NATIONAL CYBERSECURITY AWARENESS MONTH

NATIONAL CYBERSECURITY AWARENESS MONTH 2020

NATIONAL CYBERSECURITY AWARENESS MONTH

What Is NCSAM?

National Cybersecurity Awareness Month (NCSAM) raises awareness about the importance of cybersecurity across our Nation.

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

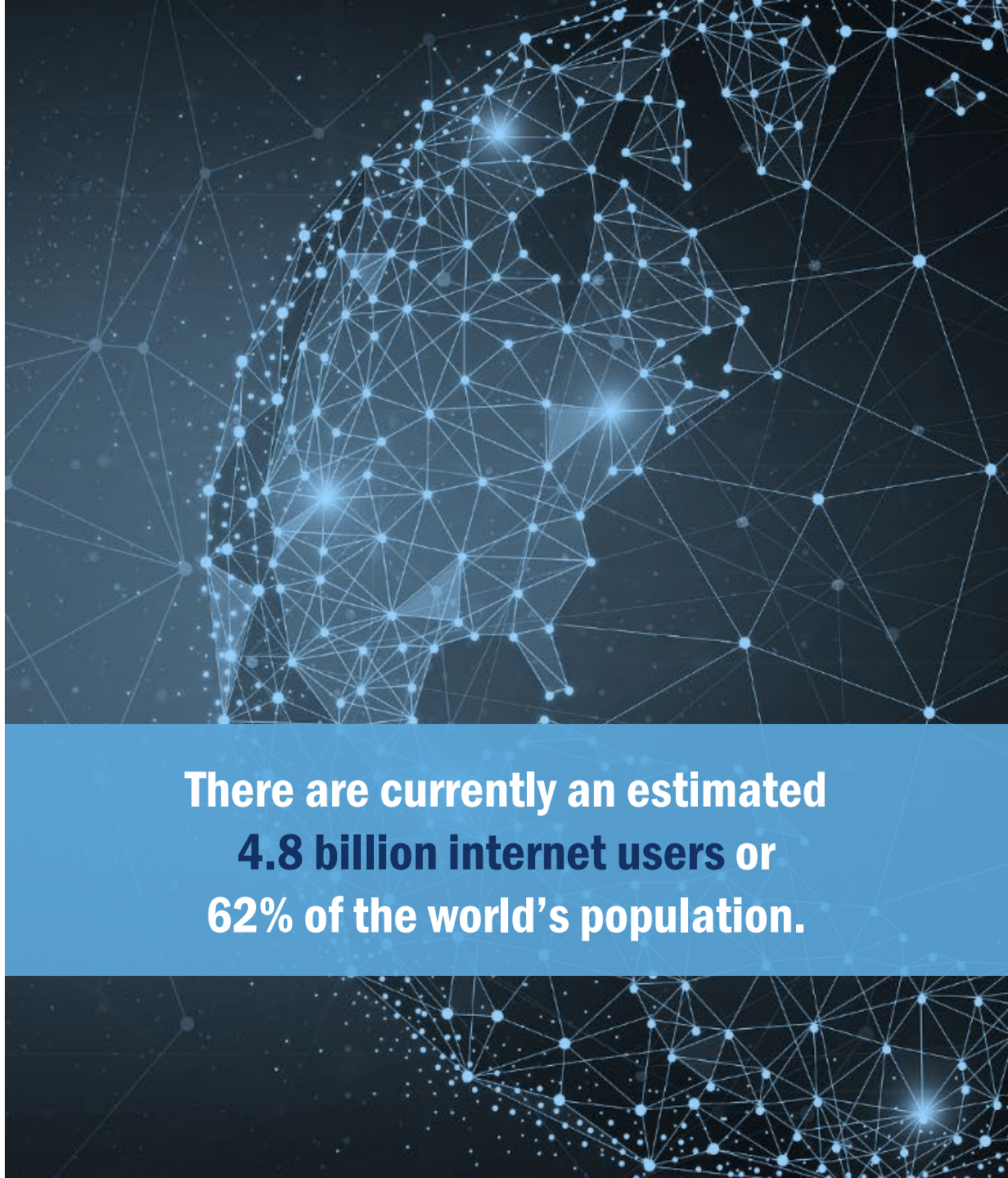
- Bad Actor
- Hacker
- Cyber Attack

NATIONAL CYBERSECURITY AWARENESS MONTH

NATIONAL CYBERSECURITY AWARENESS MONTH

Do Your Part. #BeCyberSmart.

Cybersecurity starts with YOU and is **everyone's** responsibility.



There are currently an estimated 4.8 billion internet users or 62% of the world's population.

Cybercrime

Examples

- Identity theft
- Child sexual abuse materials
- Financial theft
- Intellectual property violations
- Malware
- Malicious social engineering

What is it?

Cybercrime is any crime which is committed electronically.

This can include...

- Theft
- Fraud
- Sometimes even murder

Why should you care?

- Crime is a danger offline and on!
- Cyber self-defense basics can go a long way to keeping you and your data out of the hands of bad actors.

Malware

Examples

- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Viruses
- Worms

What is it?

Any software intended to…

- Damage
- Disable
- Or give someone unauthorized access to your computer or other internet-connected device

Why should you care?

- Most cybercrime begins with some sort of malware. You, your family, and your personal information is almost certainly at risk if malware finds its way onto your computer or devices.

Ransomware

Examples

- Cryptolocker
- Winlock
- Cryptowall
- Reveton ransomware
- Bad rabbit
- Crysis
- Wannacry

What is it?

Malware designed to make data or hardware inaccessible to the victim until a ransom is paid.

Why should you care?

- Often downloaded as malicious email links
- Damage to both financial stability and reputation
- No guarantee that you will get your data back, even if you pay
- Often used as a decoy for other malicious activity

Bots

Did You Know?

Not all bots are bad. When you use a search engine, these results are made possible by the help of bots "crawling" the internet and indexing content. Chatbots like Siri and Alexa are another common type of "good" bot.

What is it?

Bots are a type of program used for automating tasks on the internet.

Why should you care?

Malicious bots can:

- Gather passwords
- Log keystrokes
- Obtain financial information
- Hijack social media accounts
- Use your email to send spam
- Open back doors on the infected device

Physical Cyber Attacks

Did You Know?

Anything connected to the internet is potentially vulnerable, from e-scooters to laptops to cargo ships.

What is it?

Physical cyber attacks use hardware, external storage devices, or other physical attack vectors to infect, damage, or otherwise compromise digital systems. This can include...

- USB storage devices
- CD/DVD
- Internet of Things (IoT)

Why should you care?

- Easy to overlook
- Difficult to identify and detect
- Extremely difficult to remove
- Can do anything from installing ransomware, to sending copies of or modifying information systems, to dismantling networks

Social Engineering

Examples

- Phishing
- Pretexting
- Baiting
- Quid pro quo
- Tailgating
- Inside job
- Swatting

What is it?

- Cybercriminals can take advantage of you by using information commonly available through…
- Social media platforms
- Location sharing
- In-person conversations

Why should you care?

- Your privacy isn't just a luxury – it's a security measure
- Attacks can be successful with little to no programming knowledge or ability
- Technological security measures can only protect you so much – you are your best defense

Phishing

Examples

- Emails
- Text messages
- Phone calls
- Social media messages and posts
- Suspicious hyperlinks

What is it?

Fake messages from a seemingly trusted or reputable source designed to convince you to…

- Reveal information
- Give unauthorized access to a system
- Click on a link
- Commit to a financial transaction

Why should you care?

- Extremely common
- Can have severe consequences
- Devil‘s in the details

Would This Email Fool You?

New message

From Legitimate-Looking-Source@notquiteyourworkemail.com

Subject Response Required ASAP– Covid-19 Preparedness

Covid-19 Prepardness

Tom,

Due to the ongoing corona virus outbreak, “Your Company Name” is actively taking safety precations by instituting a Comunicable Disease Management Policy. The policy is a part of our organizatinal preparedness, and we require all employees to read and acknowledge the policy by the end of the day.

Also we are currenting collecting donations for frontline workers here

www.fakewebsite.com/gotcha.exe
Click or tap to follow link.

Sincerely Yours,
BossMann

REPLY

NATIONAL CYBERSECURITY AWARENESS MONTH

Swatting

Did You Know?

Your location is embedded as metadata in every picture you take with your phone. Turn location services off when you aren't using them to make it more difficult for bad actors to view this information.

What is it?

An attack centered around location sharing in which bad actors call the police claiming the victim has committed a crime...

- Bomb Threat
- Armed Intruder
- Violent Incident

Why should you care?

- Physical and immediate consequences
- Sometimes was intended merely as a prank
- Arrest and serious injury can result
- Reduce risk by sharing your location only with trusted individuals, and share vacation photos only after you've returned safely home

Other Avenues of Attack

Examples

- Smart devices
- Mobile phone
- Thermostat
- Vehicles
- Gaming consoles
- Printers
- Medical equipment
- Industrial systems

What are your vulnerabilities?

- Internet of everything
- Any device connected to your network
- Information collection
- Remote access
- Bluetooth
- Open ports

Why should you care?

- Your network can be used to attack someone else
- Any device that stores information or is connected to the internet can be a vulnerability
- Assume that you are vulnerable, and take measures to understand and mitigate risk
- Don‘t be the “low-hanging fruit”

How Can You Better Protect Yourself Online?

Secure your networks.

Wireless routers are a way for cybercriminals to access online devices.

Stay up to date.

Keep software updated to the latest versions and set security software to run regular scans.

If You Connect It, Protect It.

One proven defense against intrusion is updating to the latest virus protection software.

Double your login protection.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you.

NATIONAL CYBERSECURITY AWARENESS MONTH

Password Tips

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

NCSAM's Theme and Key Message

Theme:

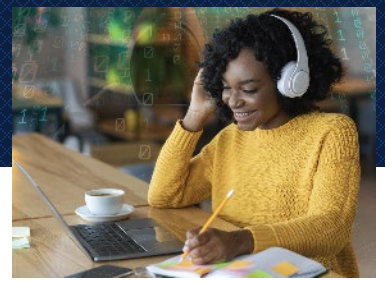
- **Do Your Part. #BeCyberSmart.**

Key Message:

- **If You Connect It, Protect It.**

NATIONAL CYBERSECURITY AWARENESS MONTH

NCSAM 2020 Schedule



October 1 and 2:
Official NCSAM Kick-off

WEEK 1:
Week of October 5
If You Connect It, Protect It

WEEK 2:
Week of October 12
Securing Devices at Home and Work

WEEK 3:
Week of October 19
Securing Internet-Connected Devices in Healthcare

WEEK 4:
Week of October 26
The Future of Connected Devices

NATIONAL CYBERSECURITY AWARENESS MONTH

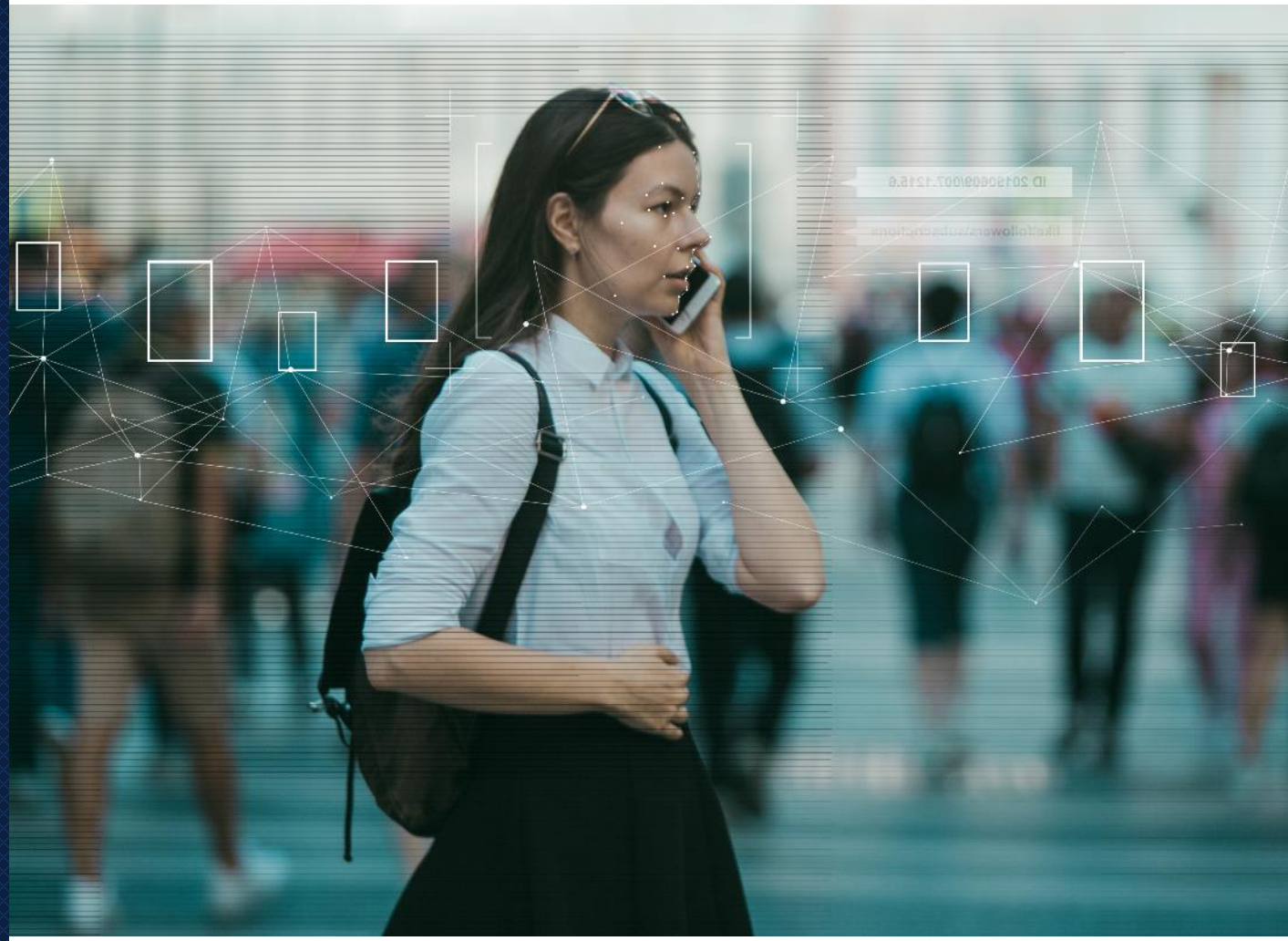
NCSAM Week 1:
If You Connect It, Protect It.

NATIONAL CYBERSECURITY AWARENESS MONTH

NCSAM Week 2:
Securing Devices at Home and Work

NCSAM Week 3:
Securing Internet-Connected Devices in Healthcare

NCSAM Week 4:
The Future of Connected Devices



NATIONAL CYBERSECURITY AWARENESS MONTH

Raise Awareness and Get Involved

- Promote National Cybersecurity Awareness Month in social media; use the #BeCyberSmart hashtag
- Pass on cybersecurity tips to your friends, family, and coworkers

NATIONAL CYBERSECURITY AWARENESS MONTH

For more information, contact stopthinkconnect@hq.dhs.gov

Visit www.cisa.gov/ncsam or staysafeonline.org/cybersecurity-awareness-month/ for more resources.

NATIONAL CYBERSECURITY AWARENESS MONTH