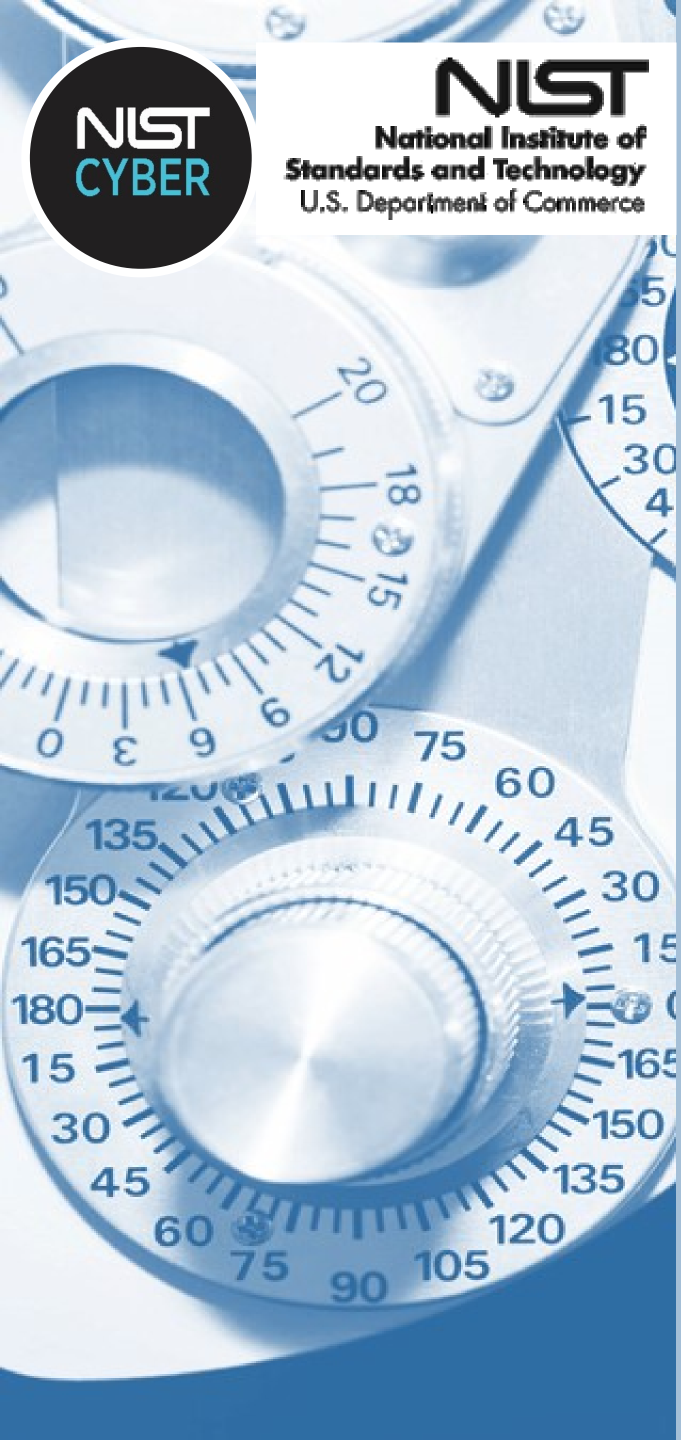


NIST CYBER

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

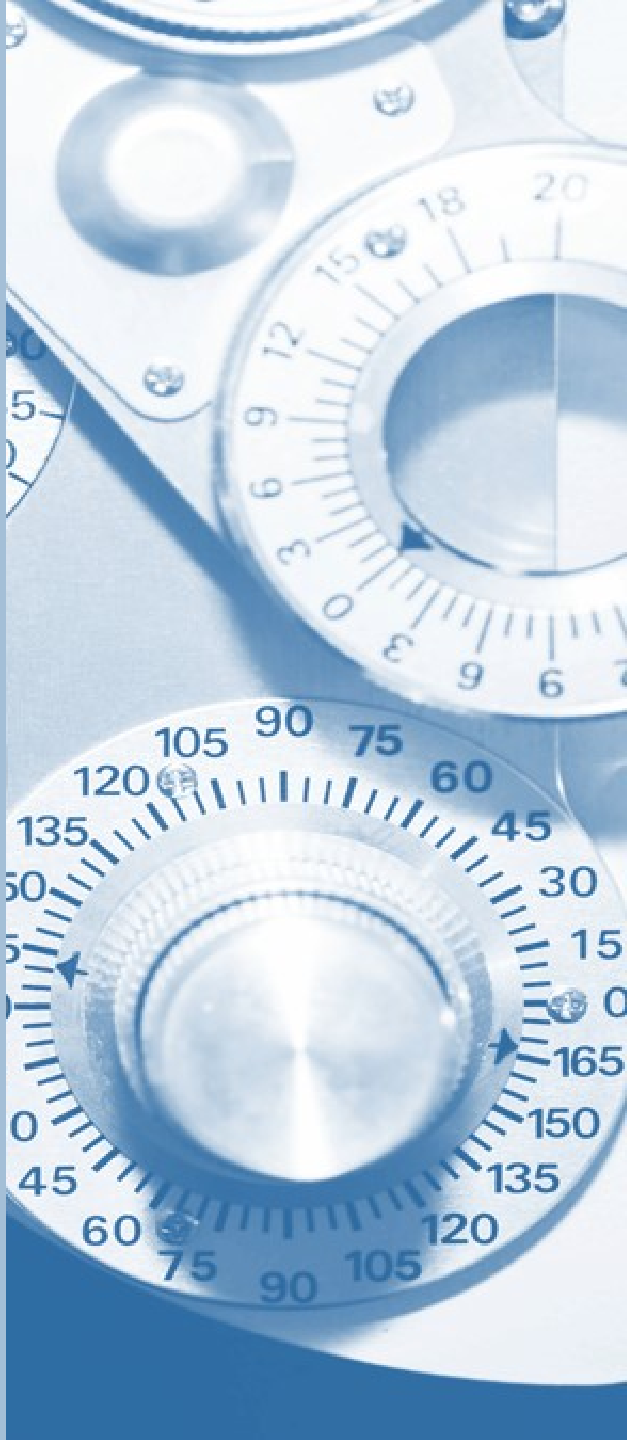
2020 Vision:

Bringing the Future of Cybersecurity Awareness and Training Into Focus

33rd Annual FISSEA Conference 2020 Summer Webinar Series

#FISSEA2020 | nist.gov/fissea

WEBINAR TO BEGIN SHORTLY



fissea

FEDERAL

2020

Summer Series

July 20, 2020

“Preparing for National Cyber Security Awareness Month”

presented by the National Cyber Security Alliance (NCSA)

- Sylvia Layton - Chief Operating Officer
- Daniel Eliot - Director of Education & Strategic Initiatives

Federal Information Security Educators (FISSEA)

About FISSEA

FISSEA, founded in 1987, is an organization run by and for Federal government information security professionals to assist Federal agencies in strengthening their employee cybersecurity awareness and training programs.

Purpose

- Elevate the general level of information security knowledge for the federal government and federally-related workforce.
- Serve as a professional forum for the exchange of information and improvement of information systems security awareness and training programs throughout the federal government.
- Provide for the professional development of community members.

Organization

- FISSEA seeks to bring together information security professionals.
- Each year, an award is presented to a candidate selected as Awareness and Training Innovator of the Year, honoring distinguished accomplishments in information security training programs.

The Learning Continuum

Awareness

- Campaigns: Cybersecurity Awareness Month; Stop.Think.Connect
- Building a Security Awareness and Training Program (NIST SP 800-50)
- Federal Information Security Educators (FISSEA)

Training

- Learning Experiences and Credentials (e.g., Certification, Certificate, Badge, etc.)
- Role-Based Training (NIST SP 800-16)
- FISSEA and National Initiative for Cybersecurity Education (NICE)

Education

- K12: Elementary, Middle, and High School
- Higher Education: Community Colleges, Colleges and Universities, and Professional Schools
- NICE – Education and Workforce

Engagement Opportunities

Awareness and Training ~ FISSEA (federal environments)

- FISSEA Community of Interest
- FISSEA Summer Series
- Annual FISSEA Conference and Exhibitor Showcase

Training and Education ~ NICE (education and workforce for the nation)

- Federal Cybersecurity Workforce Summit & Webinar Series
- Annual NICE Conference and Expo
- NICE K12 Cybersecurity Education Conference
- NICE Webinar Series

JOIN US FOR THE NEXT WEBINAR

Adaptive Learning: Utilizing AI and Social Collaboration for User-Centric

August 17, 2020 1:00PM-2:30PM

Have you enrolled in training where much of the material covered was far too simple for you? Or clicked through on-demand training modules as quickly as possible because the content was largely irrelevant to your job role, yet needed to be completed to show your competency on a topic? Many thought leaders in training and development believe that Adaptive Learning and AI will change the way that the next-gen workforce will learn and adopt new skills into practice. Adaptive learning is a method of on-demand instruction that orchestrates artificial intelligence and sophisticated algorithms to present the next appropriate action, based on what it knows about each unique learner. It evolves moment-by-moment using trial and error as the environment changes for the individual learner. Joi n in to hear a panel discussion that will provide insight into how and why adaptive learning and artificial intelligence will transform the way that the workforce will learn new skills in the future.

Featuring: Presentation of the FISSEA Security Awareness and Training Contest Winners

REGISTER
https://csrc.nist.gov/Projects/fissea/2020-summer-series

NIST CYBER

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

fissea
FEDERAL

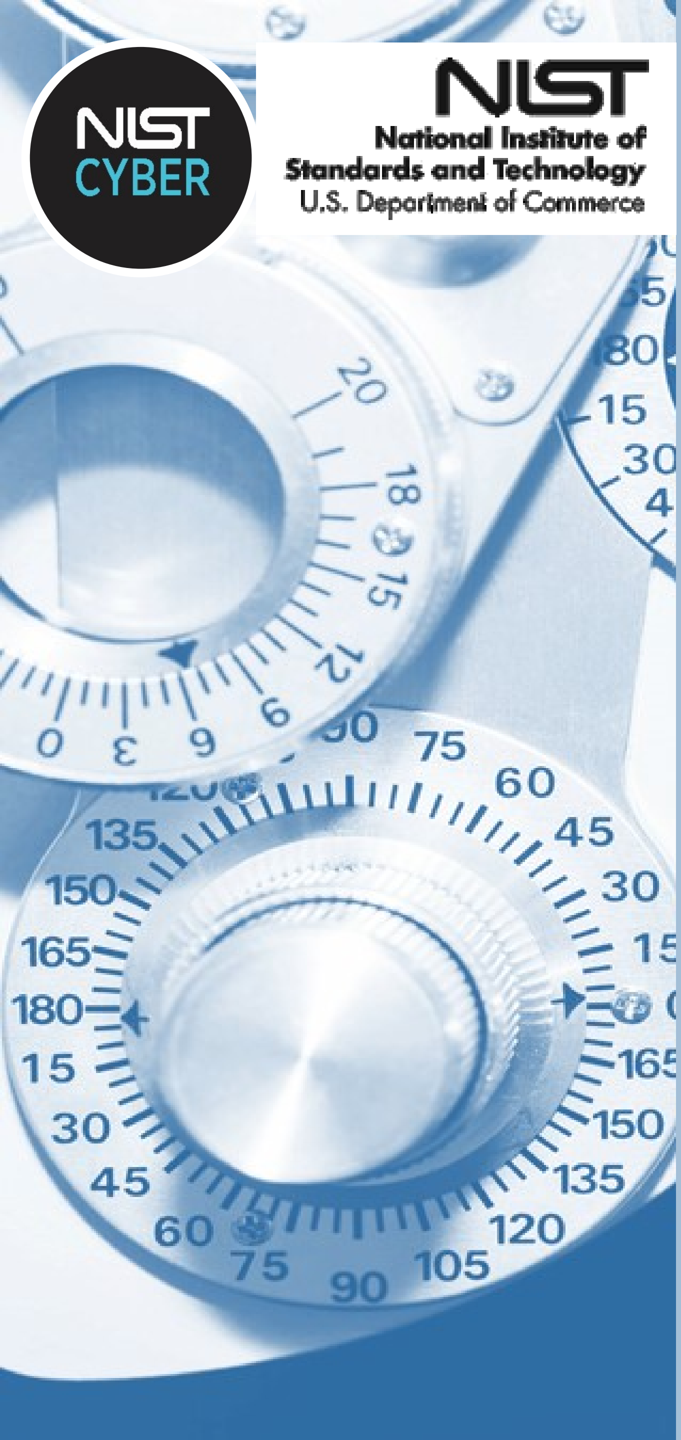
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Register Today for the FISSEA Summer Series 2020

August 17, 2020, 1:00-2:30 pm
"Adaptive Learning: Utilizing AI and Social Collaboration for User-Centric Training Results"
Featuring: Presentation of the FISSEA Security Awareness and Training Contest Winners

September 21, 2020, 1:00-2:30 pm
Topic to be announced

Visit: https://csrc.nist.gov/Projects/fissea/2020-summer-series



NIST CYBER

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

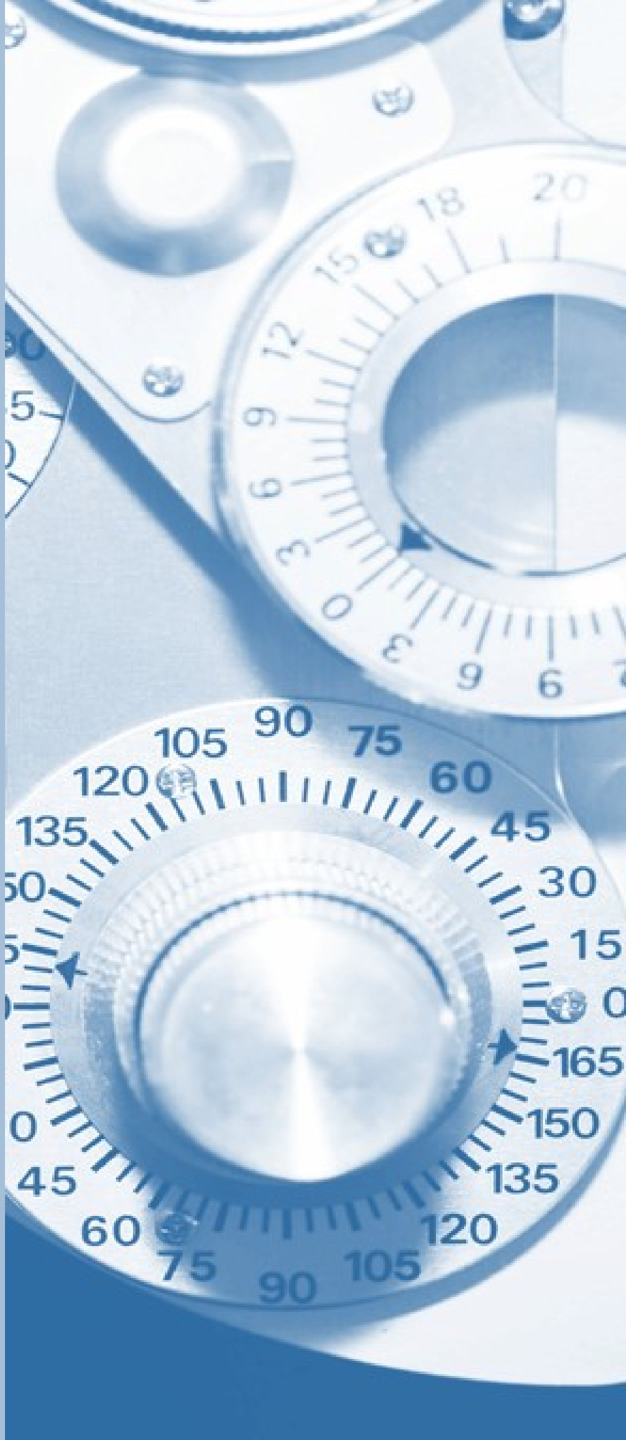
fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Save the Date

FISSEA 2021

June 16-17, 2021
NIST Campus
Gaithersburg, Maryland



CYBERSECURITY
AWARENESS
MONTH

2020 Updates and Theme Overview

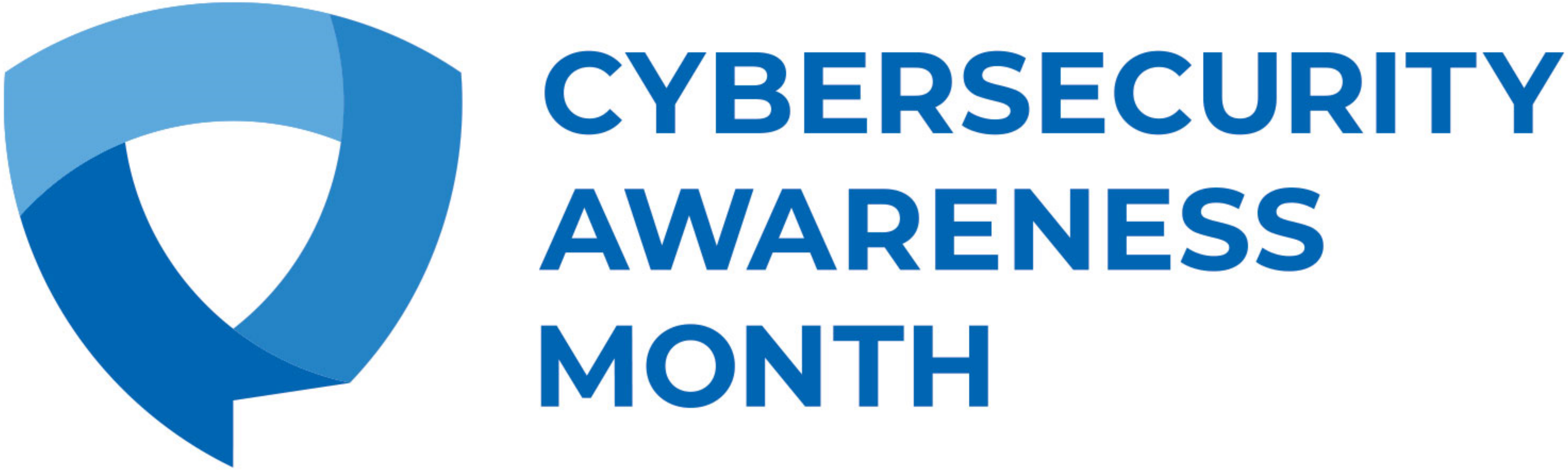
Presenter: Sylvia Layton, Chief Operating Officer, NCSA

Date: July 20, 2020

NATIONAL CYBERSECURITY ALLIANCE

Do Your Part. #BeCyberSmart

Introducing the New Cybersecurity Awareness Month Logo



Download the new **Cybersecurity Awareness Month Logo** and **Branding Guideline** here: https://staysafeonline.org/resource/awareness-month-images-logos/

Do Your Part. #BeCyberSmart

OCTOBER MEANS...

1. HALLOWEEN
2. PUMPKIN SPICE LATTES
3. CYBERSECURITY AWARENESS MONTH

STAYSAFEONLINE.ORG/
CYBERSECURITY-AWARENESS-MONTH

OCTOBER IS

CYBERSECURITY AWARENESS MONTH

DO YOUR PART.
#BECYBERSMART.

STAYSAFEONLINE.ORG/
CYBERSECURITY-AWARENESS-MONTH

Weekly Focus Areas

Key Message

October 1- 4	Official Cybersecurity Awareness Month Kick-off
Week of October 5	If You Connect It, Protect It
Week of October 12	Securing Devices at Home & Work
Week of October 19	Securing Internet-Connected Devices in Healthcare
Week of October 26	The Future of Connected Devices

Do Your Part. #BeCyberSmart

If You Connect It, Protect It.

Cybersecurity Awareness Month 2020 is about taking proactive steps to enhance cybersecurity at home and in the workplace

41 Billion

There will be more than 41 billion connected devices by 2027, up from about 8 billion in 2019[3]

75 % infected

75% of infected connected devices are routers[1]

5 Minutes 24 hours

Once plugged into the Internet, connected devices are attacked within 5 minutes and targeted by specific exploits within 24 hours[2]

Do Your Part. #BeCyberSmart

[1] **Symantec**: https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse

[2] **NETSCOUT Threat Intelligence Report**: https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf

[3] **Business Insider Intelligence**: https://www.businessinsider.com/internet-of-things-report?IR=T

Ways to Get Involved

- Sign your company up as a Champion: https://staysafeonline.org/cybersecurity-awareness-month/champions/
- Encourage colleagues, friends & family to register as individual Champions
- Post on social media using **#BeCyberSmart**
- Contribute a guest blog to staysafeonline.org. Contact: info@staysafeonline.org
- Use this PowerPoint template & host an educational event for your community
- Use the new logo to co-brand digital materials with Cybersecurity Awareness Month (infographics, website, resources, emails, etc.)

Own Your Role in Cybersecurity

- LOCK DOWN YOUR LOGIN
- WHEN IN DOUBT, THROW IT OUT
- KEEP A CLEAN MACHINE
- BACK IT UP
- OWN YOUR ONLINE PRESENCE
- SHARE WITH CARE
- GET SAVVY ABOUT WIFI HOTSPOTS

CYBERSECURITY IS EVERYONE'S JOB.

INCLUDING YOURS.

CYBERSECURITY AWARENESS MONTH

STAYSAFEONLINE.ORG/ CYBERSECURITY-AWARENESS-MONTH

Do Your Part. #BeCyberSmart

Creating Your Awareness Campaign

Presenter: Daniel Eliot, Director of Education & Strategic Initiatives, NCSA

Date: July 20, 2020

NATIONAL CYBERSECURITY ALLIANCE

Do Your Part. #BeCyberSmart

“Just Because I’m Aware Doesn’t Mean That I Care”

~ Perry Carpenter, *Transformational Security Awareness*

The Human Element

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”

--

Creating Your Campaign

- Who is your audience?
- Is there a specific behavior you'd like to change?
- Beware the Curse of Knowledge
- The convergence of home, work, & school

Get Creative

- Imagery
- Storytelling
- Emotion
- Humor

KEEP TABS ON YOUR APPS

DELETE THOSE APPS YOU'RE NO LONGER USING TO FREE UP SPACE AND ENHANCE YOUR SECURITY

CYBERSECURITY AWARENESS MONTH

STAYSAFEONLINE.ORG/CYBERSECURITY-AWARENESS-MONTH

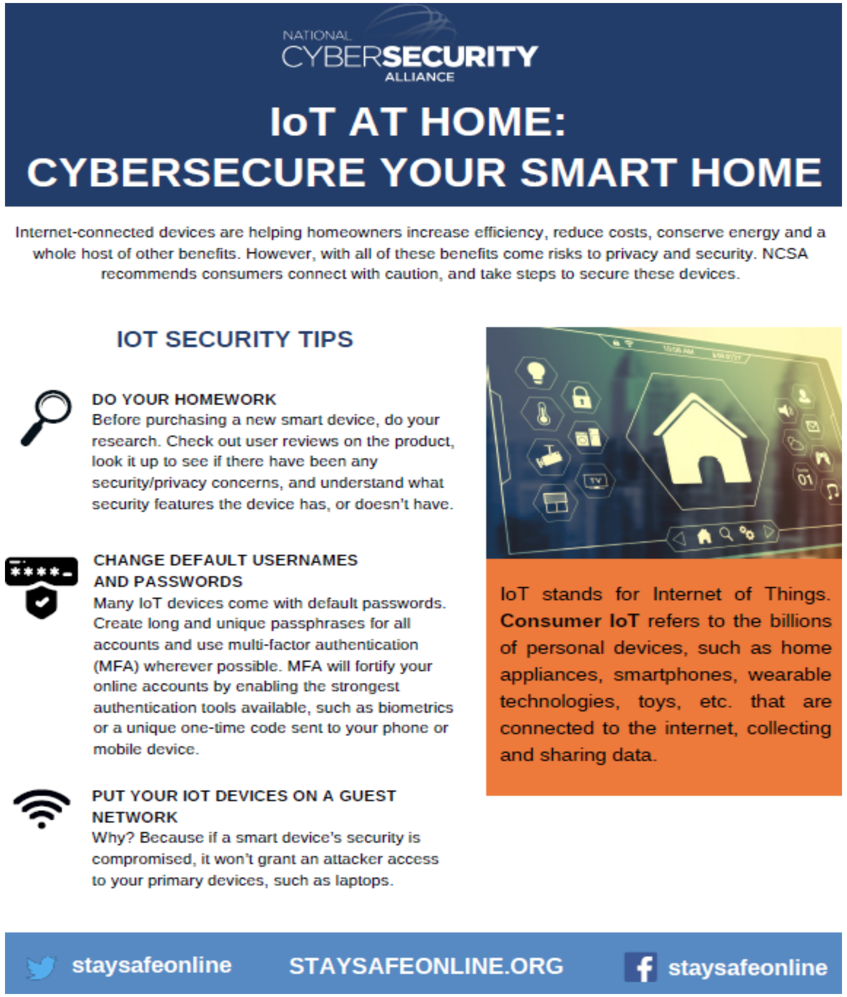
DON'T GET TRICKED THIS OCTOBER

TREAT YOURSELF WITH

CYBERSECURITY AWARENESS MONTH

STAYSAFEONLINE.ORG/CYBERSECURITY-AWARENESS-MONTH

NCSA Tip Sheets & Infographics



NATIONAL CYBERSECURITY ALLIANCE

IoT AT HOME: CYBERSECURE YOUR SMART HOME

Internet-connected devices are helping homeowners increase efficiency, reduce costs, conserve energy and a whole host of other benefits. However, with all of these benefits come risks to privacy and security. NCSA recommends consumers connect with caution, and take steps to secure these devices.

IOT SECURITY TIPS

DO YOUR HOMEWORK
Before purchasing a new smart device, do your research. Check out user reviews on the product, look it up to see if there have been any security/privacy concerns, and understand what security features the device has, or doesn't have.

CHANGE DEFAULT USERNAMES AND PASSWORDS
Many IoT devices come with default passwords. Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

PUT YOUR IOT DEVICES ON A GUEST NETWORK
Why? Because if a smart device's security is compromised, it won't grant an attacker access to your primary devices, such as laptops.

IoT stands for Internet of Things. **Consumer IoT** refers to the billions of personal devices, such as home appliances, smartphones, wearable technologies, toys, etc. that are connected to the internet, collecting and sharing data.

staysafeonline STAYSAFEONLINE.ORG staysafeonline

NATIONAL CYBERSECURITY ALLIANCE

CYBER TRIP ADVISOR: BUSINESS TRAVEL SECURITY TIPS

These days, no matter where you're headed, being continuously connected is part of the travel plan. As you embark upon your next work trip, the National Cyber Security Alliance (NCSA) urges travelers to be cyber safe while away from the office by following some simple practices to help keep your devices safe and your travel plans from going awry.

REMEMBER

Treat your boarding pass like it's a passport. Boarding passes contain information that, if accessed by a criminal, can reveal information like a traveler's frequent-flyer number. What could they do with this information? Access to your frequent flyer number could help a criminal steal earned miles or access any other sensitive information contained in an rewards account--particularly if you don't have a strong passphrase and 2-factor authentication enabled on those accounts.

GETTING READY TO GO

Before you head out on vacation, here's a simple security checklist to add to your packing routine.

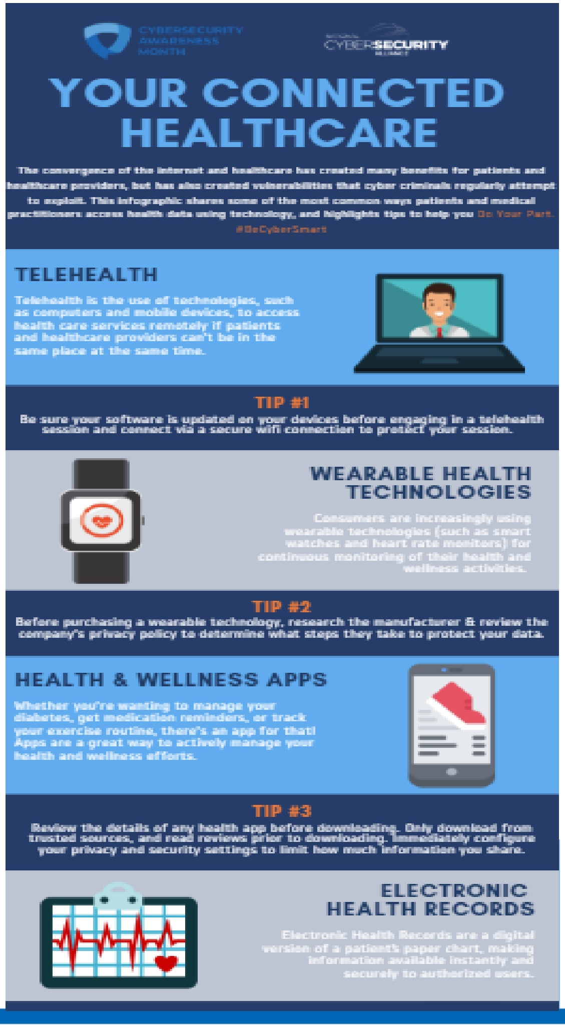
UPDATE YOUR SYSTEM AND SOFTWARE
Before you hit the road, make sure all security and critical software is up-to-date on your connected devices and keep them updated during travel. Turn on "automatic updates" on your devices if you're prone to forgetting.

OWN YOUR ONLINE PRESENCE
Set the privacy and security settings on web services and apps. It is okay to limit how and with whom you share information (like location tracking) – especially when you are away.

BACK IT UP
If you haven't taken a moment to back up the information on your devices, do so before heading out. If something unfortunate does happen and you lose your device or access to it, you'll at least be able to recover the information you backed up.

PASSWORD PROTECT YOUR DEVICES
Make sure you require the use of a passcode or extra security feature (like a fingerprint) to unlock your phone or mobile device in case either is misplaced or stolen.

staysafeonline STAYSAFEONLINE.ORG staysafeonline



CYBERSECURITY AWARENESS MONTH

NATIONAL CYBERSECURITY ALLIANCE

YOUR CONNECTED HEALTHCARE

The convergence of the internet and healthcare has created many benefits for patients and healthcare providers, but has also created vulnerabilities that cyber criminals regularly attempt to exploit. This infographic shares some of the most common ways patients and medical practitioners access health data using technology, and highlights tips to help you Do Your Part. #BeCyberSmart

TELEHEALTH

Telehealth is the use of technologies, such as computers and mobile devices, to access health care services remotely if patients and healthcare providers can't be in the same place at the same time.

TIP #1
Be sure your software is updated on your devices before engaging in a telehealth session and connect via a secure wifi connection to protect your session.

WEARABLE HEALTH TECHNOLOGIES

Consumers are increasingly using wearable technologies (such as smart watches and heart rate monitors) for continuous monitoring of their health and wellness activities.

TIP #2
Before purchasing a wearable technology, research the manufacturer & review the company's privacy policy to determine what steps they take to protect your data.

HEALTH & WELLNESS APPS

Whether you're wanting to manage your diabetes, get medication reminders, or track your exercise routine, there's an app for that! Apps are a great way to actively manage your health and wellness efforts.

TIP #3
Review the details of any health app before downloading. Only download from trusted sources, and read reviews prior to downloading. Immediately configure your privacy and security settings to limit how much information you share.

ELECTRONIC HEALTH RECORDS

Electronic Health Records are a digital version of a patient's paper chart, making information available instantly and securely to authorized users.

Access tip sheets, videos, infographics and more at
https://staysafeonline.org/resources/

Do Your Part. #BeCyberSmart

NCSA Videos

The Psychology of Passwords

Psychology of Passwords: Combatting Cognitive Dissonance in Password Creation

JUNE 25, 2020

Webinar How to Avoid COVID 19 Scams

COVID-19 Scams

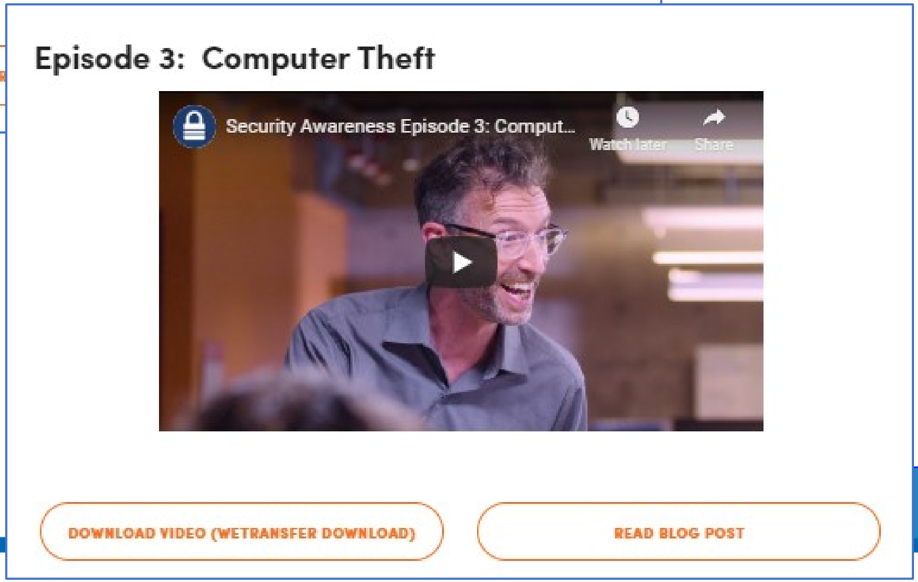
www.staysafeonline.org

@staysafeonline

Episode 2: Data Handling

Security Awareness Episode 2: Data Ha...

DOWNLOAD VIDEO (WETR


Episode 3: Computer Theft

Security Awareness Episode 3: Comput...

DOWNLOAD VIDEO (WETRANSFER DOWNLOAD)

READ BLOG POST

Access tip sheets, videos, infographics and more at https://staysafeonline.org/resources/

Do Your Part. #BeCyberSmart

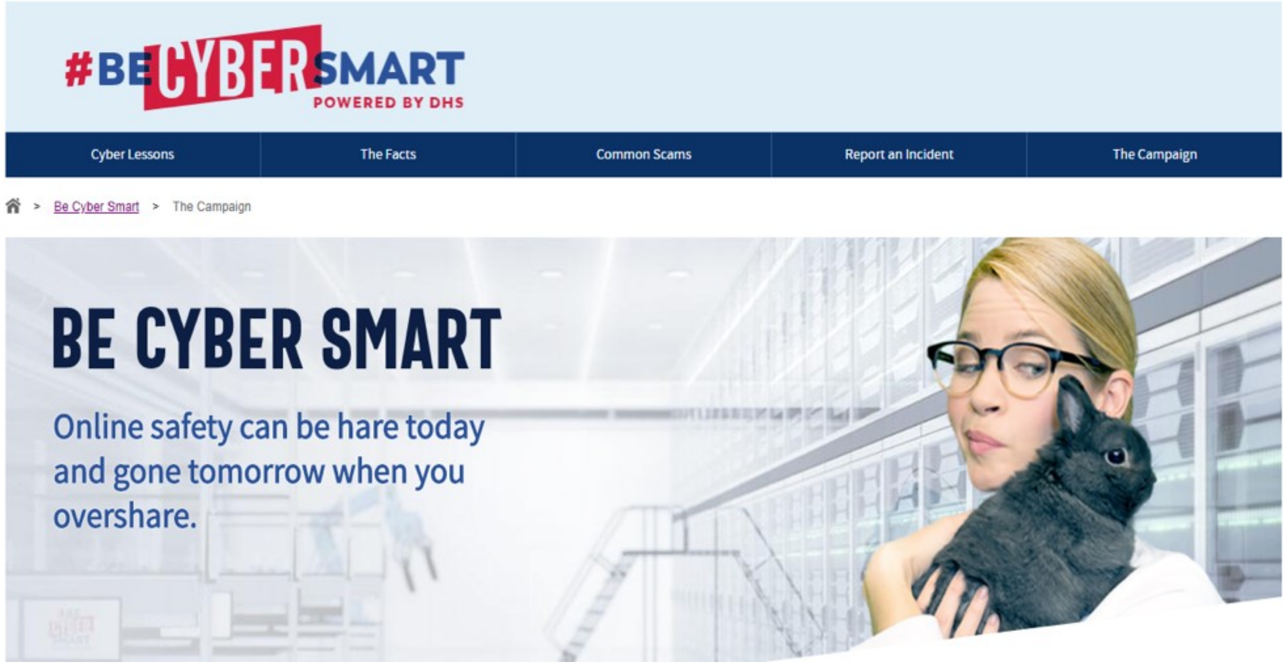
CISA Resources

STOP. THINK. CONNECT.™
https://www.dhs.gov/stopthinkconnect

#BeCyberSmart Campaign
https://www.dhs.gov/be-cyber-smart/campaign

CISA's Cyber Essentials:
https://www.cisa.gov/publication/cisa-cyber-essentials

Telework Guidance & Resources:
https://www.cisa.gov/telework



BE CYBER SMART

Online safety can be hare today and gone tomorrow when you overshare.

Cybersecurity is: “Making it easier for your employees to do the right thing, and harder for them to do the wrong thing.”

~ Brian Krebs, KrebsonSecurity

Do Your Part. #BeCyberSmart

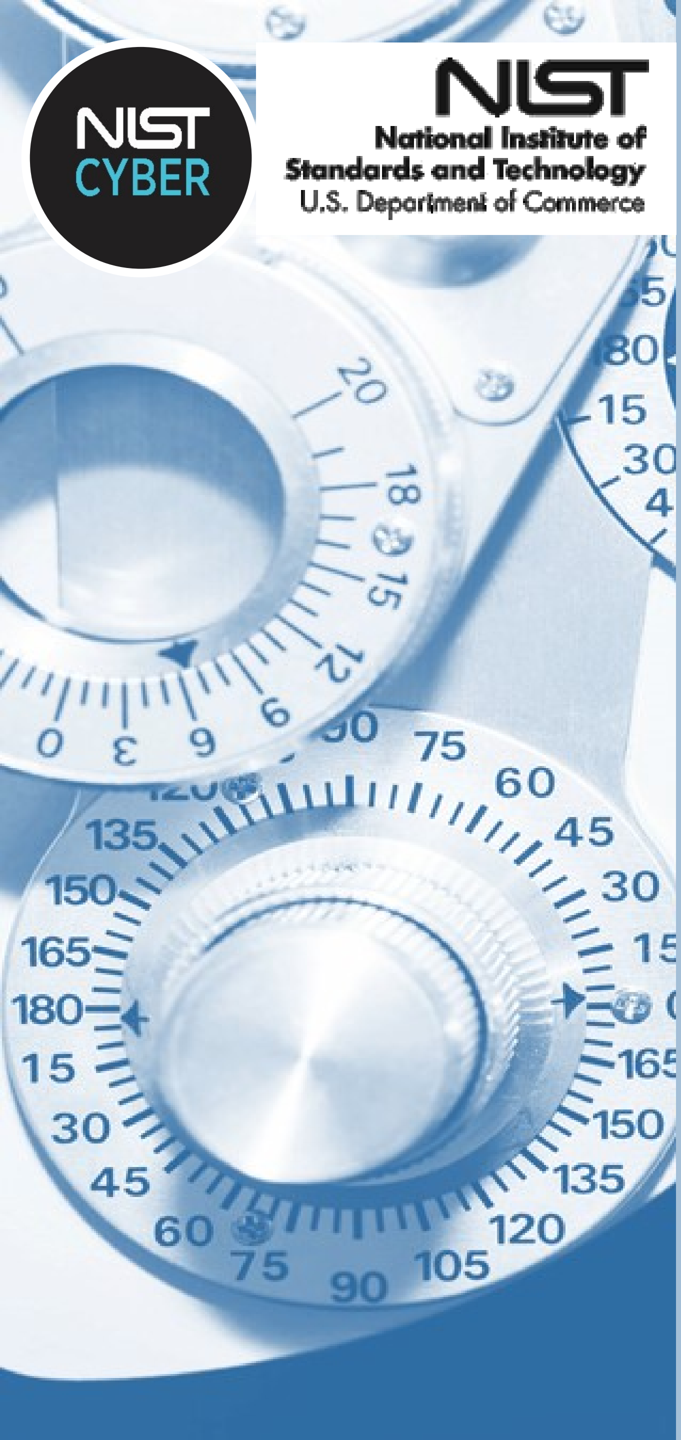
Keep In Touch

NATIONAL CYBERSECURITY ALLIANCE

Twitter:	@Staysafeonline
Facebook:	/staysafeonline
LinkedIn:	/national-cyber-security-alliance/
Email:	info@staysafeonline.org

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Twitter:	@CISAgov
Facebook:	/CISA
LinkedIn:	/cisagov/
Email:	stopthinkconnect@hq.dhs.gov



NIST CYBER

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Save the Date

FISSEA 2021

June 16-17, 2021
NIST Campus
Gaithersburg, Maryland