Cybersecurity Incident

May 26, 2023

Northeastern State University

May

Thursday, May 25 – Story aired on Fox 23 of NSU Cancer Cluster

Friday, May 26 – (Friday before Memorial Day weekend) – intersession classes are in session.

- 4:30 am NSU notified by Federal Agency of suspicious activity on our Network - no notification from our paid vendors that monitor our network.
- Shortly after, NSU disconnected from the network
  - Phones, internet, printers, card swipe, cafeteria, admission, etc.
  - Website is still active – hosted off site (University Relations Managed)
  - Email, Blackboard and a few other 3rd party services was available from off campus or a hotspot through our website
  - Cabinet was notified of the outage and internet-based services – investigation into what/when/why. - Told service should be restored soon.
- Later that day, Campus and Public was notified of a Network Outage – via Website, email, social media and other media outlets
- Notice sent to RUSO and OSRHE as we recognized we were not able to return to normal operations

May

May 26 - 29 – IT worked through the holiday to determine the extent of the incident

- Became clear that the suspicious activity was the result of cyber criminals

Monday, May 29 – NSU website was destroyed by cyber criminals – 5,000+ webpages gone

- Suspected reasoning – to draw further attention to the breach
  - Eliminated access to email, Blackboard and other 3rd party internet-based services
  - You could still access email from off campus if you had not logged out of your device
  - All digital marketing efforts were suspended – we had no where to drive perspective students.
  - Notice to RUSO and OSRHE
  - Notice to Campus via social media, email and media outlets

"Good afternoon,

NSU is experiencing a network disruption that continues to impact our internet-based services, including phone lines and Blackboard. We continue to ask for your patience as technicians slowly bring services back online over the next several days."

May

May 30 – Daily updates from IT via Text

- False information attributed to IT
- University Relations will handle all communications
- Website rebuild in progress
- Grades and coursework being questioned by students

May 31 (day 7) – Suspected incident was aided by Phishing Scam and password access

- MFA and password strengthening plan is being developed
- Investigation continues into how to reconnect to the network safely
- Investigation continues into how to complete intersession and record grades
- *RUSO sends embargoed PR for new President announcement – to be released on June 1*

June

June 1 (day 8) – Website (single domain) restored – main page only

- Unable to edit website
  - Links to email restored
  - No internet access from campus
- *New President announced on via email, social media and media outlets*
- Campus notification
- M/L Drives are being questioned
- 3 copper phones lines were established for all of NSU

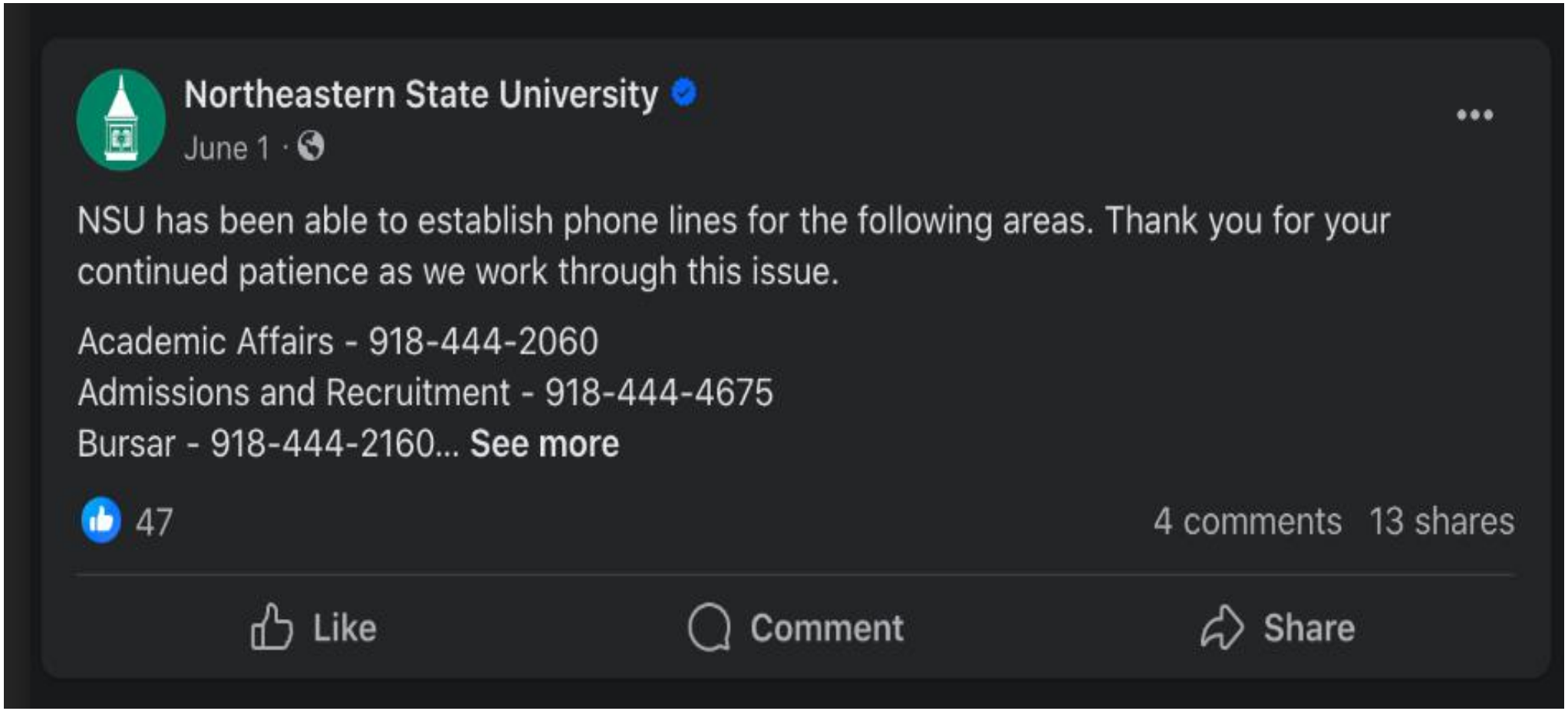
"NSU Camps Network Update

In the early hours on May 26, the IT team at NSU became aware of a cybersecurity incident that impacted our network. Out of an abundance of caution, the IT department disabled the network at 4:30 am on May 26 and began investigating the issue with the assistance of external consultants. At this time, our consultants have found no evidence that NSU data has been stolen.

As we move forward, the IT team is methodically working through our network to ensure we can safely reconnect enterprise systems and servers. Systems are coming online at an appropriate pace based upon established priorities. Internet connectivity will be reestablished by campus zones as early as today.

Please continue to be patient and understanding as we safely navigate this issue."

June


Northeastern State University
June 1 ·
NSU has been able to establish phone lines for the following areas. Thank you for your continued patience as we work through this issue.
Academic Affairs - 918-444-2060
Admissions and Recruitment - 918-444-4675
Bursar - 918-444-2160... See more
47
4 comments 13 shares
Like
Comment
Share

June

June 3 – IT notified Cabinet that over 230 servers have to be spun up and rebuilt for reconnection

- Assume that all communications are being read by the cyber criminals

June 4 – Notification sent to campus via social media and email regarding MFA requirement, connection to Blackboard via website, some services running and intersession and summer classes will resume as planned on June 5 (first day of summer session)

- Each computer on campus must be scanned before network connection established
- The below message was scheduled for 10 AM

Network Update - 6-04-23 @ 5:15 PM

"The NSU IT team continues to work long hours to repair services. In the meantime, please plan on face to face classes starting as normal Monday, June 5.

We are working on the final connections to Blackboard and will report the status of online classes later this evening.

Thank you to our IT department for the around the clock efforts during this network disruption.

We are very appreciative of all the kindness and understanding that has been shown by our students, faculty and staff as we work though this complicated issue."

June

Network Update - 6-04-23 @ 10 PM

“RiverHawk Family,

The IT department has been working tirelessly to reconnect our campuses and provide internet-based services to our students, faculty and staff. You can now access email and Blackboard from off-campus once you change your password.

Enhanced security features such as Multi-Factor Authentication (MFA) have been added. Many of you are likely already familiar with and use MFAs. Please note that when you log in, you will be required to establish a MFA and change your password.

To connect to email, set up your MFA and find instructions for changing your password, please use the link: http://www.nsuok.edu/MyNSU

You can connect to Blackboard at https://bb.nsuok.edu

These links are also available on the NSU website at http://www.nsuok.edu

All summer or intersession courses scheduled for Monday, June 5, are expected to meet as planned.

To change your password while on campus in Tahlequah or Muskogee, please go to the IT Service Desk in the Webb Tower, the library or the Admin Building on the Muskogee Campus. Once your password is changed, you will be able to log in as normal.

The Broken Arrow Campus network is still down.

While some of our services are now running, please know we are continuing to bring more services back online daily. We will continue to refine our services as we progress.”

June

June 5 (day 12) - First sign of Life

- IT underprepared for the response
- Lack of available staff at help desk
- MFA and Password reset instructions are not well-written
- Campus notification

"We apologize for the delay this morning.

The NSU IT department, working with external security consultants, has successfully connected many of our systems online. Progress with additional systems is being made hourly. However, like many things in life – the best results take time.

We continue to actively scan each computer, and our security vendors are monitoring our network to ensure we are maximizing the safety of our digital environment.

As we continue to reconnect systems to our network, we will likely discover files or drives that are no longer safely accessible. If so, we will err on the side of caution and seek to restore these files from a safe backup copy. For example, we know the data our enterprise system, Banner, is using is from a safe copy dated May 24, 2023.

We appreciate your patience as we address this issue as safely as possible."

June

June 6 - Some progress

- Website is being rebuilt domain by domain
- Most services still not connected
- Computers not connected to the network
- M/L Drives are feared to be lost forever
- All 2024 recruitment marketing materials were lost

June 8 (day 15) – Computer and phones connected to the network

- Admissions feed restored to Banner
- *NSU Budget Due*
- Notice from cyber criminals that they have stolen data

June

Friday, June 9 - Another Crises

- *Near drowning – 4 year old attending a summer camp*
- Notifications via email, social media and media outlets
- Police Department's good intentions

Monday, June 12 – Phones still down on 2/3 campuses

June 13 (day 20) – Dark Web Notice

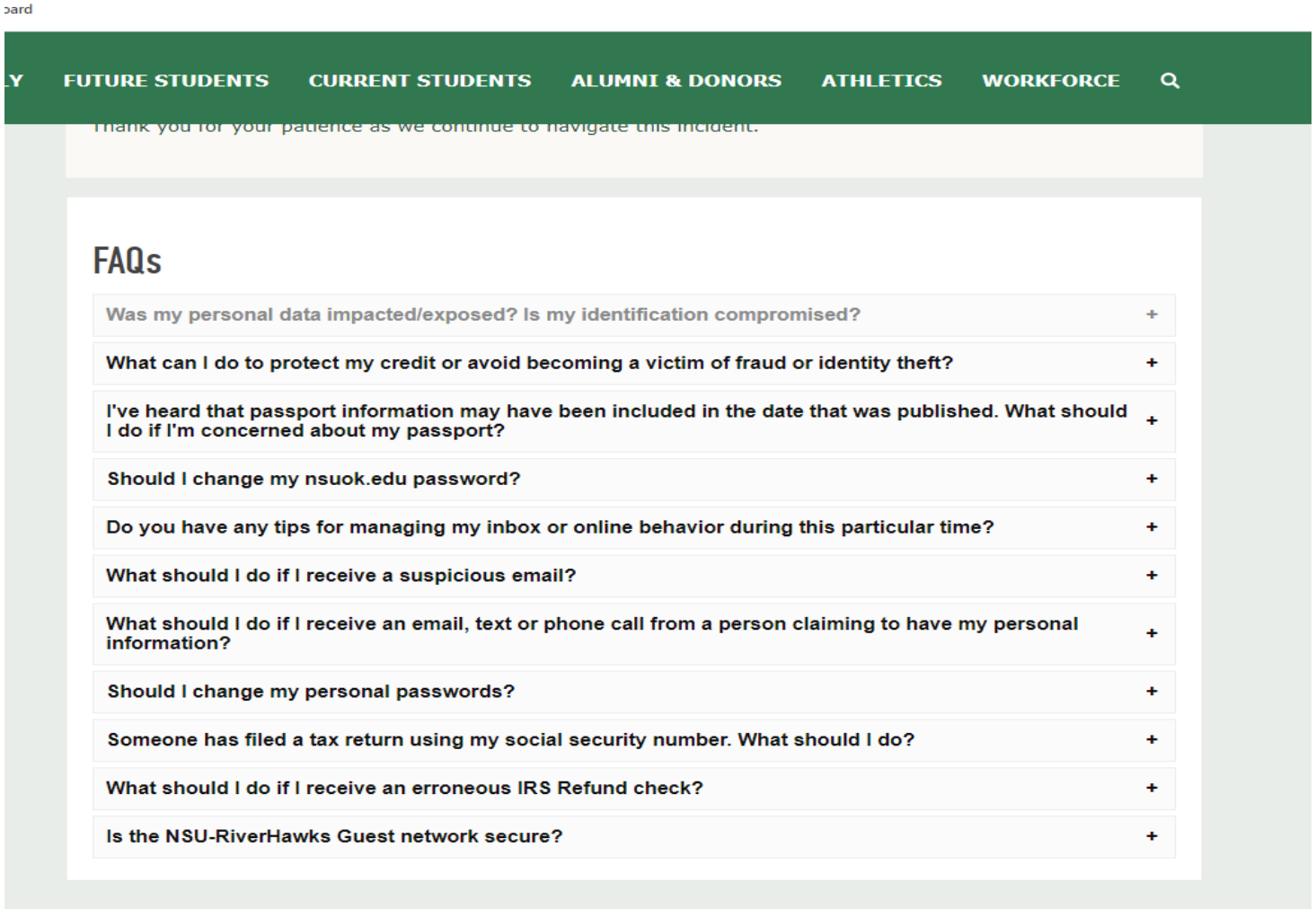
June 14 – Dark Web Confirmation

- Screen shot of information from the dark web
- Notice to RUSO

June

June 15 - Response to Data Breach

- Notice to campus community, patients, students, staff and vendors
- Dedicated webpage with FAQs
- Dedicated email address
- Credit monitoring services



June 15

RiverHawk Family,

As you are aware, in the early hours on May 26, the IT team at NSU became aware of a cybersecurity incident that impacted our network.

Unfortunately, our external security experts now have confirmation that some NSU data has been posted on the dark web. This includes images of personal identification data such as driver's licenses, passports, W-9 forms and social security numbers, as well as spreadsheets and letters.

NSU IT is working diligently with federal law enforcement and cyber experts to further assess the extent of the data compromised, as well as next steps for its retrieval.

We recommend the NSU community monitor their personal data and guard against any attempts of identity theft. In accordance with state and federal regulations, individuals will be notified should it be determined that their protected information was accessed during this cyber incident.

A list of frequently asked questions and important security resources is available below.

As a reminder, if you receive communications from persons claiming to have your personal information, or which are otherwise suspicious, please do not respond, and immediately report the incident to itsecurityresponse@nsuok.edu.

Thank you for your patience as we continue to navigate this incident.

June

June 16 – Media Story – Fox 23 CIO interview

June 21 - A Cherokee Nation fraud service found data on Dark Web

June 23 – Confirmation that 165 GB of 2 TB stored data in a drive left the campus network

June 27 – Students required to use MFA

June 29 – *Optometry Groundbreaking Event – Planned and executed by U.R.*

July

July 5 - *Fox 23 follow up for Cancer Cluster*

July 6 – M/L Drives

- A Copy is located from 2022 on an old device

Mid-July – M/L Drives restored

- Notice to campus and new location of storage

July 18-19 – New Branding Commercials were shot and produced on campus by University Relations

July 20 – *President Turner Retirement Event – Planned and executed by U.R.*

August

Aug. 1 – New President

Aug. 25 - Some people just woke from their summer slumber

- Resent campus credit monitoring notification
- Offered Free Services to 60,000+
- 115 took advantage

https://offices.nsuok.edu/businessfinance/Departments/cyber_security_incident_2023.aspx

Aug. 31 – Student Newspaper Interview

- Print edition for Homecoming
- Front Page “Cyber security attack stuns campus community”

Thank You!

NORTHEASTERN
STATE UNIVERSITY