Science and Security – Protecting Research Data

Dennis Schmidt

Assistant Vice Chancellor for Information Security and Privacy and Chief Information Security Officer

UNC INFORMATION TECHNOLOGY SERVICES

Agenda

- Why is Security Important?
- Federal Regulations
- Security Requirements for State Contracts
- Foreign Travel
- Risk Assessment Processes
- Available Services from ITS Security
- Recent Security Enhancements
- Safecomputing.unc.edu

Why is Security Important?

- **The threat is real!**
  - Nation-state sponsored actors are actively attempting to steal your research
  - COVID-19 research is of particular interest now, but any research data is at risk
  - Even if your data is not “sensitive”, it is still valuable
  - Thieves can obtain patents or build up capability based on your hard work
  - Insider threat is a growing concern
  - Export laws affect data, too.

https://research.unc.edu/compliance/export-controls/

National Security Working Group

- “Some foreign governments have initiated systematic programs to unduly influence and capitalize on U.S.-conducted research, including that funded by NIH.”
- China’s Thousand Talents program
  - 56,000 recruits
  - 6,000 top-tier recruits across many scientific disciplines and at highly prestigious institutions
  - Self-stated mission: “…to gather the global wisdom and create the China great exploit.”
- These kinds of Information collection efforts are not unique to China

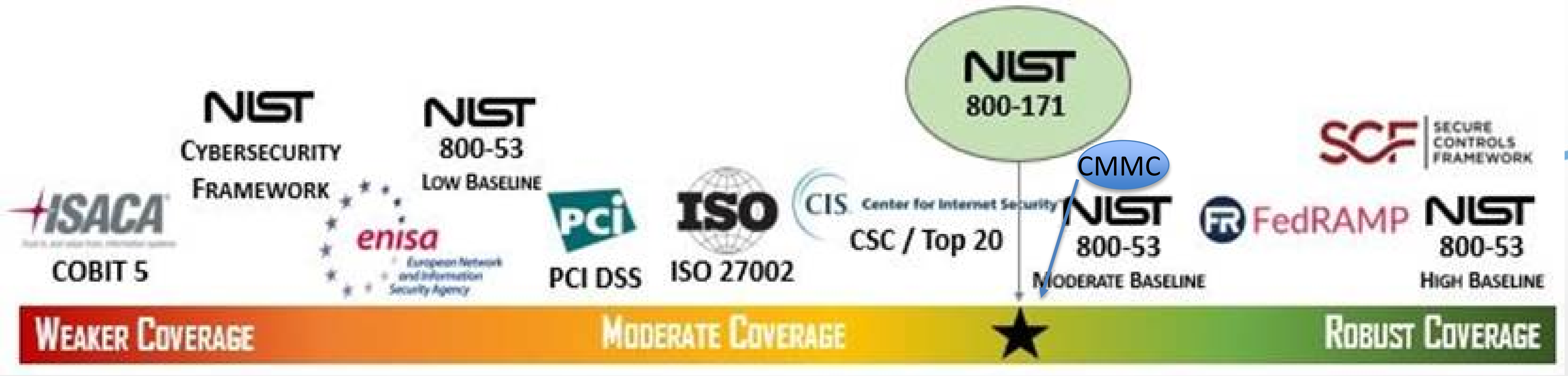
*******https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf*

Advanced Persistent Threat (ATP)

- Acronym to describe well-funded and organized cyber attackers
- Primarily nation-state sponsored or organized crime
- Highly trained professionals; many are government sanctioned and/or funded
- Teams may be assigned to specific targets (e.g. UNC is a likely target!)
- Fly low, slow, and persistent to avoid detection.
  - Shotgun scans from multiple addresses
  - Targeted phishing attacks
  - Social engineering and background research
  - Spread to other targets once inside a network
- Very effective and often successful

Federal Regulations

More security frameworks than you can shake a stick at!



https://www.complianceforge.com/reasons-to-buy/nist-800-171-compliance/

Federal Regulations

- **NIST 800-53 (Rev 4 is current. Rev 5 in draft)**
  - Intended for federal agencies, but required by State of NC
  - 159 Security controls plus 102 security enhancements for Moderate risk level
  - Difficult for a university to satisfy all 261.
  - Only 1 certified environment in ITS (Secure Research Workspace)
- **NIST 800-171 (Rev 2 is current.)**
  - Focuses on Controlled Unclassified Information (CUI) such as research or PII
  - Intended for entities that support federal contracts
  - 110 Security controls
  - Much more feasible for universities to comply
  - Several systems at UNC have met 800-171 requirements.
  - 800-171B in draft. – Focuses on protection from Advanced Persistent Threats

Federal Regulations

- **Cybersecurity Maturity Model Certification (CMMC)**
  - Applies to DOD contracts – 5 levels of certification
  - Levels 1-3 loosely based on NIST 800-171.
  - Required 3rd party audit and certification every 3 years.
  - Training classes for auditors underway now.
  - Becomes effective end of 2020. Will be phased in as auditors come up to speed.

Federal Regulations

NDAA Section 889

- The National Defense Authorization Act (NDAA) for FY 2019 includes two new prohibitions regarding telecommunications and video surveillance equipment and services.
- Also covered in FAR 532.204-24/25/26
- The new rules apply to UNC-CH as the recipient of contracts and grants from the federal government.
- Section 889, Part A, effective August 13, 2019, prohibits the government from obtaining certain telecommunications equipment and services (as part of a contract or other instrument) produced by the following companies and their subsidiaries/affiliates:
  - Huawei Technologies Company
  - ZTE Corporation
  - Hyetra Communications
  - Hangzhou Hikvision Digital Technology Company
  - Dahua Technology Company

Federal Regulations

NDAA Section 889 (cont.)

- NDAA Section 889, Part B, effective August 13, 2020, prohibits government contractors from using certain telecommunications equipment or services (as a substantial or essential component of any system or as critical technology as part of any system) produced by the same companies listed on the prior slide.

- “Use” applies to any UNC-CH function, regardless if the function is involved in the performance of a Federal contract.

- Contractors are required to conduct a “reasonable inquiry” prior to submitting a certification to the government under Part B.

  - Currently contract specific certification.
  - Effective October 26, 2020, an annual certification requirement will be in place.

Federal Regulations

NDAA Section 889 (cont.)

- For Federal grants, a new Uniform Guidance provision prohibits recipients and subrecipients from obligating or expending grant funds to procure or obtain equipment, services, or systems that uses telecommunications equipment or services (as a substantial/essential component or critical technology as part of any system) produced by any of the listed companies.

- A working group has been established within the University to develop the University's compliance plan. Further information will be forthcoming to the campus.

Requirements for Contracts with State Agencies

- **New more stringent security requirements in State Contracts**
  - Applies to new contracts AND renewals of existing projects.
  - Compliance with NC State Information Security Manual.
    - Based on NIST 800-53 MODERATE – regardless of data classification!
  - Required annual risk assessment.
    - Every third year must be performed by outside party. (Costly)
  - Annual update of Vendor Readiness Assessment Report (VRAR)
  - NC DHHS has been particularly rigid in applying requirements.
  - Before signing a new or renewed contract, check with your IT support to make sure you can comply!

UNC INFORMATION TECHNOLOGY SERVICES

Foreign Travel

- https://safecomputing.unc.edu/identity/travel-safely-with-technology/
- **Before your trip:**
  - **Assume that your device will be compromised** while visiting some countries!
  - Talk to your IT support staff for help to ensure that your devices are safely configured.
  - Take only the devices that you will need to use.
  - Consider taking a "burner" device that can be rebuilt when you return.
  - Ensure your devices are encrypted, so that if they become lost, no data can be stolen.
  - Ensure data is backed up on a server, drive, or other device NOT making the trip.
    - OneDrive is a great resource for that. Delete any data not needed on the trip.
  - Ensure you have a VPN client installed and know how to use it.
  - Ensure your PC has the latest patches and that antimalware software is updated.
  - Disable Bluetooth and Wi-Fi on your devices and only turn them on when needed.
  - Carry charging devices so that you won't have to use a public charging service.

Foreign Travel

- **During your trip:**
  - Do not use public Wi-Fi networks
  - Avoid using open Wi-Fi networks to conduct personal business, bank, or shop online.
  - If you absolutely must check your bank balance or make an online purchase while you are traveling, turn off your device's Wi-Fi connection and use your mobile device's cellular data Internet connection.
  - **Assume your data on any wireless network can be monitored**, and act accordingly.
  - Use a VPN whenever possible, especially while on public networks
  - Do not let anyone else borrow or use your devices.
  - Do not borrow any devices (e.g. a USB drive) for use on your computer.
  - Do not install any software on your computer other than what your local IT department has put in place.
  - Be aware of "shoulder surfers" — anyone physically monitoring the use of your device.
  - Keep your devices under your physical control or secured in a proper location when they are not.
  - Never check devices or storage devices in luggage.

Foreign Travel

- **When you return:**
  - **Assume that your machine was compromised** while on your trip.
  - Change any passwords that you used on the trip. Make sure that you use different passwords for different accounts.
  - Clean your machine by running an antivirus scan of your device for malware and follow the instructions to correct any issues.
  - Consider “wiping” the hard drive and restoring from backups made before your trip.
  - Talk to your local IT support. They should be able to help with this.

If you have any questions or need assistance with your travel preparations, please contact your local IT support, the UNC Study Abroad Office, or the ITS Service Desk at 919-962-HELP.

Risk Assessment Process

- *Any system that creates, receives, maintains, or transmits University-owned sensitive information OR that is considered mission-critical must have a risk assessment.*
- **What is a risk assessment?**
  - Process of evaluating the potential for loss or harm (risks).
  - Review of security measures implemented to assure they reduce risk.
  - Evaluate any vendors that might be a part of the project.
  - Developing a plan (POA&M) to treat any remaining risk (i.e. acceptance, mitigation, avoidance, transference).
- **How long does it take?**
  - It varies but the target is 5 weeks.
- **How do I request one?**
  - Talk to your local IT and submit a ticket at help.unc.edu.
- **Can my local IT conduct one?**
  - Possibly. We have partnered with SOM, Dentistry, SOP, SOPH, RENCI.

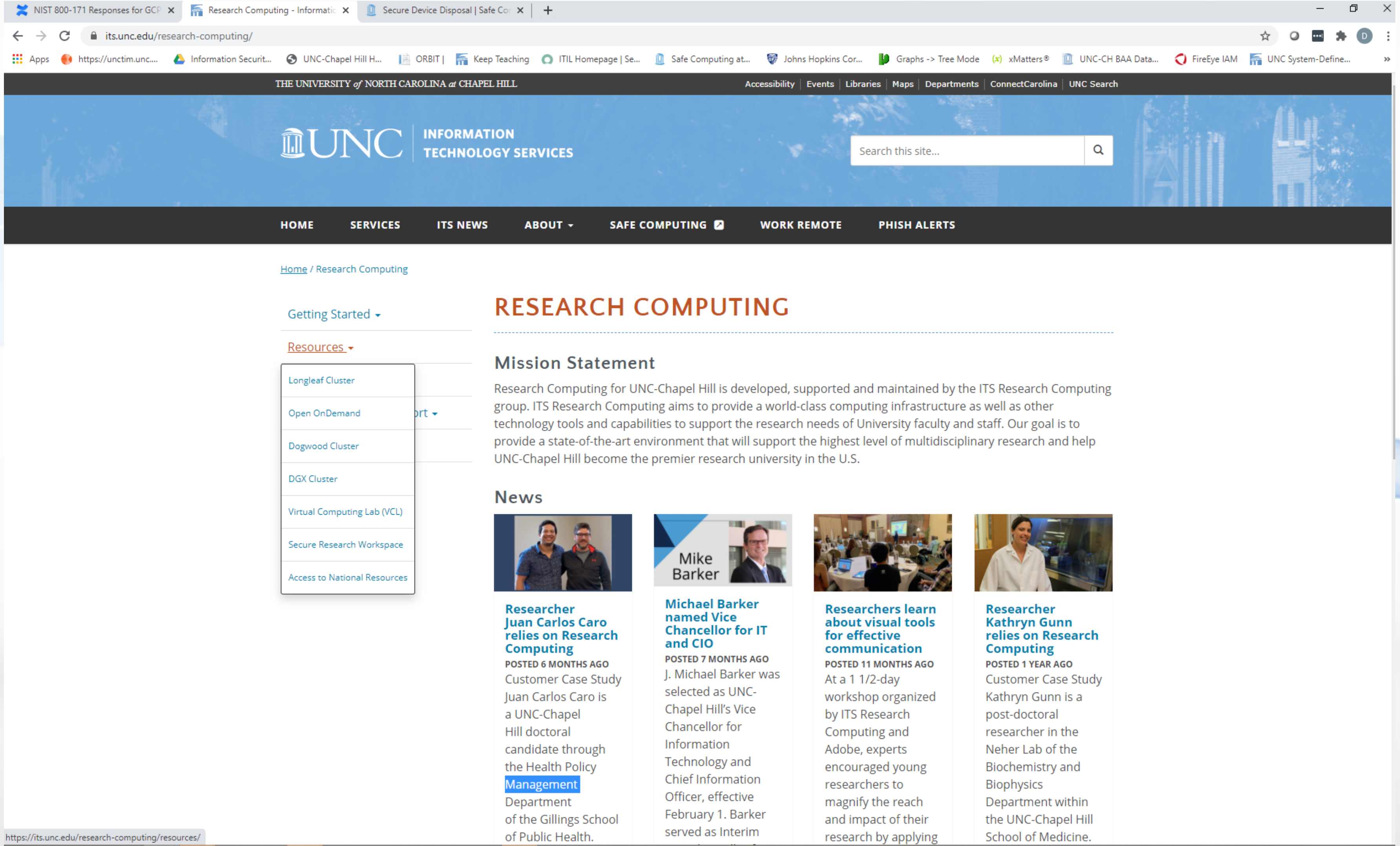
Available ITS Security Services

- **Security Outreach**
- **Phishing Campaigns**
- **Consultation**
- **Risk Reviews**
- **Incident Response**
- **Firewall service**
- **Vulnerability Management Tools**

UNC INFORMATION TECHNOLOGY SERVICES

Research Computing Resources

https://its.unc.edu/research-computing/



NIST 800-171 Responses for GCP
Research Computing - Informatic
Secure Device Disposal | Safe Co
its.unc.edu/research-computing/
Apps
https://unctim.unc....
Information Securit...
UNC-Chapel Hill H...
ORBIT |
Keep Teaching
ITIL Homepage | Se...
Safe Computing at...
Johns Hopkins Cor...
Graphs -> Tree Mode
xMatters®
UNC-CH BAA Data...
FireEye IAM
UNC System-Define...
THE UNIVERSITY *of* NORTH CAROLINA *at* CHAPEL HILL
Accessibility | Events | Libraries | Maps | Departments | ConnectCarolina | UNC Search
UNC INFORMATION TECHNOLOGY SERVICES
Search this site...
HOME
SERVICES
ITS NEWS
ABOUT
SAFE COMPUTING
WORK REMOTE
PHISH ALERTS
Home / Research Computing
Getting Started
Resources
Longleaf Cluster
Open OnDemand
Dogwood Cluster
DGX Cluster
Virtual Computing Lab (VCL)
Secure Research Workspace
Access to National Resources
rt
Mike Barker
https://its.unc.edu/research-computing/resources/

RESEARCH COMPUTING

Mission Statement

Research Computing for UNC-Chapel Hill is developed, supported and maintained by the ITS Research Computing group. ITS Research Computing aims to provide a world-class computing infrastructure as well as other technology tools and capabilities to support the research needs of University faculty and staff. Our goal is to provide a state-of-the-art environment that will support the highest level of multidisciplinary research and help UNC-Chapel Hill become the premier research university in the U.S.

News

Researcher Juan Carlos Caro relies on Research Computing

POSTED 6 MONTHS AGO

Customer Case Study Juan Carlos Caro is a UNC-Chapel Hill doctoral candidate through the Health Policy Management Department of the Gillings School of Public Health.

Michael Barker named Vice Chancellor for IT and CIO

POSTED 7 MONTHS AGO

J. Michael Barker was selected as UNC-Chapel Hill's Vice Chancellor for Information Technology and Chief Information Officer, effective February 1. Barker served as Interim

Researchers learn about visual tools for effective communication

POSTED 11 MONTHS AGO

At a 1 1/2-day workshop organized by ITS Research Computing and Adobe, experts encouraged young researchers to magnify the reach and impact of their research by applying

Researcher Kathryn Gunn relies on Research Computing

POSTED 1 YEAR AGO

Customer Case Study Kathryn Gunn is a post-doctoral researcher in the Neher Lab of the Biochemistry and Biophysics Department within the UNC-Chapel Hill School of Medicine.

Local IT Resources

- Get to know your local IT Support. They can be a great resource for helping keep your data secure.

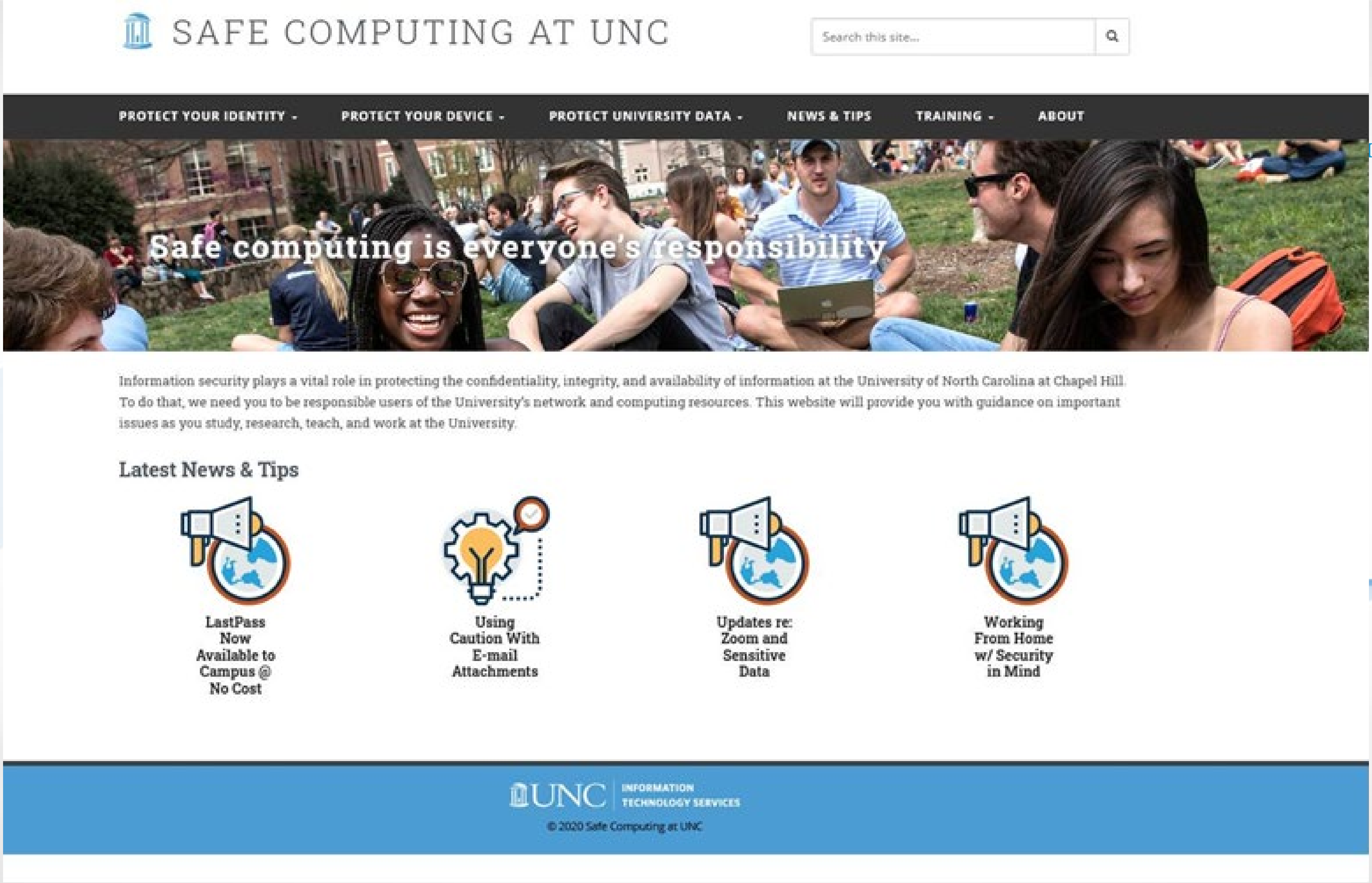
- Information Security Liaisons
- Consultation
- Help with Risk Reviews

UNC INFORMATION TECHNOLOGY SERVICES

Recent Security Enhancements

- **Firewall Expansion Project**
  - Goal: Move ALL campus VLANs behind hardware firewall (~200)
  - Will deny all incoming connection attempts unless specifically allowed by the end user
  - Not optional
  - Expected completion mid 2022
- **Mandiant/FireEye Managed Defense**
  - 24x7x365 monitoring of traffic going through our borders
  - 22,000 FireEye agents deployed on servers and user machines
  - Has already detected and blocked several web shell installations by attackers
- **LastPass Password Manager Enterprise License**
  - Helps users safely manage their passwords
  - **Free** to all faculty, staff, and students.
  - Registration for LastPass Premium (personal edition): https://lastpass.unc.edu

ICES



Safe computing is everyone's responsibility

Information security plays a vital role in protecting the confidentiality, integrity, and availability of information at the University of North Carolina at Chapel Hill. To do that, we need you to be responsible users of the University's network and computing resources. This website will provide you with guidance on important issues as you study, research, teach, and work at the University.

Latest News & Tips

- LastPass Now Available to Campus @ No Cost
- Using Caution With E-mail Attachments
- Updates re: Zoom and Sensitive Data
- Working From Home w/ Security in Mind

© 2020 Safe Computing at UNC

Overview of SafeComputing.unc.edu

- **Central website containing a wealth of IT security resources**
  - **Tips and News**
  - **End point security**
  - **Awareness training**
  - **What data is approved for central applications**
  - **Who is your Information Security Liaison?**
  - **Travel guidelines**
  - **Risk assessment guidelines**
  - **Working from home**
  - **Data encryption**

Questions?