



# CYBERSECURITY AWARENESS MONTH 2023

UNIVERSITY SYSTEM OF NEW HAMPSHIRE



# Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.



# Theme



SECURE.  
OUR **WORLD**

# What is Cybersecurity?

- Defined as "the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data..."
- Security should be part of the design and development phase of projects.
- **Wherever there is technology, there needs to be cybersecurity.**





# Cybersecurity “So What?”

## Did You Know?

Antivirus software is available for mobile devices, which are an easy, common target for hackers and other bad actors.



## Cybersecurity Common Sense

---

- **Being safe online isn't so different from being safe in the physical world!**
- **Keep Calm and Trust Your Gut!**



## Commonly Used Terms

---

- **Bad Actor**
- **Hacker**
- **Cyber Attack**

# Our Online Behaviors

- **Only 33% of individuals create unique passwords for all accounts**
  - Only 18% of individuals have downloaded a password manager
- **43% of respondents have never heard of multifactor authentication (MFA)**
  - Out of the 57% of the participants who had heard about it:
    - 79% applied it at least once and 94% of them reporting that they were still using MFA
- **92% of respondents took action after a security training**
  - 58% say they are better at recognizing phishing
  - 45% started using strong and unique passwords
  - 40% started using MFA
  - 40% started regularly installing software updates

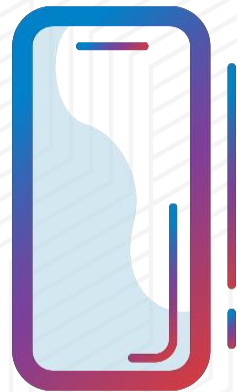
# 4 Easy Ways to Stay Safe Online

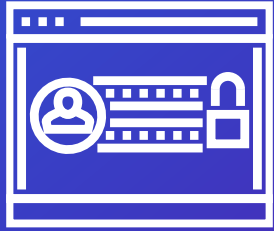
**Use Strong Passwords and a Password Manager**

**Turn on Multifactor Authentication**

**Recognize and Report Phishing Attacks**

**Update Your Software**





# Use Strong Passwords

## Did You Know?

Password or credential stuffing is a cyberattack that tries “stuffing” already comprised username and passwords from one site into another site in hopes that the user uses the same login information across platforms.

\*\*\*\*\*

Use different passwords on different systems and accounts

\*\*\*\*\*

Use the longest password allowed

\*\*\*\*\*

Use a mix of uppercase and lowercase letter, numbers, and symbols

\*\*\*\*\*

Reset your password every few months

\*\*\*\*\*

Use a password manager



# Use a Password Manager

## WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.



# Turn on Multifactor Authentication

## WHAT IS IT?

- **A code sent to your phone or email**
- **An authenticator app**
- **A security key**
- **Biometrics**
  - Fingerprint
  - Facial recognition



# Turn on Multifactor Authentication

## WHERE SHOULD YOU USE MFA?

- **Email**
- **Accounts with financial information**  
Ex: Online store
- **Accounts with personal information**  
Ex: Social media



# Recognize and Report Phishing


## PHISHING RED FLAGS:



- **A tone that's urgent or makes you scared**  
*"Click this link immediately or your account will be closed"*
- **Bad spellings, bad grammar**
- **Requests to send personal info**
- **Sender email address doesn't match the company it's coming from**  
Ex: Amazon.com vs. Amaz0n.com
- **An email you weren't expecting**

# Would This Email Fool You?



 New message — ↗ ✕


---

**From** Legitimate-Looking-Source@notquiteyourworkemail.com

---

**Subject** Urgent IT Update: Software Vulnerability


---

 SoftwareUpdate.exe

Good afternoon,







A vulnerability has been identified in your software that allows an attacker to record calls and videos from your computer without your knowledge. Please install the update by the end of the day or your workstation will be locked.

We have also created app for all employees to determine if they been affected by this vulnerability. Click [here](#) to run the app.

Sincerely,  [www.fakewebsite.com/gotcha.exe](http://www.fakewebsite.com/gotcha.exe)  
Click or tap to follow link.

Your Company IT Department

---

**REPLY**      

# Recognize and Report Phishing

## WHAT TO DO

### Do NOT

- Don't click any links
- Don't click any attachments
- Don't send personal info



### Do

- Verify
- Contact that person directly if it's someone you know
- Report it to your IT department or email/phone provider
- DELETE IT

# Update Your Software

## WHY?

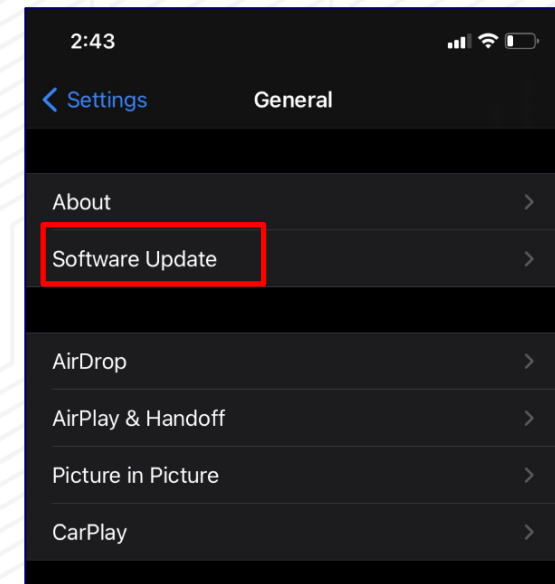
- Updates ensure your devices and apps are protected from the latest threats
- Don't click "remind me later", it could leave you vulnerable to cyber threats
- Automatic updates are the easiest way to stay secure



# Update Your Software

## WHERE TO FIND AVAILABLE UPDATES

- Check for notifications to your phone or computer
- Look in your phone, browser or app settings
- Check the upper corner of your browser for any alerts





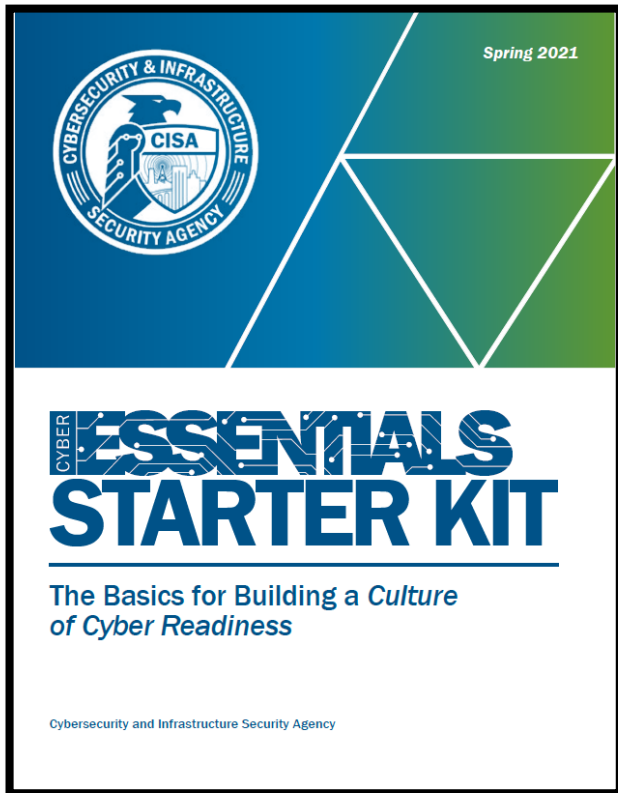
# Building a Strong Cybersecurity Culture

- **Use basic cybersecurity training.** This helps familiarize staff with cybersecurity concepts and activities associated with implementing cybersecurity best practices.
- **Identify available cybersecurity training resources.** Cybersecurity training resources—on topics like phishing and good email practices—are available through professional association, educational institutions, as well as private sector and government sources.
- **Stay current on cybersecurity events and incidents.** This helps identify lessons learned and helps to maintain vigilance and agility to cybersecurity trends.
- **Encourage employees to make good choices online and learn about risks** like phishing and business email compromise.



**Free Resources**

# CYBER ESSENTIALS



- The Cyber Essentials are a set of easy to adopt and understand, community-endorsed cybersecurity practices that together constitute “the basics.” They are CISA’s answer to the question we hear often from stakeholders - “Where do I start?”
- The Cyber Essentials are written for those with limited or no knowledge of cybersecurity practice or terminology but who nevertheless are responsible for safeguarding their organizations.
- The Cyber Essentials will take a organizational risk-management approach from a leadership-driven perspective.
- The Cyber Essentials encourage organizations to approach cyber risks as they would other operational risks – through a holistic approach.

# List of Free Cybersecurity Tools

As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community.



# Resources for Students



Online Safety + Privacy Basics





# DEFEND TODAY, SECURE TOMORROW

**Cybersecurity Advisor (CSA) for New Hampshire  
Cybersecurity State Coordinator**

**Rick Rossi**

**Email: [richard.rossi@cisa.dhs.gov](mailto:richard.rossi@cisa.dhs.gov)**

**Cell: 202-770-8991**

**Protective Security Advisor (PSA) for New  
Hampshire**

**Jason Climer**

**Email: [jason.climer@cisa.dhs.gov](mailto:jason.climer@cisa.dhs.gov)**

**Cell: 202-897-7666**

