PCI & E-COMMERCE

Presenters:
Robin Owens
Dee Bowling

WHAT IS PCI & WHAT DOES IT HAVE TO DO WITH ME?

- PCI - Payment Card Industry
- Set of policies and standards created to ensure the security of payment card data
- If your department accepts any form of payment card (Visa, MasterCard, etc.) you must be PCI compliant to maintain your merchant status

WHY IS PCI IMPORTANT?

- If you experience a breach, potential liabilities include:
  - Fines up to $500,000 per card brand
  - All fraud losses incurred
  - Cost of re-issuing cards
  - Consumer fraud monitoring
WHAT SHOULD I DO?

Secure your network
- Computers, POS terminals, etc. connected to campus network should be behind a firewall
  - POS terminals connected via a phone line are secure
- Laptops and any other wireless devices (iPad, iPhone, etc.) should not be used to collect payment card info (wireless network is not secure)
  - Laptops can be used if they are connected via ethernet cord to the campus network but they must also be behind the firewall

WHAT SHOULD I DO?

Passwords
- Never use default passwords from a vendor
- Require a unique log in for each user
- Maintain a list of all users with access
  - Be sure to remove users when their access is no longer required, they are terminated, etc.
- Require password changes at least every 60-90 days
- Review user logs

WHAT SHOULD I DO?

Protect Cardholder Data
- Only keep info as long as it is needed for business purposes, then safely destroy (cross cut shredder)
- Never store card holder data electronically (PAN, exp date, PIN, Mag stripe data, CVV code, etc.)
- PAN (Primary account number) must be masked on all receipts/printouts
  - All POS terminals on campus should have the PAN masked so that you can only view the first and last four digits
  - Any third party systems should be setup this way as well

WHAT SHOULD I DO?
WHAT SHOULD I DO?

- Protect Cardholder Data (cont.)
  - Lock up and restrict access to any hard copies of card holder data
  - Log and monitor all access
  - Fax machines which are used to collect credit card info (highly discouraged) should be in a private area where access is restricted
  - Request customers not to email card information
  - Mail that could include credit card info (checks or cash) should be opened and secured immediately

WHAT IF I THINK I HAVE A BREACH?

- Report any possibly breaches or problems regarding cardholder data to the E-Commerce Manager immediately

WHAT ELSE SHOULD I KNOW?

- If your department wants to purchase new software or make changes/upgrades to your existing software (software that processes payment cards) you MUST contact the Ecommerce Manager
  - All software purchases/upgrades must be approved by Financial Services as well as ITCS
- Any new software purchases are highly encouraged to be with companies who are Touchnet Ready Partners
  - http://www.touchnet.com/web/display/TN/Ready+Partner+Program
WHAT ELSE SHOULD I KNOW?

- POS (Credit card) terminals
  - Contact the E-Commerce Manager if...
    - You need additional POS terminals
    - You need to destroy/replace a POS terminal
    - You want to start accepting payment cards and need a POS terminal(s)

- Touchnet
  - Software purchased by ECU and currently in use which has the capability for departments to have an online presence and accept payment cards
  - Stores are currently being used to:
    - Sell products
    - Workshop registration
    - Conference registration
    - Camp registration
    - Test Prep course registration
    - Audition/Membership Fees
    
  [https://epay.banner.ecu.edu/420644_ustores/web/index.jsp](https://epay.banner.ecu.edu/420644_ustores/web/index.jsp)

CONTACT INFO

- [ecommerce@ecu.edu](mailto:ecommerce@ecu.edu)