On December 5th, an email went out to the Emory Community concerning some recent cases of Emory employees providing their Network ID and Password in response to “phishing” emails. The emails appear to come from an official Emory source or colleague. The information was used to access the employee’s Self Service record in PeopleSoft HR where their Direct Deposit information was changed. To help secure employee data, changes have been implemented to mask sensitive data in PeopleSoft Employee Self Service.

- Data to be masked includes:
  - Social Security Numbers (SSN) of employees and their Dependents and Beneficiaries. Only the last 4 digits will remain visible.
  - The Birth Year for Employees and their Dependents and Beneficiaries.
  - Direct Deposit Account Numbers and Routing Numbers will be masked down to two digits.

- In addition, employees will have to respond to a security question before they can Add, Edit or Delete accounts from their Direct Deposit record. For existing records, the security question will ask that you provide one of the account numbers in your current banking record information. For new employees, the employee will have to provide the first five digits of their SSN. An employee who does not yet have an SSN will need to submit their direct deposit change to the Payroll Office because the system will not recognize them.

- Employees will have three attempts to enter the correct data. After three failed attempts, the system will log the employee off. The employee may return later to try again.