THE STOP.THINK.CONNECT.™ CAMPAIGN:
GEORGE MASON UNIVERSITY
CYBERSECURITY AWARENESS EVENT
October is National Cyber Security Awareness Month (NCSAM)!

NCSAM engages public and private sector partners around the country to raise awareness and educate Americans about cybersecurity. NCSAM is sponsored by DHS, the National Cyber Security Alliance (NCSA), and the Multi-State Information Sharing and Analysis Center.

- Started in 2004, NCSAM has been formally recognized by the President; Congress; federal, state, and local governments; and leaders from industry and academia.

- 2014 marks NCSAM’s 11th year, spreading cybersecurity awareness across the nation.

NCSAM is a month to focus on the cyber awareness successes from year-round efforts.
ABOUT STOP.THINK.CONNECT.

• In 2009, President Obama issued the *Cyberspace Policy Review*, which tasked the Department of Homeland Security (DHS) with creating an ongoing cybersecurity awareness campaign—Stop.Think.Connect.—to help Americans understand the risks that come with being online.

• Stop.Think.Connect. challenges the American public to be more vigilant about practicing safe online habits and persuades Americans to view Internet safety as a **shared responsibility** at home, in the workplace, and in our communities.
SHARED RESPONSIBILITY

• Students, faculty, and staff play a critical role in promoting cybersecurity.
• Not only do they rely on technology to perform daily functions, but the Internet provides easy ways for them to stay connected and informed.
• However, these conveniences come with increased risks.
• Many of the crimes that occur in real life are now facilitated through the Internet, including human trafficking, credit card fraud, identity theft, and embezzlement.
• No country, industry, community, or individual is immune to cyber risks, and no single organization can solve our nation’s cybersecurity challenges alone.
AMERICANS AND THE INTERNET

• One in five (18%) Americans has been the victim of a cybercrime

• 15% of Americans have never checked their social networking privacy and security account settings and only 18% said the last time they checked their settings was within the past year

• In 2012, 31% of all identity theft complaints received by the Federal Trade Commission were filed by young adults

Sources:
1. 2011 NCSA/McAfee Internet Home Users Survey
2. Ibid
3. cencal.bbb.org/article/attention-college-students-43437, 2013
Universities store valuable data, such as:
• Cutting-edge research
• Sensitive commercial and government information
• Personal information on test subjects, students, and faculty

Threats are both internal and external:
• Corporate and nation-state espionage
• “Hacktivists” and cyber criminals
• Students and other insiders

Aspiring medical student sentenced to three months in prison in MCAT hacking case – Washington Post, December 2013

Universities Face a Rising Barrage of Cyberattacks – New York Times, July 2013
CYBER ISSUES THAT AFFECT THE UNIVERSITY COMMUNITY

• Social Media Use
• Fraud & Phishing
• Sharing Information Online
• Online Identity Management
• Cyber Predators
• Identity Theft
• Mobile Security
While social media allows us to stay more involved, informed, and interconnected than ever before, it comes with risks.

Cyber criminals love when you share information online. They can use details from your Facebook Timeline and where you’ve “checked-in” to follow your every move.

Did You Know?
The Library of Congress archives every single public tweet
Facebook posts can be used in court

Sources: 1. Library of Congress; 2. Lawyers.com
**FRAUD & PHISHING**

**Fraud** is the intentional perversion of truth in order to induce another to part with something of value.

**Phishing** is a scam by which a user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.

**Tips:**
- Most organizations—banks, universities, companies, etc.—don’t ask for your personal information over email. Beware of requests to update or confirm your personal information.
- Make sure you change your passwords often and avoid using the same password on multiple sites.
- Be wary of messages that encourage you to act immediately, as well as offers that invite you to join an event or group on a social networking site with incentives like free gift cards.
PHISHING EXAMPLE

Subject: FW: Agenda
From: Steven Chu steven.chu@gmail.com
Date: Wed, 02 Mar 2011 03:21:01
To: you@lbl.gov

This came in earlier this morning. FYI,

----- Original Message ----- 
From: Morgan, Susan (ORO) [mailto:smorgan@doe.gov]
Sent: 3/2/2011 3:21:01 AM
To: Steven, Chu;
Cc: Bisell, Mina;
Subject: Agenda
Attachment: agenda.exe

Thanks Steven, I enjoy knowing you care about this!

Susan

Susan Morgan
Manager (510) 495-2522
smorgan@doe.gov

Source: Lawrence Berkeley National Laboratory
Fraud and phishing can become more effective when we over-share information online. Criminals use information about a person’s birthday, routine, hobbies, and interests to impersonate a trusted friend or convince the unsuspecting that they have the authority to access personal or financial information. The education industry is one of the most targeted for phishing.¹

Source: Symantec Intelligence Report, Sep. 2013
REAL LIFE EXAMPLE

Sharing too much information online can have serious consequences.

• A female student at the University of Central Florida made headlines after she was stalked by a fellow student via Twitter and YouTube
  – She received death threats over Twitter from her stalker
  – The stalker also posted at least 27 lewd and threatening videos to her on YouTube, sent threatening messages to her over Facebook, and left hundreds of messages on her voicemail
MANAGING YOUR ONLINE IDENTITY

Set Up Privacy Restrictions
• Your social media network has likely expanded to include peers and potential employers who may have access to your photos, comments, check-ins, and status updates. Spend time creating appropriate privacy settings for the various members of your network.

Think About Your Future
• Perform a quick search of yourself online. Do your findings represent the identity you would want a potential employer or university admissions officer to see?
REAL LIFE EXAMPLE

In 2013, a sorority member at the University of Maryland sent a scathing email to her chapter about being “awkward” and “boring” at Greek Week events.

- Email was widely distributed and publicized through social media and traditional media channels
- Demonstrates how what you say online, even in an email, can damage your reputation and that of your school or organization
Cyber predators are people who search online for other people in order to use, control, or harm them in some way

Tips:
- Keep your personal information private, including the names of your family members, your school, your telephone number, and your address
- Think twice before you post or say anything online; once it’s in cyberspace, it’s out there forever
- If you think someone is contacting you under false pretenses, inform university or local authorities
IDENTITY THEFT

Identity theft is the illegal use of someone else’s personal information in order to obtain money or credit.

Tips:

• Keep social security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name and date of birth.
• Don’t open emails from strangers and don’t click on links for unfamiliar sites.
• Lock your computer and smartphone whenever they are not in use.
• Create strong passwords with eight characters or more that use a combination of numbers, letters, and symbols.
Mobile devices enable Americans to get online wherever they are. It’s important to understand how to protect yourself when connecting on the go.

Tips

- Change any pre-configured default passwords on your mobile device to ones that would be difficult for an outsider to guess
- Use your mobile device carefully; emails that can harm your computer can also harm your mobile device
- Be sure to review and understand the details of an app before installing it and be wary of the information it requests
- Restrict access to your wireless networks by only allowing authorized users access to your network
What Else Can You Do to Stay Safe Online?
SIMPLE TIPS

Own Your Online Presence

• Always use privacy settings on social networking websites

• Think twice about what you are posting and saying online. It can affect your ability to get a job later in life

Protect Yourself

• Limit your online friends to people who you actually know

• Trust your gut if you feel threatened or uncomfortable because of someone or something you find online

Protect Your Computer

• Be cautious about opening attachments or clicking on links

• Use peer-to-peer (P2P) file-sharing services with caution

• Remember that free stuff—games, ring tones, and screen savers—can hide viruses or spyware
Are You Interested in a Career in Cybersecurity?
VIDEO: DHS CYBER CAREERS

IT TAKES A GREAT TEAM
The Stop.Think.Connect. Campaign also promotes science, technology, engineering, and math (STEM) education among students.

To help keep our computers and our country’s networks safe, we need more cybersecurity professionals.

To do that, we need students who have skills in science, technology, engineering, and math.

To learn more about STEM education and careers, visit the National Initiative for Cyber Careers and Studies (NICCS) Portal at http://niccs.us-cert.gov/
CALL TO ACTION

Become an advocate on your campus or in your community to help educate and empower the American public to take steps to protect themselves and their families online.

- Become a Friend of the Campaign by visiting www.dhs.gov/stopthinkconnect
- Link to the Campaign to share resources
- Distribute tips and resources in an email, campus newspaper article, blog or social media post
- Team up with other academic institutions to bring cybersecurity awareness to the community
- Participate in National Cyber Security Awareness Month
The Stop.Think.Connect. Campaign provides a number of resources to the public, with toolkit materials designed for:

- Government
- Industry
- Law Enforcement
- Small Business
- Older Americans
- Parents and Educators
- Students (K-8, 9-12, and Undergraduate)
- Young Professionals

Download at: www.dhs.gov/stophinkconnect
CONTACT INFORMATION

For additional information, contact:
stopthinkconnect@dhs.gov

Or visit:
www.dhs.gov/stopthinkconnect
Questions?