# AUBURN INFORMATION TECHNOLOGY

# Cyber Security Risks & Strategies

AUBURN UNIVERSITY

# CYBER SECURITY RISKS TO AUBURN

- **Threat statistics:**
  - **Processed 231M emails August 1-31**
  - **92.2% of email in August contained some form of malware/SPAM**
  - **350 viruses blocked at the border**
  - **120 compromised accounts just in Aug.**
    - **Projecting 500+ in 2017 (currently @ 341)**
    - **241 incidents in all of 2016**
    - **115 incidents in all of 2015**
  - **Credit card fraud will cost Americans $16B in 2017 (per CNBC)**

- **Equifax breach – unpatched web server**

# SOLUTIONS TO THESE RISKS

- **2-Factors (2FA) Security Roll-out**
- **Clean-up Old Data**
- **Continue scanning and threat monitoring**
- **Implemented automated patching tools for IT staff**
- **Education and Awareness Campaigns – Phishing, Equifax**

**Auburn Cyber Security Center**

# MORE INFORMATION

- June 27 – [To: Ditmc] Training Message – Compromised Credentials
- June 30 – [To: IT Providers] 2-Factor (Duo) Registration Lists & Support Docs
- August 11 – [To: IT Providers] List of users not Duo registered
- August 25 –[To: Campus Leadership] Data Clean-up Project
- August 15 – [To: Provost Fall Leadership Team] General Security Update
- August 21 – [To: Students] – Phishing Information
- Sept 13 – [To: IT Providers] Sending messages about Duo enrollment
- Sept 13 – [To: IT Providers] Upgrades (includes “2-Factor Authentication”)
- Sept 13 – [To: (Targeted) Employees not registered] Duo Security enrollment
- Sept 13 – [Auburn News] DUO security/2-Factor authentication expanding
- Sept 13 – [Auburn News Article] Equifax Data Breach Information
- Sept 13 – [To: Campus] OIT homepage – Cyber Security Central Link