

Monthly InfoSec Newsletter

October 2020



Current trending attacks

Phishing attempt- The “waiting package” text attack (image 1) has been targeting college students recently by sending text messages asking them to claim a package. A link is included for the recipient to click on containing malware. If you encounter a similar text do not click on the link, instead contact the company using their legit website or number.

Ransomware- Universities have been the target of much more than normal amount of ransomware attacks. These attacks are normally preceded by phishing attempts like the one above, so watch out for any suspicious emails or texts containing links.

One way IT and BFS are working to protect CSUP

The Payment Card Industry Data Security Standard or PCI DSS (image 2) are a set of data security standards developed by major credit card companies like Visa or Mastercard. These standards are set to ensure merchants who process credit cards are transferring that data in a secure manner and are following the best practices. CSU Pueblo is working hard to ensure all departments are in full compliance to the standards.

Being compliant with PCI DSS standards is important because major the credit card companies can prohibit our campus from using their brands if we're not compliant.

Feedback

Thank you for reading our first monthly newsletter! We would love to hear some feedback from you, whether it's things you would like us to include or some criticisms you have. Please feel free to email us at infosec@csupueblo.edu and we hope you will continue to read our monthly newsletters!

Trending news

- “Waiting package” text targeting students
- Universities have been facing significantly higher ransomware attacks
- PCI DSS compliance is falling worldwide, but CSUP is working hard to maintain compliance

“On average only 27.9% of global organizations maintained full compliance with the PCI DSS, a drop of over 27% since compliance peaked in 2016.”

1

THOMAS, WE STILL HAVE A PACKAGE WAITING FOR YOU FROM MAY 15 2020, TO CLAIM PLEASE CLAIM BY CONTACTING US AT malware.com

2

