



State Capitol – 600 E Boulevard Ave – Dept. 215
 Bismarck ND 58505-0230
 Phone: 701.328.2960 Fax: 701.328.2961
 E-mail: ndus.office@ndus.edu Web: ndus.edu

BUDGET SECTION September 24, 2014

10:05 am - Presentation by a representative of the North Dakota University System regarding a recent spear-phishing email attack and subsequent unauthorized access to personal information at North Dakota State University

Testimony prepared by Lisa Feldner, NDUS CIO

On August 12-14, 2014, approximately 140 spoofed emails were sent to recipients at NDSU. The emails looked as if they were coming from the NDSU Human Resources department and asked that employees click a link to confirm their salary revision documents or similar language.

The link in the email actually pointed to a website in Russia that looked like an NDSU website where the users were asked for their username and password. Unfortunately, 8 individuals clicked on the link and purportedly entered their usernames and passwords.

On August 28, 2014, before I learned about the NDSU incident, I sent out a systemwide email warning users of potential phishing scams that tend to occur at the beginning of the school year. In fact, I sent a similar one last year. One NDSU individual who had clicked on the link then checked her account in ConnectND and found that it had been changed. She contacted the NDSU payroll office and they stopped the electronic payment. However, the electronic deposits of the other 7 individuals were rerouted to banks on the east coast where the funds were subsequently withdrawn. NDSU alerted law enforcement and covered the cost of the lost wages - a little over \$28,600.

Core Technology Services was alerted on September 2 of the compromised accounts. We immediately disabled ConnectND employee direct deposit self service and notified ITD and OMB who did the same on the State side. All ConnectND accounts were analyzed for suspicious changes in direct deposit but none were found. Working collaboratively, CTS and ITD continued to perform scans on ConnectND, email, and the network until the teams were satisfied nothing had been compromised. Both OMB and CTS sent out an email to all employees alerting them to phishing scams and asking them to check their direct deposit information.

To date, no other campus received the emails and no state agency received the emails.

At my request, ITD has installed the intrusion detection/threat prevention devices in the NE and NW quadrants of the network with the SE quadrant scheduled for this coming weekend and the SW quadrant for November. These devices would not have blocked these emails from coming in but they would likely have blocked the traffic from leaving the state after the user clicked on the fake link because it came from a known range of criminal sites.

This was a targeted phishing attack, referred to as spear phishing, where they target a defined group of users instead of a broadcast a massive amount of email. Most email systems are designed to detect and block mass phishing attempts.

NDSU's migration to their own email tenant occurred on July 21, 2014. At this time, we don't know if this migration is related to the phishing scam.