PHISHING 2017

Louisiana State University

The Phishing Landscape

- Globally, the rate of phishing increased 250% in Q1 2016, and is still rising (source: SC Media)
- Why is LSU being targeted?
- Who is doing this?
- What are they after?
  - *W-2's, to change direct deposit information, spawn more phish internally, intellectual property, personally identifying information for identity theft*
  - *Alternatively, they want to install Ransomware and extort money*

The Phishing Landscape

- Have University systems been hacked?
- Why can't the University block phishing emails?
- The "Problem"
  - *Email is an inherently trusted form of communication*
  - *And, …. it is a severely misplaced trust*

Compromise of Credentials (Logon/Password)

- How does it happen?
  - *Phishing emails - that scare or coax you into providing information*
  - *Malware on computers, mobile devices*
  - *Logging on to University systems from questionable computers, devices, or networks*

What is the University doing?

- Blocking malicious links contained in Phishing emails from campus
  - *This does not protect you at home or off campus*
- Scanning change logs for suspicious changes to employee information
  - *Timing is part of the attack profile for hackers. They are trying to time their attacks with University processes*
- Email filtering
- Working towards the implementation of two factor authentication to access University systems
  - *Two factor: Something you know; something you have; something you are*
- Working to implement annual security awareness training for employees
- Looking at “self-phishing” strategies tied to awareness education
- Deploying a new “Phish Tank” Web page to inform the community on phish that have been discovered or reported
  - *www.lsu.edu/phishing*

What can we individually do about it?

- Be paranoid of anything that talks about money, asks for personal information, or contains a Web link
  - *Cursor over Web links and read them in their entirety. If something smells rotten, it probably is……*
  - *Log in to computer systems directly rather than clicking on a link in an email.*
  - *Don't be in a hurry to click on attachments, especially something you didn't ask for, or not expecting to receive*

- Jealously guard your personal information
  - *Be as protective of your personal information such as SSN, date of birth, drivers license number as you would your purse or wallet*
  - *Think twice, and a third and fourth time before entering personal information into online forms*

What can we individually do about it?

- Watch for misspellings and other formatting errors
  - *The problem is that the quality of phish has increased along with the quantity*

- Again, cursor over Web links. If something doesn't feel quite right with an email, DO NOTHING
  - *Get help from your department's IT staff or contact the ITS Help Desk*
  - *If you have suspicions about an email, ask another person to look at it with you.*

- Report Phishing messages to security@lsu.edu

The End

- Questions / Discussion