raise cybersecurity awareness nationwide and help ensure that all Americans have the resources they need to be safe and secure online.

Cybersecurity Awareness Month | CISA

Partnership

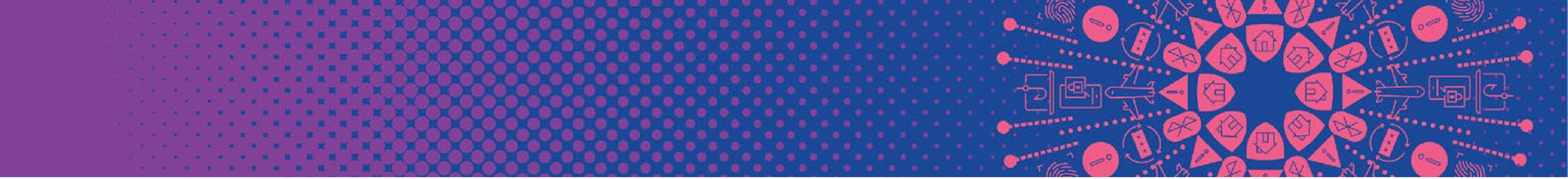
The Cybersecurity and Infrastructure Security Agency (CISA) is the federal lead for Cybersecurity Awareness Month with the National Cybersecurity Alliance (NCA) as co-lead.

National Cybersecurity Alliance (staysafeonline.org)



Theme

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 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 creating your own cyber awareness campaigns and 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.

Action Steps

This year's campaign goal is to have everyone implement these four action steps to increase online security. 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.**

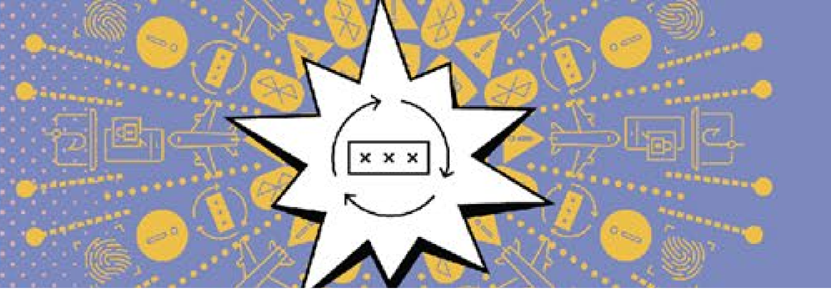
Recognize and Report Phishing

- Have you ever seen a link that looks a little off? It looks like something you’ve seen before, but it says you need to change or enter a password. Or maybe it asks you to verify personal information.
- It’s likely a phishing scheme: a link or webpage that looks legitimate, but it’s a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Once they have that information, they can use it on legitimate sites.

Update Your Software

- Bad actors will exploit flaws in the system. Network defenders are working hard to fix them as soon as they can, but their work relies on all of us updating our software with their latest fixes.
- Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too. Turn on automatic updates for all devices, applications, and operating systems.

Use Strong Passwords



- Creating strong passwords is an easy way to improve your cyber security. Strong passwords include one uppercase letter, one lowercase letter, at least one number and 11 or more characters. Be sure to use different passwords for different accounts.
- Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!
- Put cybersecurity first by protecting the information stored on devices. Much of a user's personal information is stored either on their computer, smartphone, tablet or possibly someone else's system.

Enable Multi-Factor Authentication

- It’s More than a Password: Why We all Need Multi-factor Authentication
- If you can do just one thing to protect your online valuables, set up Multi-factor Authentication.
- It goes by many names: Two Factor Authentication. Multifactor Authentication. Two Step Factor Authentication. MFA. 2FA. They all mean the same thing: opting-into an extra step when trusted websites and applications ask you to confirm you’re really who you say you are.

Report a Cyber Issue

- CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities.

www.cisa.gov/report

Resources

Cyber Hygiene Services

CISA Shields Up

Cyber Resource Hub

Communications & Cyber Resiliency Toolkit

Cybersecurity Training & Exercises

Website

For complete information and resources on Cybersecurity Awareness Month, go to:

www.cisa.gov/cybersecurity-awareness-month

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

CYBERSECURITY AWARENESS MONTH 2022