University of Houston DOWNTOWN

Office of the President
Dr. Juan Sánchez Muñoz

October 9, 2017

Dear UHD Community:

October is National Cyber Security Awareness Month and it is important to understand our responsibility to make sure UHD data is kept safe and secure. Phishing via email is among the most prevalent type of cyber-attack. This is why UHD employees must take special care when handling sensitive data.

Below are among the best practices when handling the sensitive data:

- Avoid copying or downloading sensitive data from University administrative systems to your desktop computer, laptop, USB drive, etc., unless absolutely required.
- Use Spirion software (formerly known as Identity Finder) to find and protect sensitive data on University PCs.

If downloading:

- Remove the confidential part of the information from the data if possible (e.g., Social Security numbers, etc.).
- Store the data in a secure manner by using encryption— contact UHD IT Security personnel to find out more about using encryption.
- Physically protect devices that can be easily moved such as USB drives or laptops.
- Do not send unencrypted sensitive data via email. Email messages can be intercepted by third parties or inadvertently forwarded.
- Never store unencrypted sensitive data on a portable device.
- Protect printed sensitive data in a locked desk, drawer, or cabinet.
- Shred sensitive data that needs to be discarded.
- Do not leave data storing devices in cars, lockers, purses or other unattended places.

These simple tips can help ensure the integrity and confidentiality of university data. For more information on the UHD Information Security Program, please visit https://www.uhd.edu/infosec or contact UHD IT Security at security@uhd.edu.

Sincerely,

Dr. Juan Sánchez Muñoz, UHD President