Cybersecurity and the Remote Workforce

Safeguarding IT at UNC Charlotte

UNC CHARLOTTE

Office of OneIT

The University of
North Carolina
at Charlotte

QUICK STATS

UNC CHARLOTTE
uncc.edu

Our University

Largest regional University in Charlotte, NC

Eight colleges

29,615 students

4,500 faculty/staff

UNC CHARLOTTE
Office of OneIT

The University of North Carolina at Charlotte

QUICK STATS

UNC CHARLOTTE

uncc.edu

By the Numbers

Doctoral & research intensive institution

19,500+ computing devices

3 Campus locations

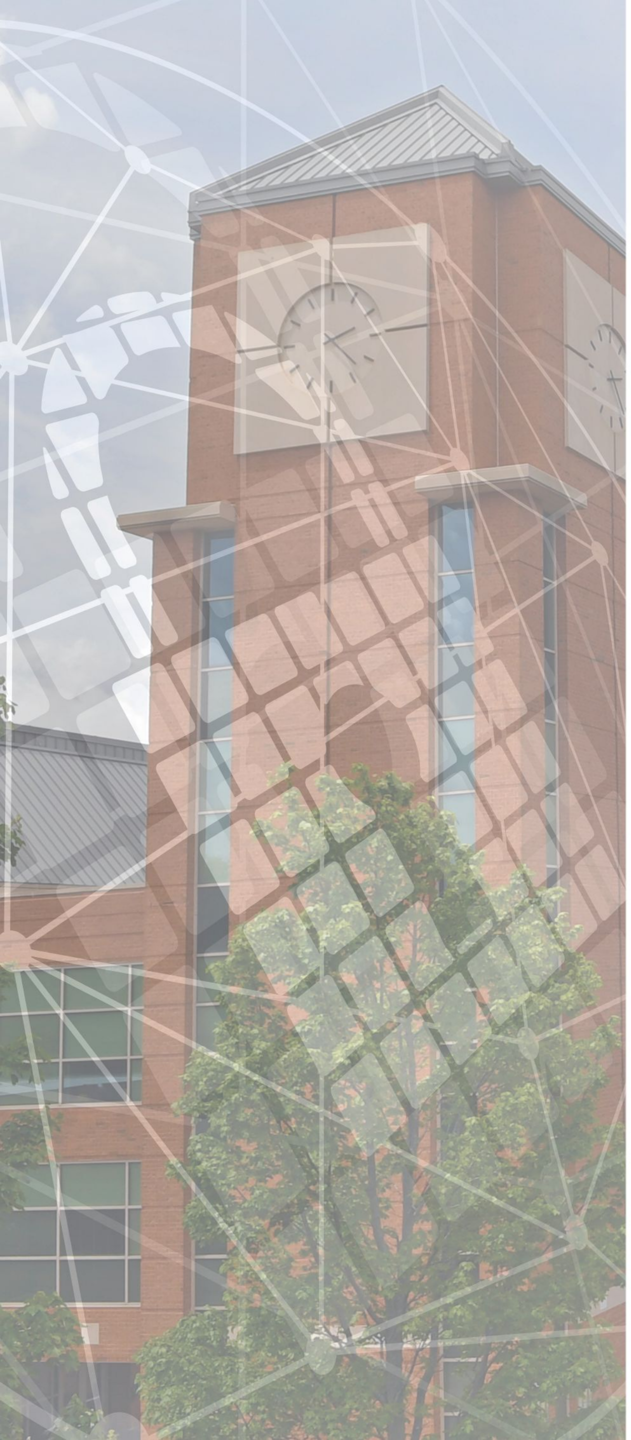
3,700 TB of storage

7 Cybersecurity Professionals

AWS, Azure, Google Cloud, On-Premise

4,801 remote workforce

UNC CHARLOTTE
Office of OneIT



The University of
North Carolina
at Charlotte

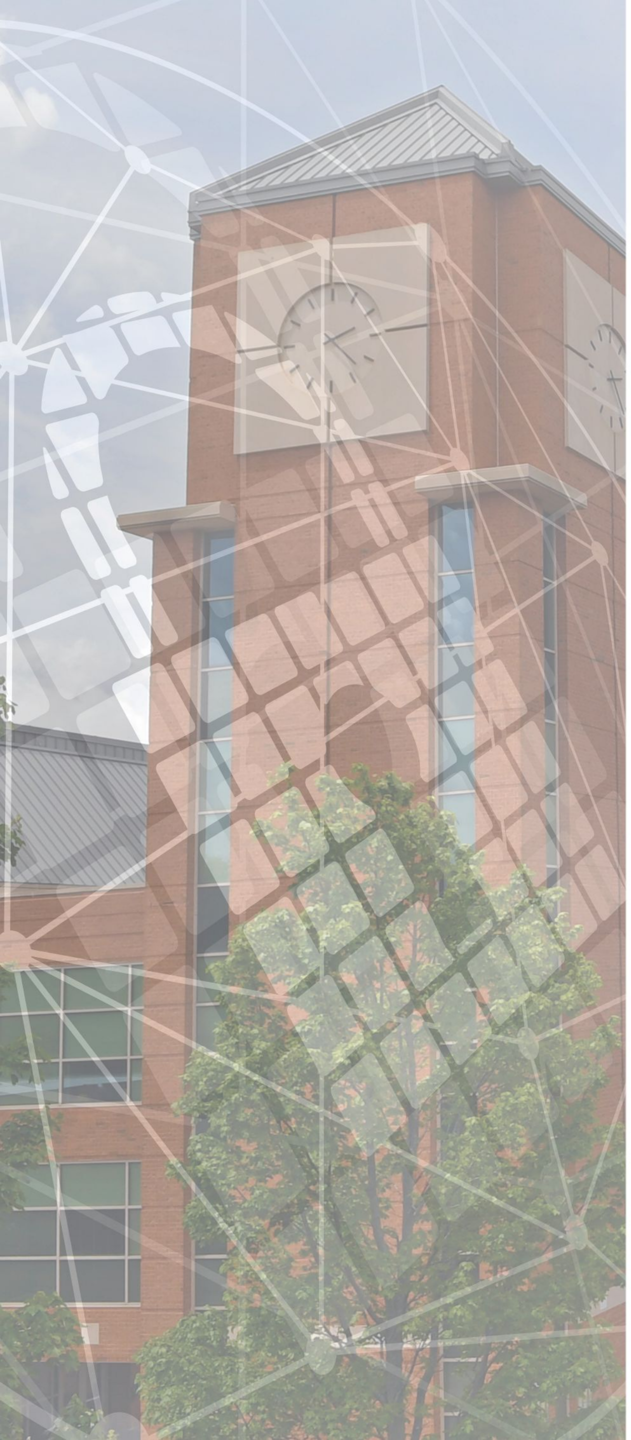
DIGITAL SECURITY

UNC CHARLOTTE
uncc.edu

Security Protection

- 1,000 system compromises blocked by Advanced Malware Protection (AMP) per month
- 22 million malware, phishing & spam emails blocked by Cisco Email Security (CES) per month

UNC CHARLOTTE
Office of OneIT



The University of
North Carolina
at Charlotte

DIGITAL
SECURITY

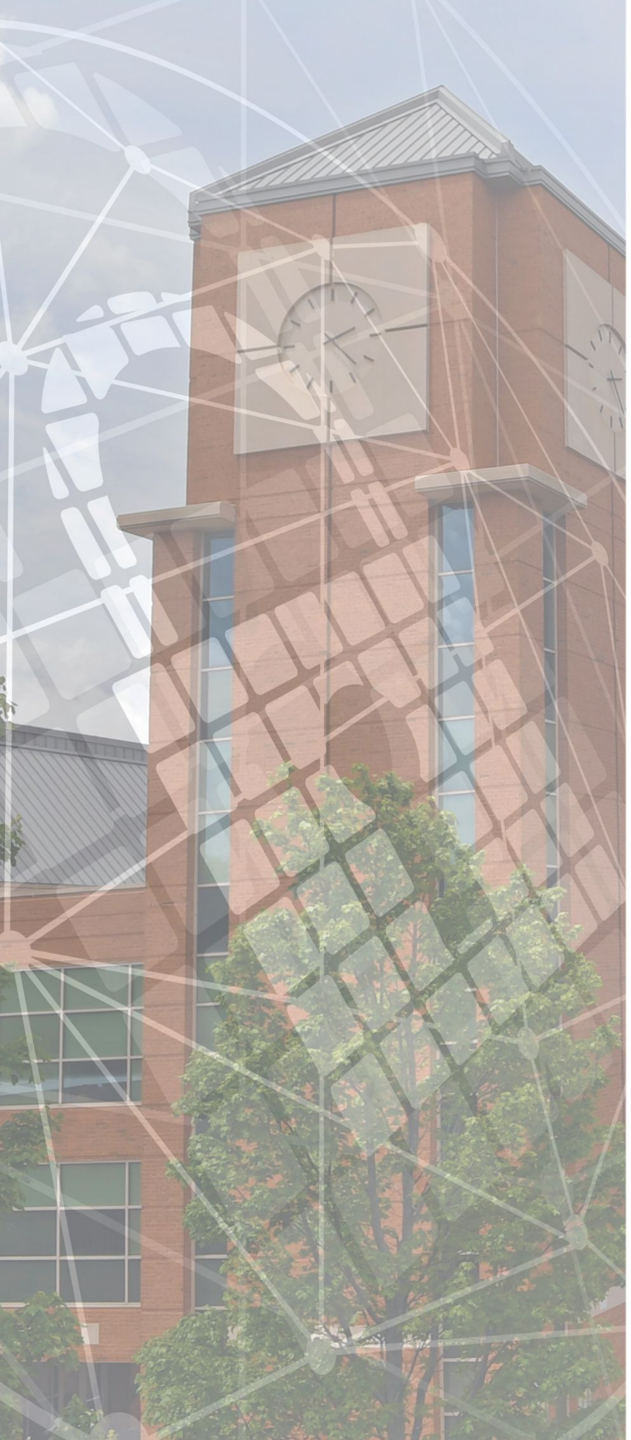
UNC CHARLOTTE
uncc.edu

Security Protection

400 million malicious perimeter connection attempts per day on average

200 account compromise detections and resets per month on average

UNC CHARLOTTE
Office of OneIT



The University of
North Carolina
at Charlotte

DIGITAL
SECURITY

UNC CHARLOTTE

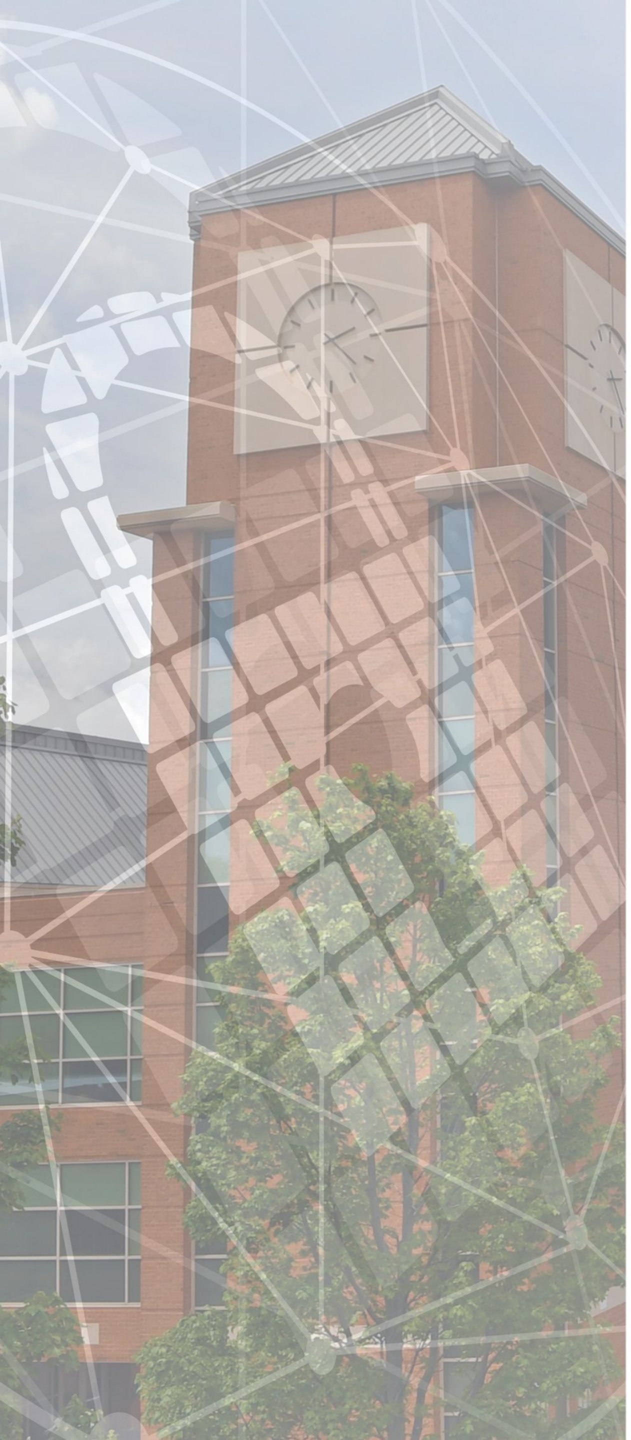
uncc.edu

Security Protection

200 Command & Control (C&C) & 100 data exfiltration attempts detected by Stealthwatch monthly

130,000 malicious URL attempts blocked by Umbrella monthly

UNC CHARLOTTE
Office of OneIT



The University of
North Carolina
at Charlotte

DIGITAL
SECURITY

UNC CHARLOTTE
uncc.edu

Breach Stats

Average cost of a U.S. Education sector breach: $4.2 million

Average breach size: 27,000 records

UNC CHARLOTTE
Office of OneIT

Our Top 3 Threat Vectors

UNC CHARLOTTE
Office of One IT

1

Phishing

Emails purporting to be from reputable sources to induce individuals to reveal personal information, such as passwords & credit card numbers

2

Malware

Short for “malicious software,” this intent to damage devices includes viruses, trojans, ransomware & spyware

3

Vulnerability Exploitation

Taking advantage of a vulnerability to compromise the confidentiality, availability, or integrity of a resource

Additional Threats We Face

Brute Force Attacks

Relentless trial & error attacks where the hacker attempts to determine passwords or access encrypted data

Nation-State Attacks

When hackers target government entities or any other industry with sensitive data or property. Examples include Crypto Mining resource theft & Intellectual property theft.

Human Error

Humans play a major role in the vulnerability of businesses worldwide

Data Exfiltration

A technique used by malicious actors to target, copy & transfer sensitive data

Social Engineering

Manipulation to get confidential information, credentials or access

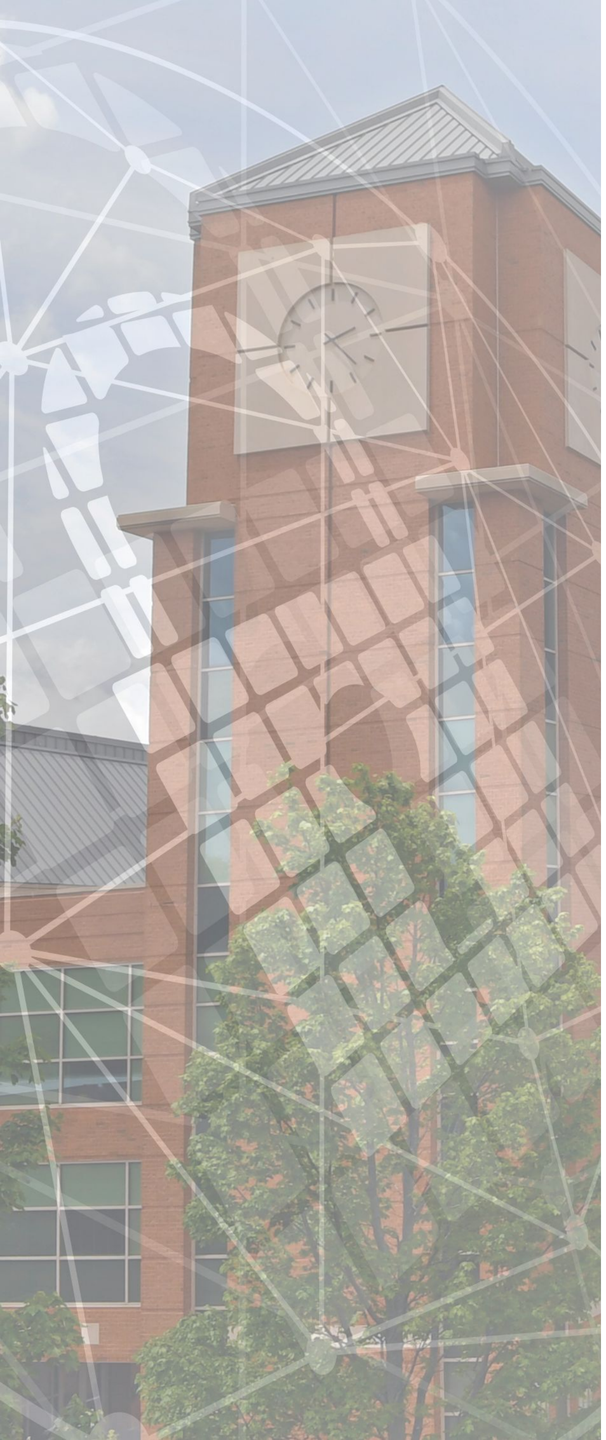
Denial of Service (DoS)

When legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor

Credential Theft

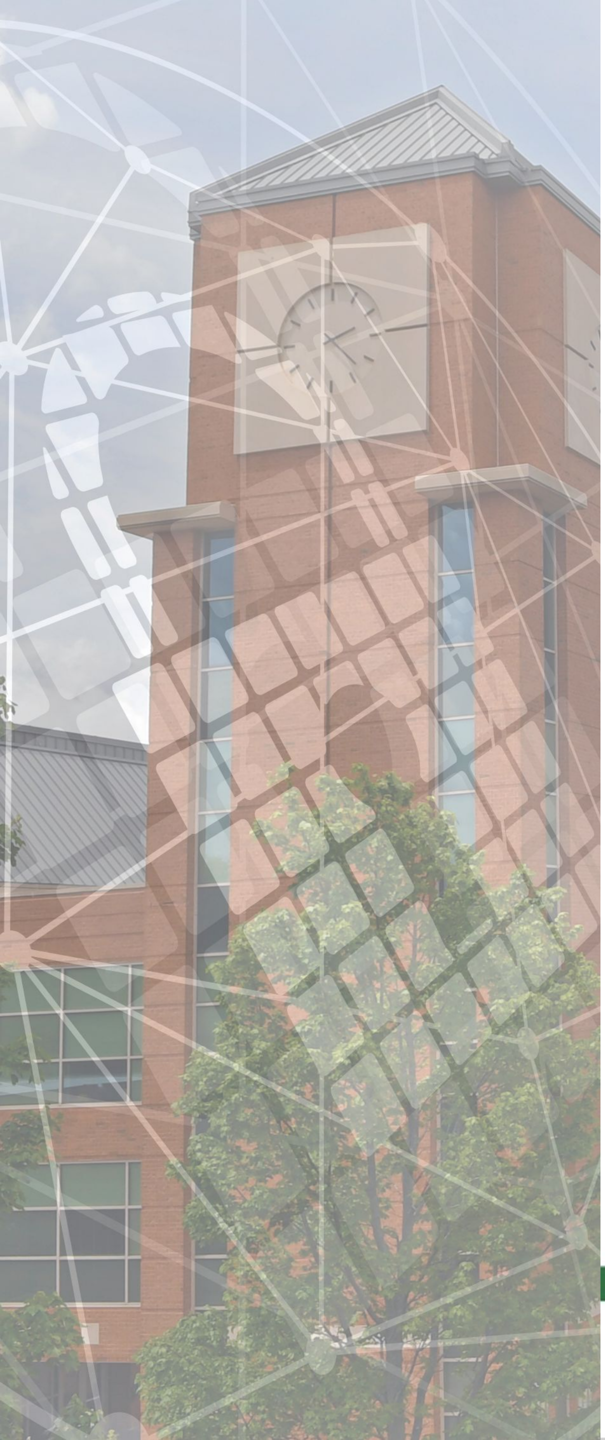
The unlawful attainment of an organization's or individual’s password(s) with intent to access & abuse/exfiltrate critical data & information

On-Campus vs Remote Security



- On-Campus
  - IPS/IDS
  - Network Firewall and Segmentation
  - DNS Security (Umbrella)
  - Next-Gen Antimalware (Amp)
  - Hardened Configuration (Center for Internet Security)
  - Enhanced Monitoring and Detection with Automated Response (Splunk)
  - Email Security (CES)
- Remote (Managed Univeristy Devices)
  - DNS Security (Umbrella)
  - Next-Gen Antimalware (Amp)
  - Hardened Configuration (Center for Internet Security)
  - Email Security (CES)

UNC CHARLOTTE
Office of OneIT



Endpoint Security

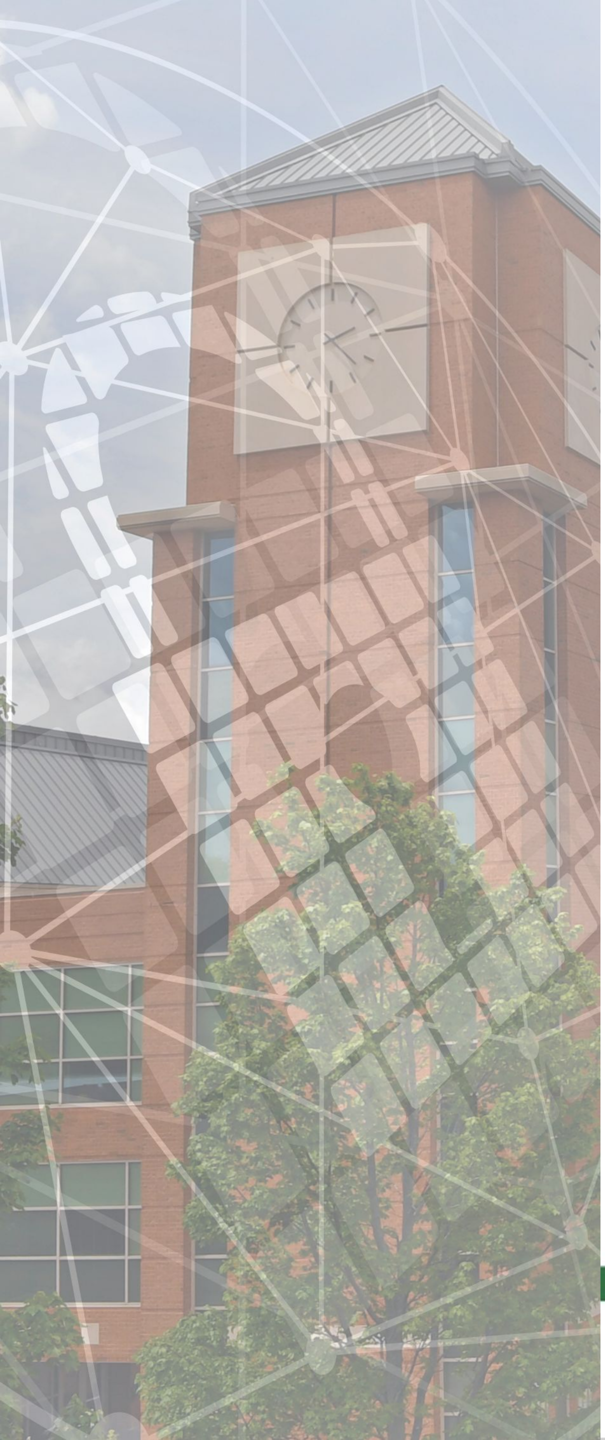
Endpoints

13,000 Computers & Tablets

700 Servers

- Next generation anti-malware (AMP)
- Domain Name System protection service (Umbrella)
  DNS = “Phonebook of the internet” e.g. uncc.edu
- Endpoint hardening
  Center for Internet Security Level 1 Security Standard
- Regular, phased-in patching
- Rapid7 Agents continuously monitor endpoint vulnerabilities

UNC CHARLOTTE
Office of One IT

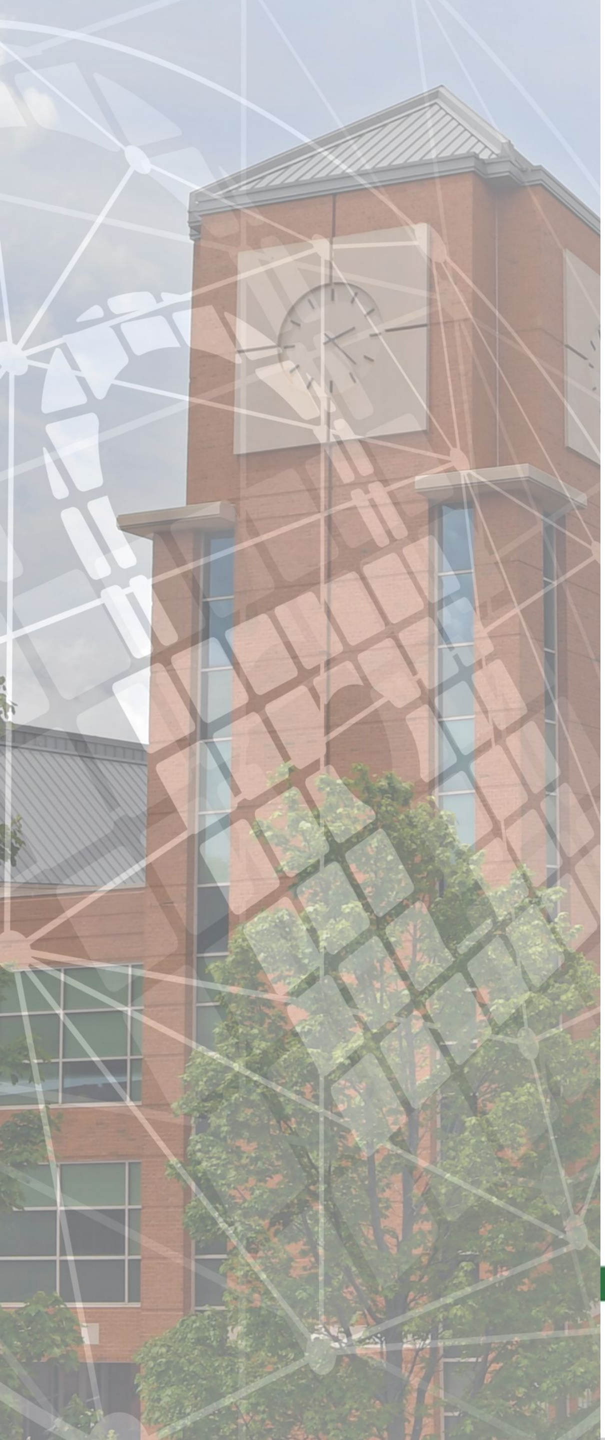


Advanced Malware Protection (AMP)

- Like virus protection but better because it pulls in threat information from multiple agencies in real-time

- Deployed on University managed endpoints & servers

UNC CHARLOTTE
Office of One IT



Umbrella

Domain Name System (DNS) protection service

DNS = "Phonebook of the internet" e.g. uncc.edu

- Protects users on- & off-campus from malicious websites by utilizing software installed on each University computer that analyzes web traffic

- Uses a global database of recognized offenders

- Stops attacks earlier with real-time analysis of unknown websites

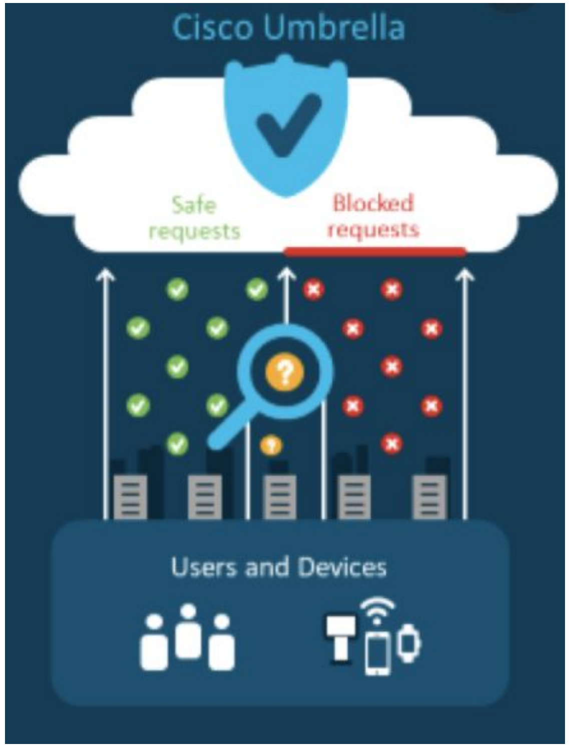
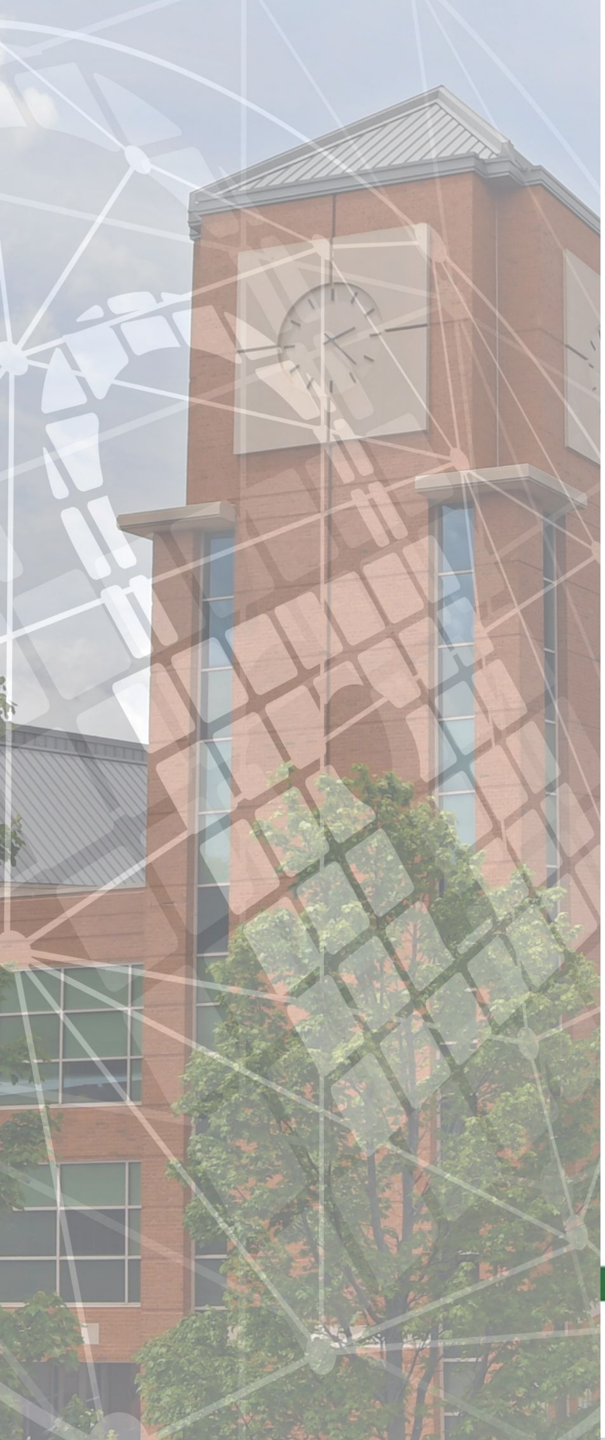


Image: Cisco

UNC CHARLOTTE
Office of One IT

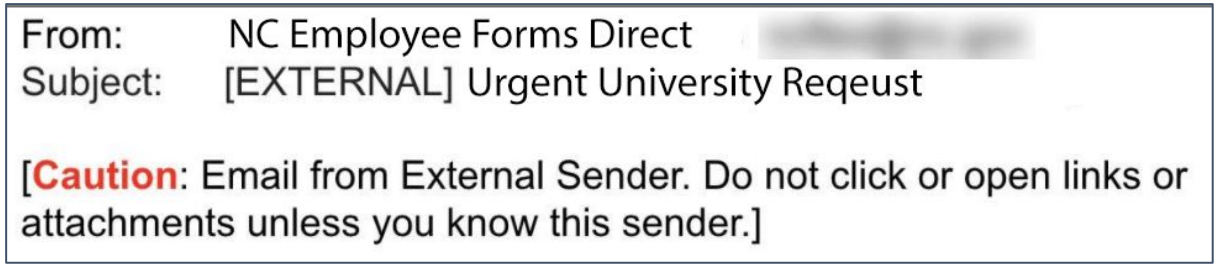


Cisco Email Security

47 mil Total incoming messages in 30 days

30 mil Incoming "threat" messages in 30 days

- Real-time analysis
- Emails identified as "threats" are NOT delivered
- Readers immediately see emails from external senders (outside @uncc) as flagged [EXTERNAL]



From: NC Employee Forms Direct [redacted]
Subject: [EXTERNAL] Urgent University Reqeust

[**Caution**: Email from External Sender. Do not click or open links or attachments unless you know this sender.]

UNC CHARLOTTE
Office of One IT

Cisco Email Security

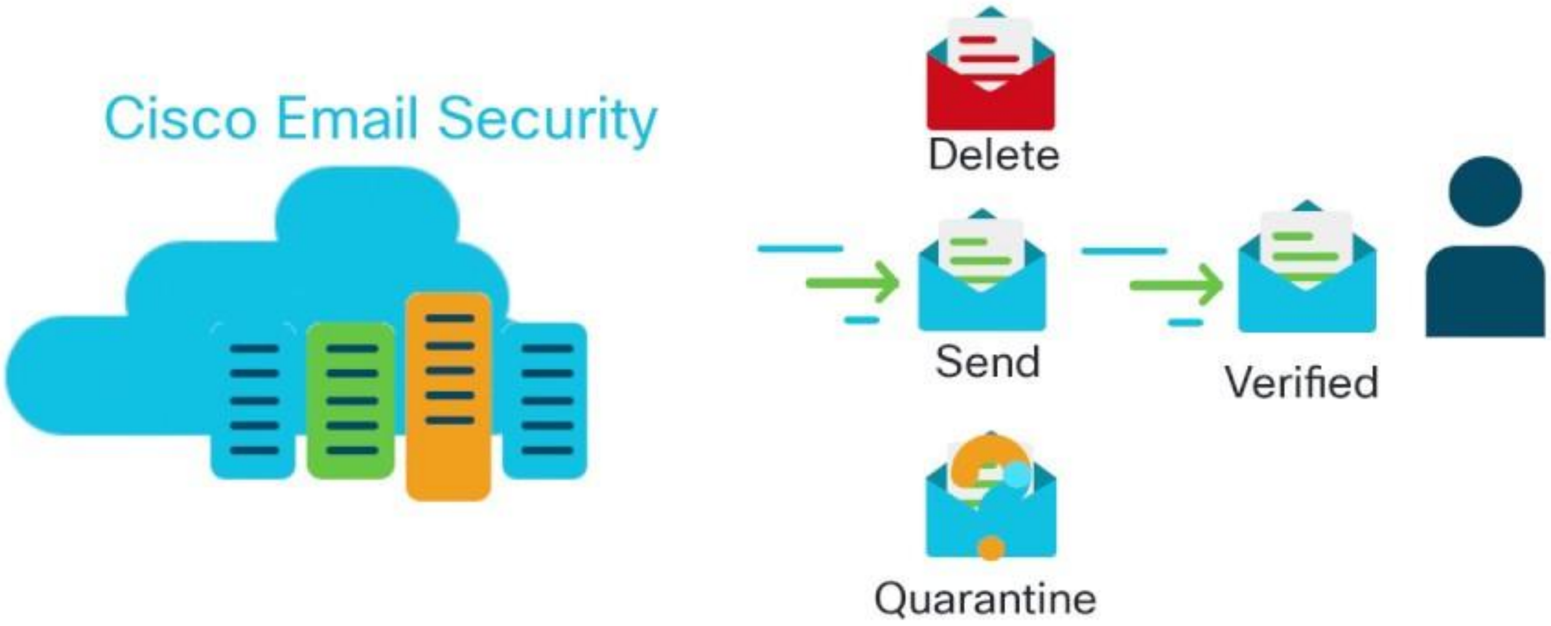
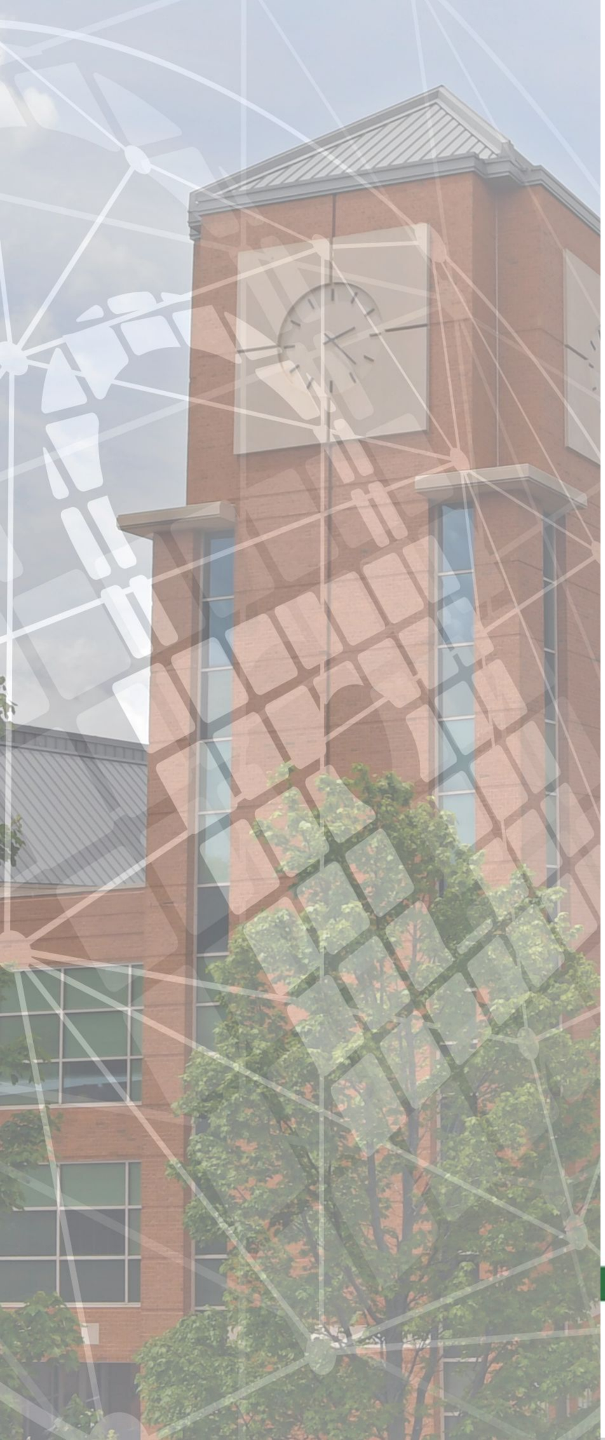


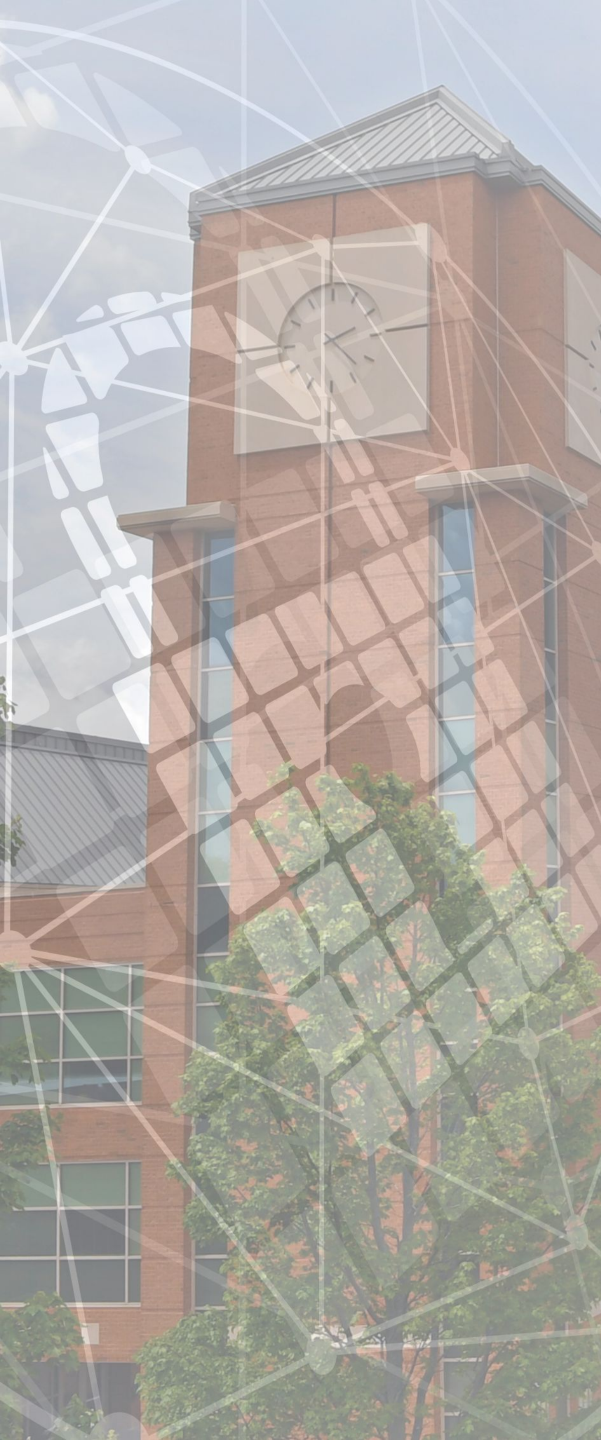
Image: Cisco YouTube



Stealthwatch

- Detects malicious behavior patterns by sampling traffic from University network devices
- Gathers real-time data from networked devices
- Uses data to detect behavior changes & predict threats

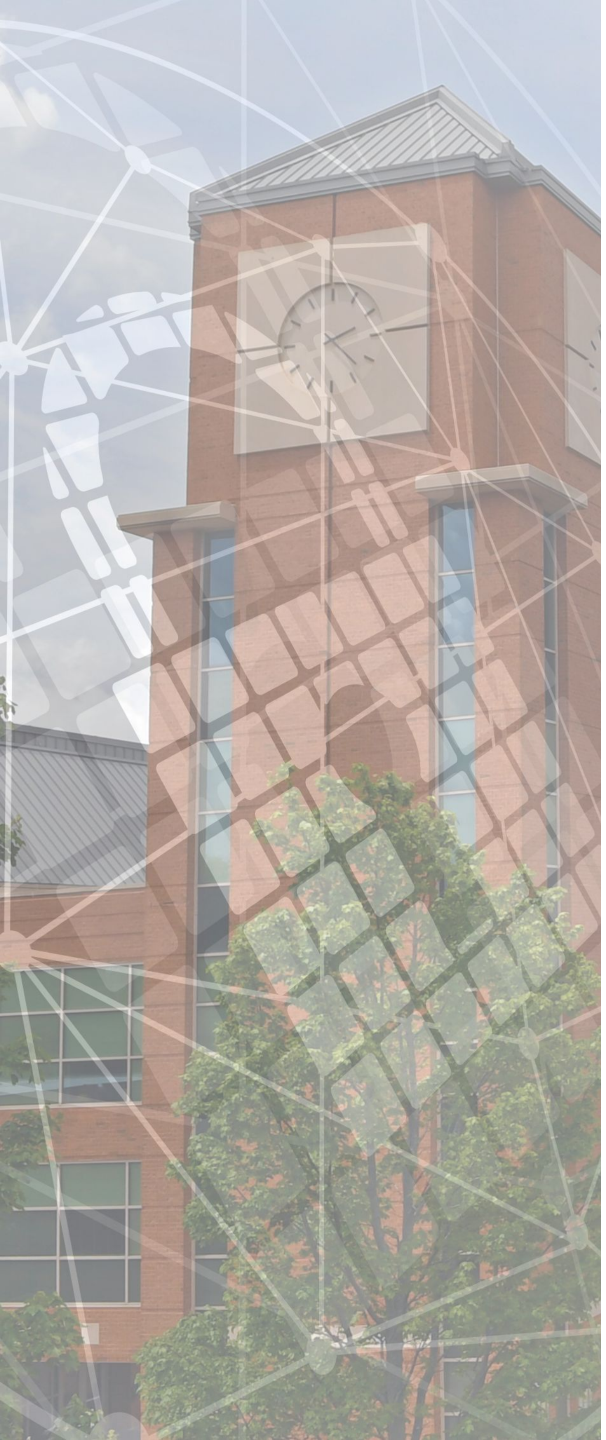
Detects threats from non-managed network devices & any device connected to our network



Remote Workforce Risks

- Some security protection measures are only available on campus
- Expanded attack vectors
  - System theft/damage
  - Insecure home networks
  - Poor user practices
- Little to no remediation or detection capability
- Employees using personal devices to accomplish sensitive University tasks
- Social Engineering
- Data theft/loss
- Ransomware
- Denial of Service

UNC CHARLOTTE
Office of OneIT

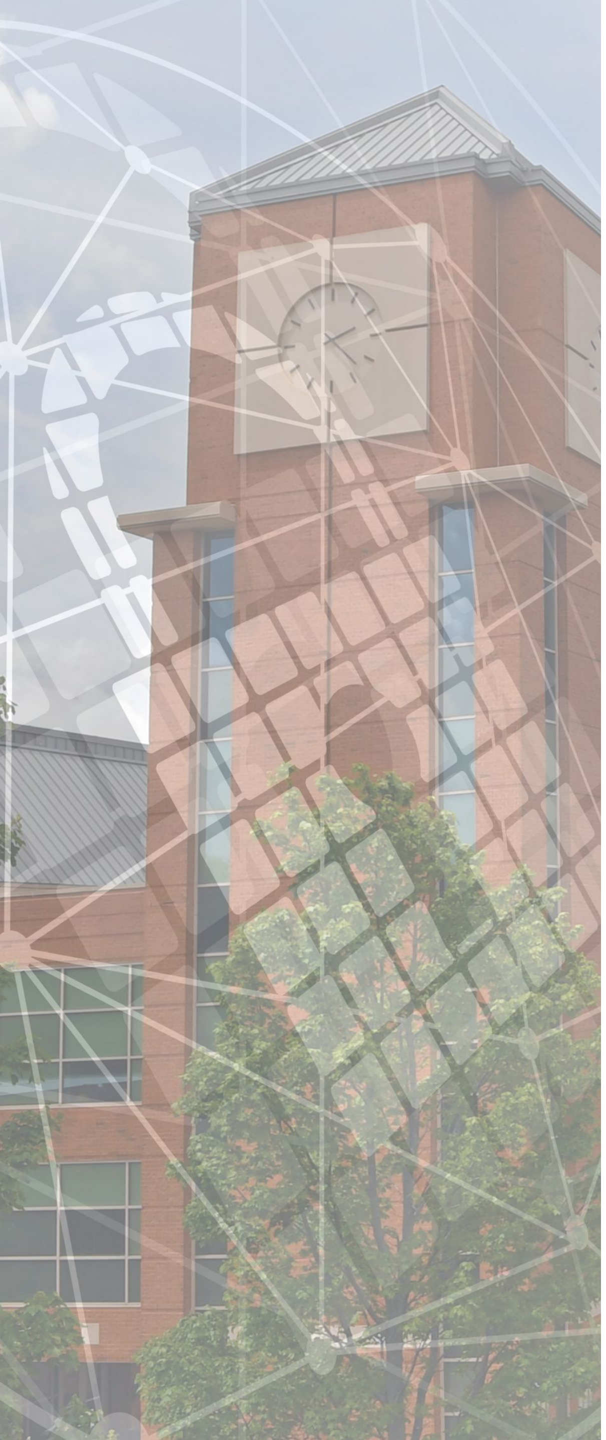


Insecure Home/Public Networks

- Average home in the US contains 11 or more connected devices
    - Smart devices are inherently insecure, may already be compromised
        - Example Mirai Botnet (October 2016)
- Most people lack technical expertise to secure home networks against attack
- Little to no remediation or detection capability
- Eavesdropping
- No network segmentation

- Mitigation Methods
    - Use the University VPN
    - Change smart device default passwords
    - Utilize modem/router built-in firewall

UNC CHARLOTTE
Office of OneIT

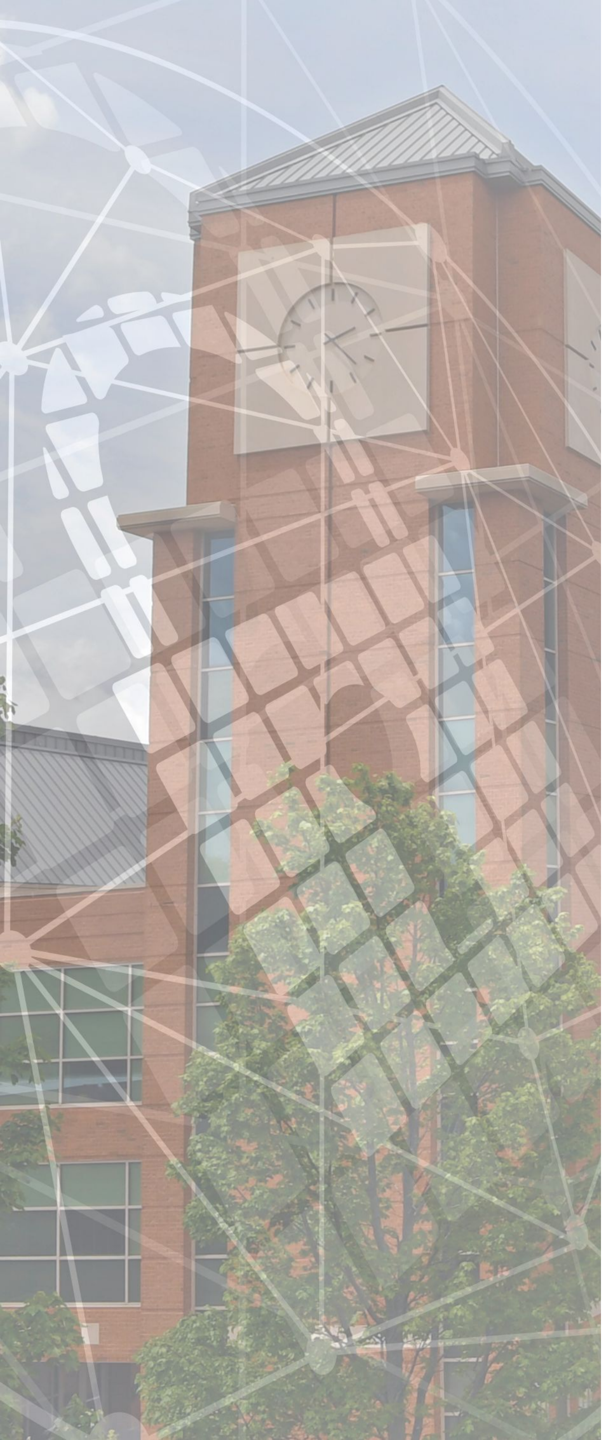


BYOD vs University-Managed Devices

- Employees often utilize personal devices to accomplish sensitive tasks
- University devices used for personal business

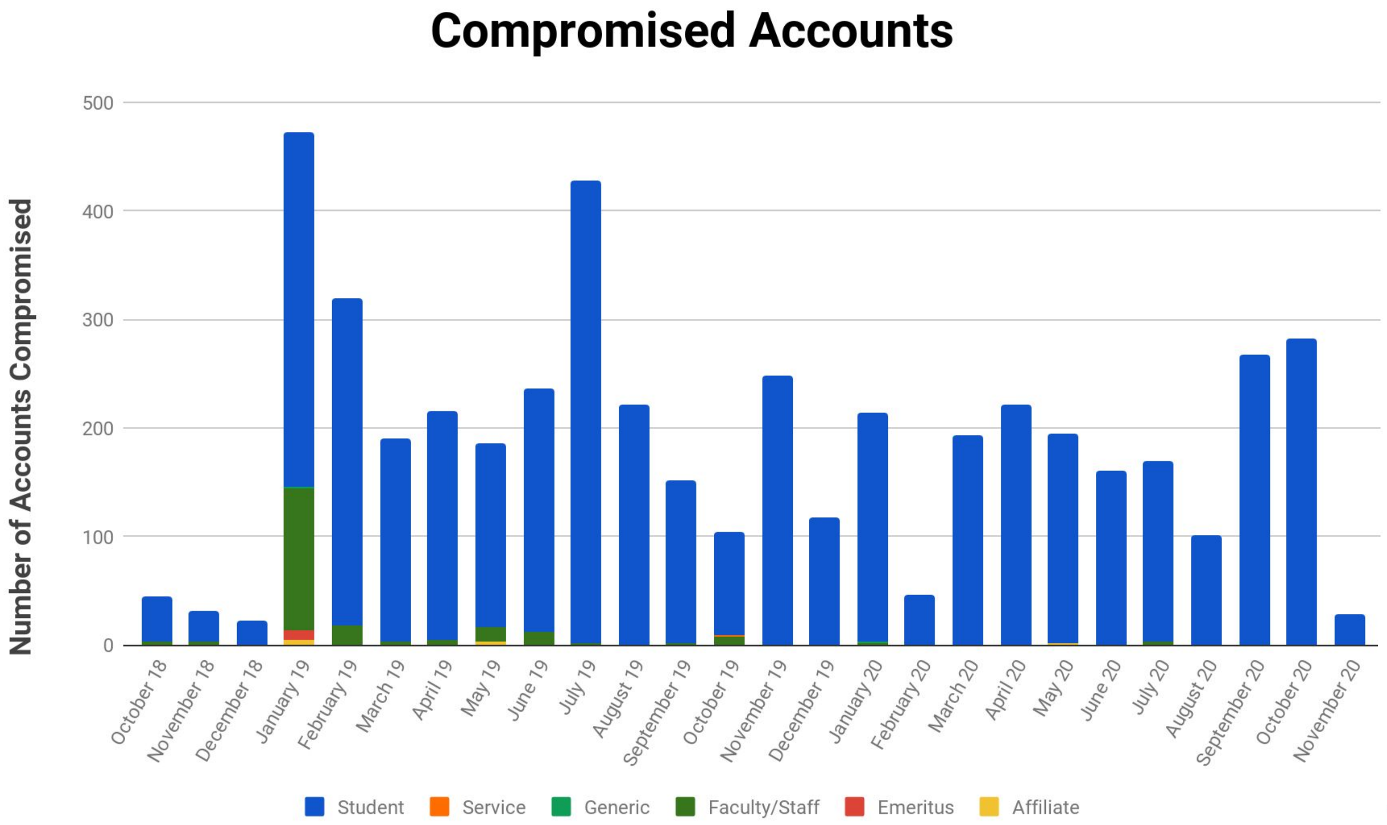
- Mitigation methods (for home)
  - Keep your digital life separate
  - Ensure you utilize up to date Anti-virus
  - Enable host-based firewall
  - Utilize DNS Security service such as OpenDNS
  - Utilize a password manager (average person has 50+ online accounts)
  - Use MFA anywhere possible
  - Keep system and applications patched to current levels
  - Utilize full disk Encryption (Bitlocker/FIleVault)
  - Enterprise Application Access (EAA)
  - VPN

UNC CHARLOTTE
Office of OneIT



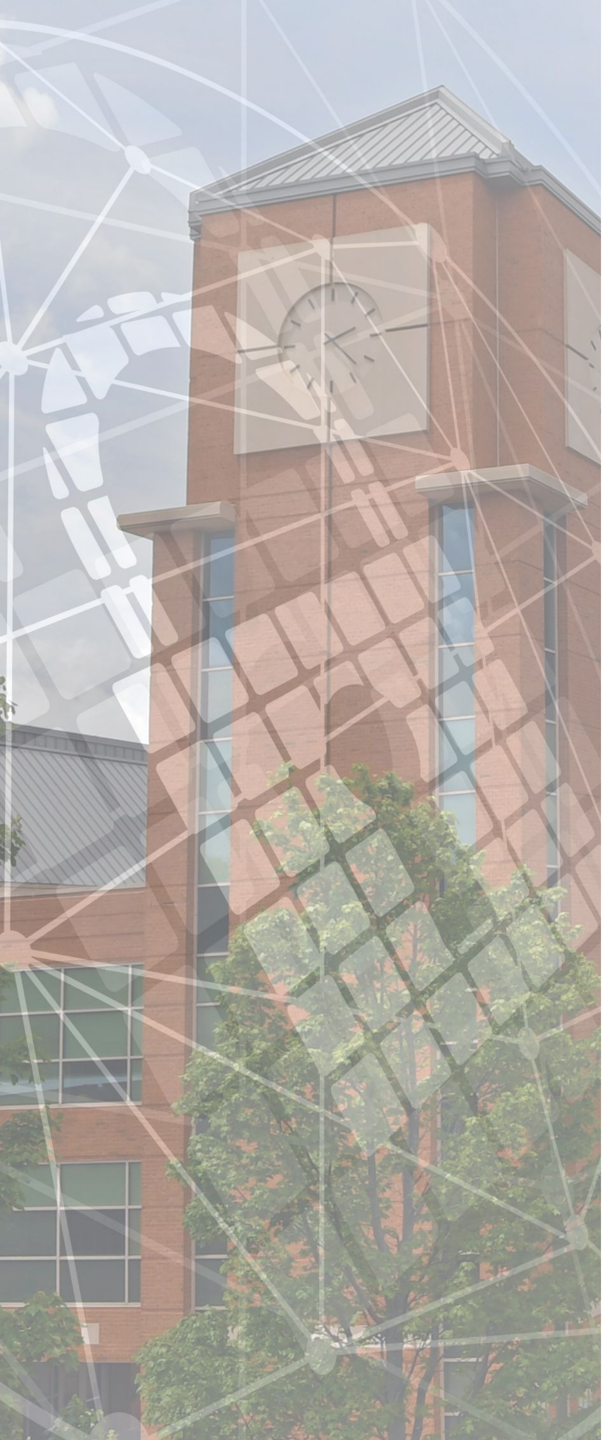
Account Compromise

- Multi-Factor is the best defense (Duo)
- OneIT detects and resets constant account compromise attempts



Compromised Accounts

UNC CHARLOTTE
Office of OneIT

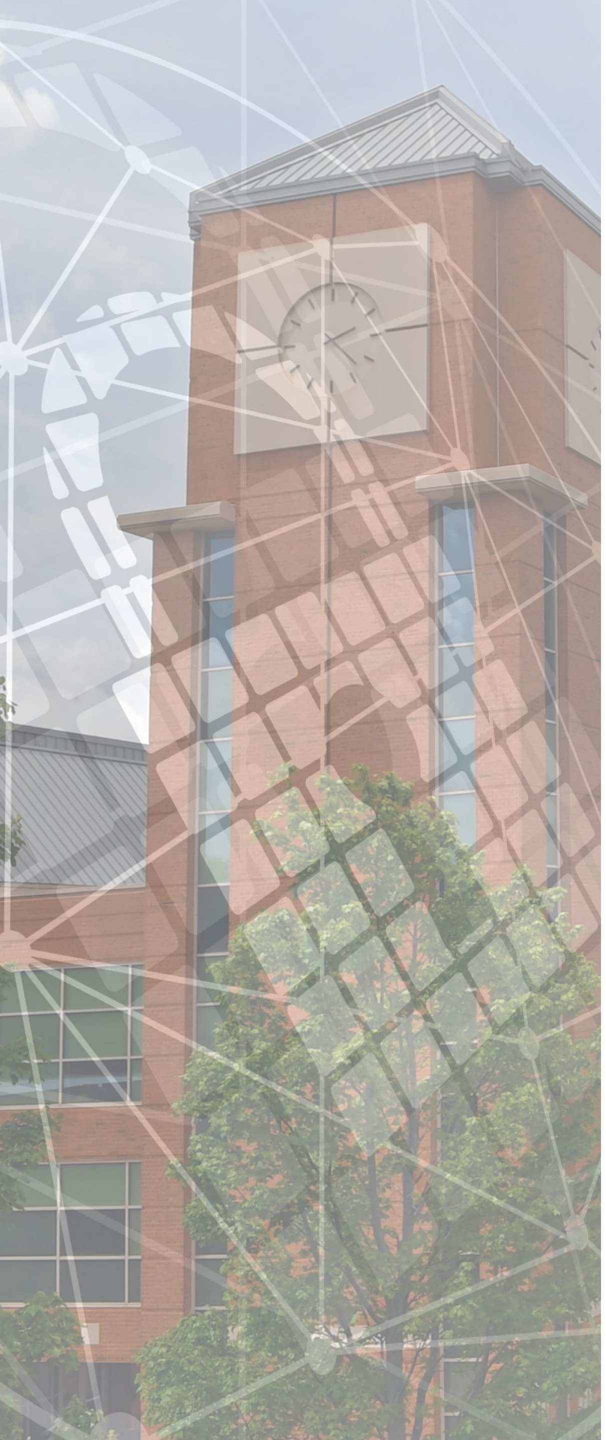


Social Engineering

- 80% of hacking attempts have a social aspect
- Social engineering is non technical attack type, but is often combined with technical attacks
- Remote workers have additional distractions = more susceptible
- Social attacks work best when there is a lack of established documented procedures

- Mitigation Methods
  - Security Awareness Training (SAT)
  - Establish written procedures for sensitive business tasks
  - Ensure employees are trained and held to policies and standards

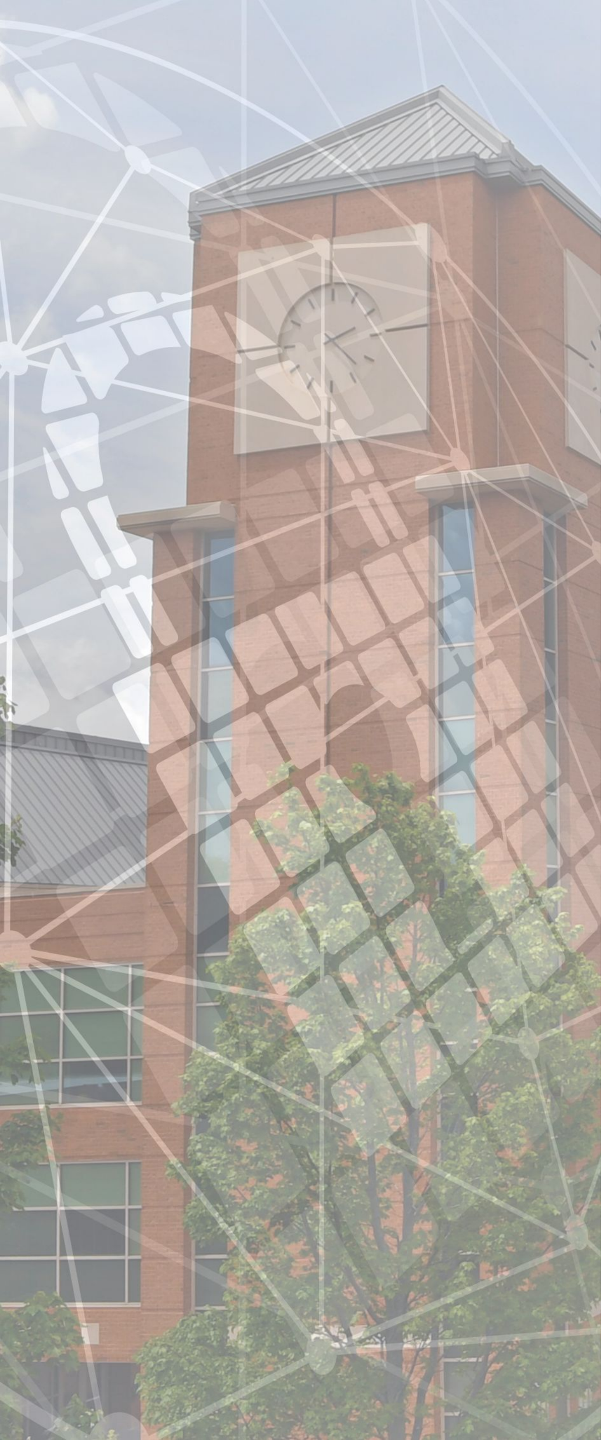
UNC CHARLOTTE
Office of OneIT



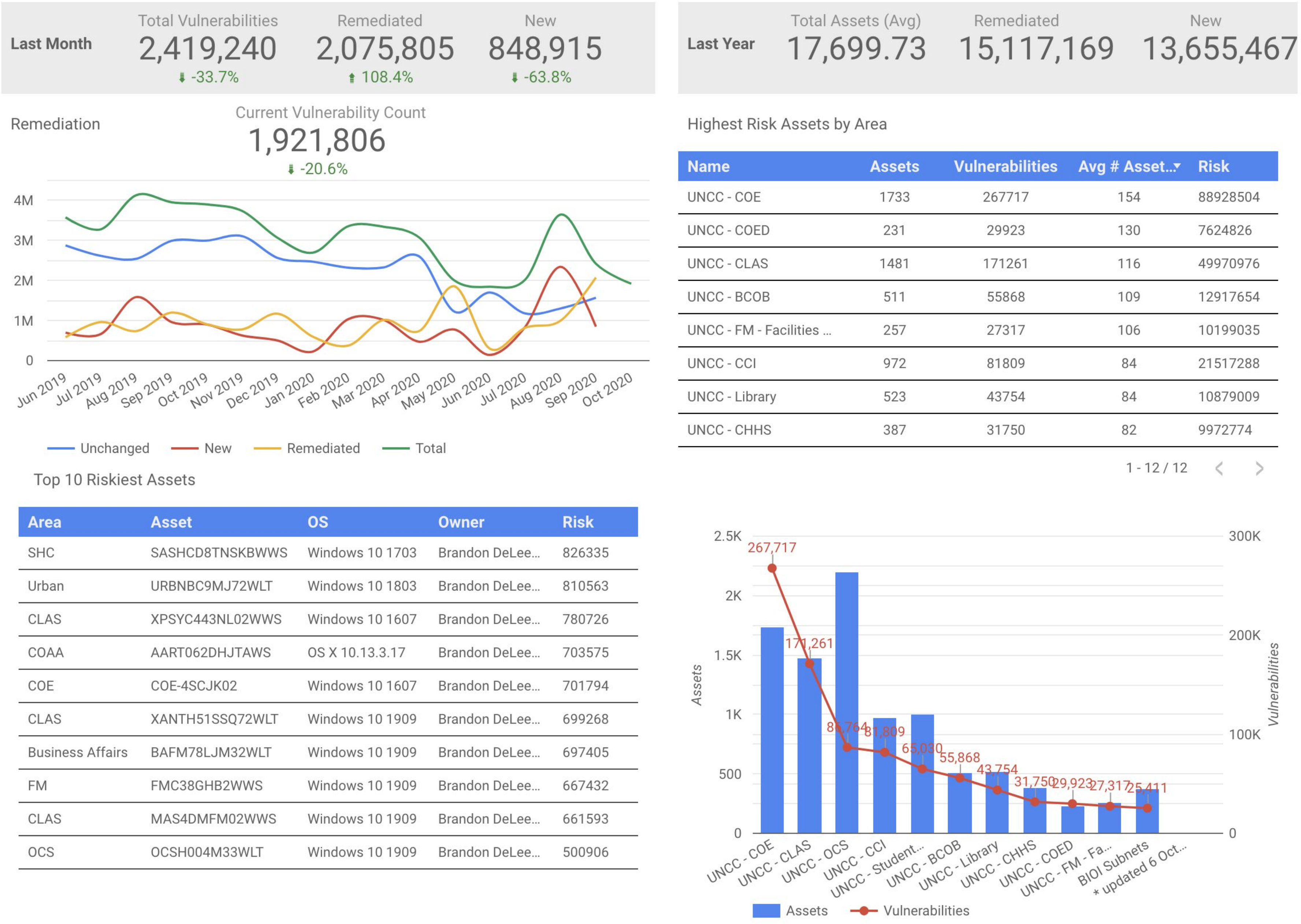
Phishing

- Phishing email is the No. 1 threat vector
- Over 50% of incoming emails are threats
- Remote work = distractions = more susceptible

- Mitigation Methods
  - Security Awareness Training (SAT)
  - Cisco Email Security (CES)
  - Umbrella DNS Protection
  - Phishing Training
  - Next Generation Anti-malware (AMP)



Vulnerability Management



Last Month	Total Vulnerabilities	Remediated	New
	2,419,240	2,075,805	848,915
	⬇ -33.7%	⬆ 108.4%	⬇ -63.8%

Last Year	Total Assets (Avg)	Remediated	New
	17,699.73	15,117,169	13,655,467

Remediation

Current Vulnerability Count

1,921,806

⬇ -20.6%

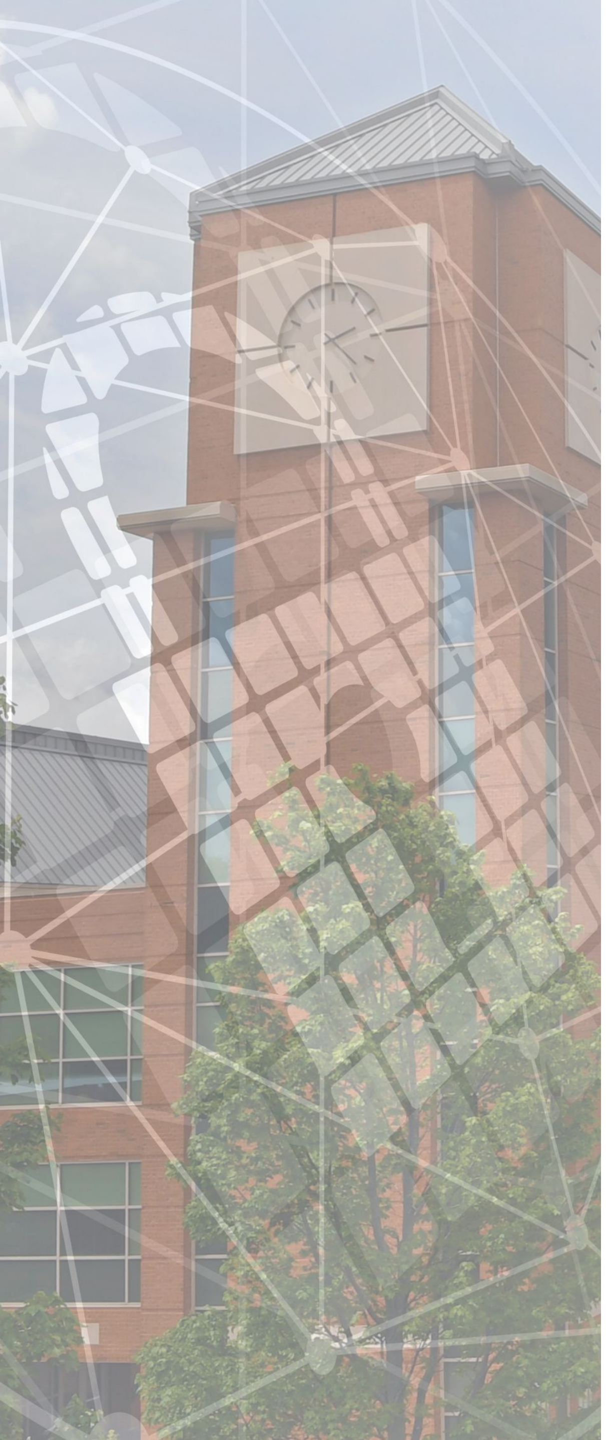
Top 10 Riskiest Assets

Area	Asset	OS	Owner	Risk
SHC	SASHCD8TNSKBWWS	Windows 10 1703	Brandon DeLee...	826335
Urban	URBNBC9MJ72WLT	Windows 10 1803	Brandon DeLee...	810563
CLAS	XPSYC443NL02WWS	Windows 10 1607	Brandon DeLee...	780726
COAA	AART062DHJTAWS	OS X 10.13.3.17	Brandon DeLee...	703575
COE	COE-4SCJK02	Windows 10 1607	Brandon DeLee...	701794
CLAS	XANTH51SSQ72WLT	Windows 10 1909	Brandon DeLee...	699268
Business Affairs	BAFM78LJM32WLT	Windows 10 1909	Brandon DeLee...	697405
FM	FMC38GHB2WWS	Windows 10 1909	Brandon DeLee...	667432
CLAS	MAS4DMFM02WWS	Windows 10 1909	Brandon DeLee...	661593
OCS	OCSH004M33WLT	Windows 10 1909	Brandon DeLee...	500906

Highest Risk Assets by Area

Name	Assets	Vulnerabilities	Avg # Asset...▾	Risk
UNCC - COE	1733	267717	154	88928504
UNCC - COED	231	29923	130	7624826
UNCC - CLAS	1481	171261	116	49970976
UNCC - BCOB	511	55868	109	12917654
UNCC - FM - Facilities ...	257	27317	106	10199035
UNCC - CCI	972	81809	84	21517288
UNCC - Library	523	43754	84	10879009
UNCC - CHHS	387	31750	82	9972774

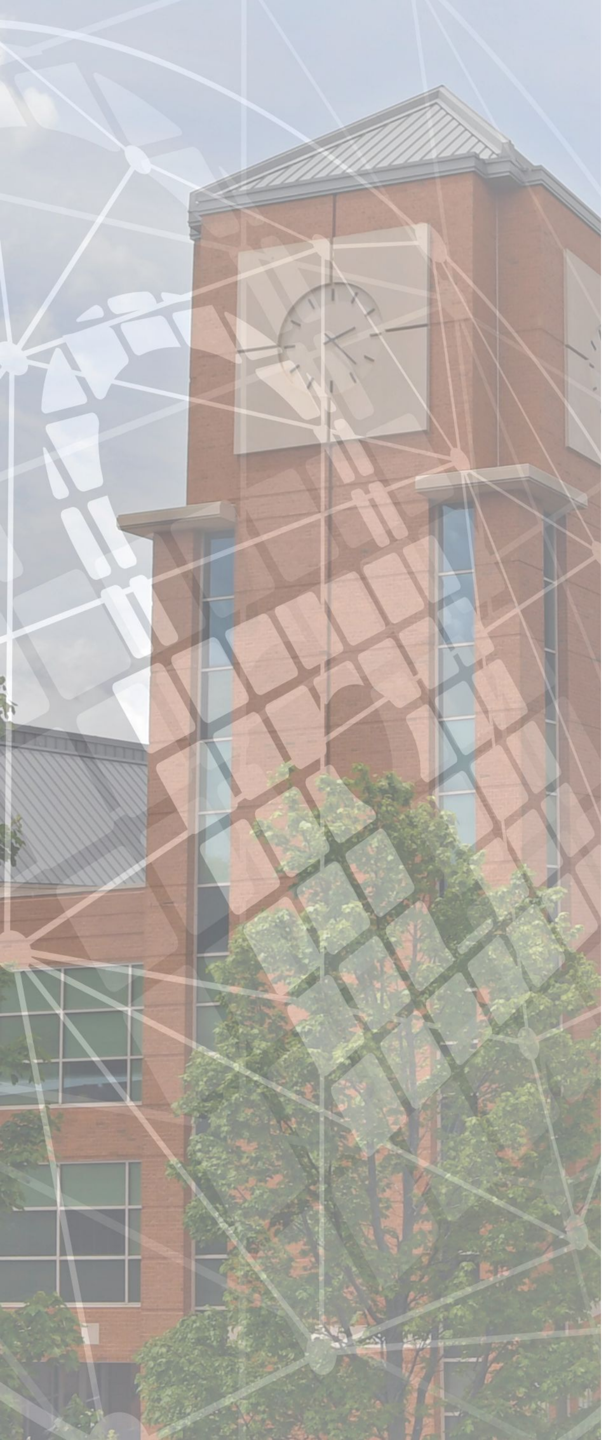
1 - 12 / 12 ‹ ›



Expanded Risk Vectors

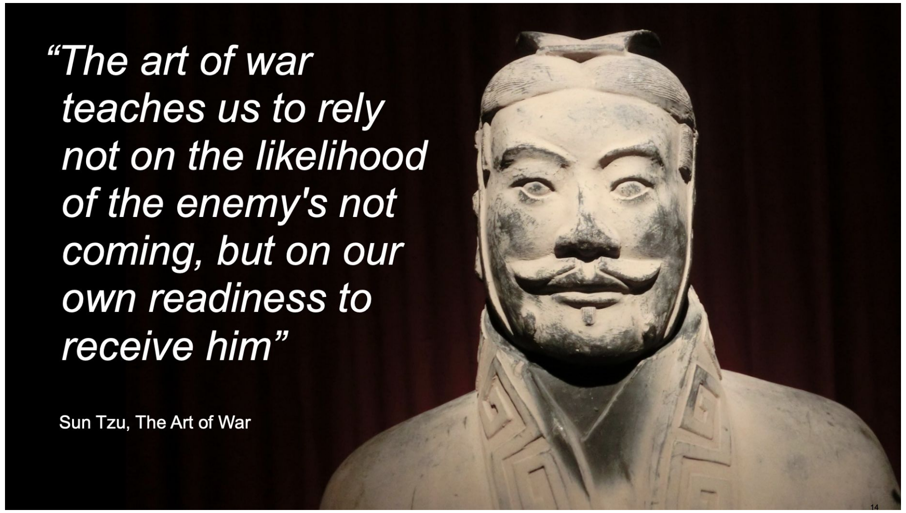
- Unauthorized remote access tools
- Lack of Data Loss Protection (DLP)
- Non-University Cloud Services
- Freeware
- Local Admin
- Security Awareness Training not required for all UNCC Staff/Faculty

UNC CHARLOTTE
Office of OneIT



Cyber Resilience

- Defense in Depth
- User training
- Zero-Trust architecture
- Continuous monitoring
- Incident Response tabletop exercises
- Identity based access control
- Cyclical Vulnerability Management
- Cybersecurity Insurance



“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him”

Sun Tzu, The Art of War

UNC CHARLOTTE
Office of OneIT

What makes us Cyber Resilient?

OneIT prepares for, responds to & recovers from cyber attacks when they occur at UNC Charlotte.

- We defend against cyber attacks with a Defense in Depth methodology
- We limit the effects of a security incident
- We guarantee the continuity of University operations during & after the attacks

UNC CHARLOTTE
Office of OneIT