Cybersecurity Awareness Month: Proper credit card data usage and storage on campus — PCI Compliance

Anyone at CWRU who accepts payment for goods, services or events should be aware of safe credit card transaction practices, also known as PCI (Payment Card Industry) compliance. Payment Account Number (PAN) or Credit Card Number (CCN) data is considered Restricted Data, requiring the most stringent controls to maintain confidentiality.

Authorized Payment Processes - Only those payment processes approved by the Office of the Treasurer are authorized. Contact treasurer@case.edu to initiate a request for approval.

Transaction Devices - Most people rely on credit card point-of-purchase terminals like the Square or Verifone card swipe readers, which encrypt the card data both at rest and in transit when the transaction processes, and keep it from spreading to the user's local workstation or the campus network.

Over the Phone - Some approved phone collection processes involve entering the CCN from a phone conversation directly into the payment portal, or using the card terminal equipment. Never write down the numbers for later key entry or store them in an online file.

In-person - Face-to-face transactions should use a point-of-sale device that encrypts the CCN both at rest and in transmission to the payment clearinghouse.

Online - Websites handling credit card transactions should not record or store the credit card data. Confirm with the software developer that credit card data is not stored after the transaction is completed.

On Computers/In Emails - CCNs should never be stored in plain text on the user's workstation or laptop, and should never be transmitted via email.

Past Transactions - Those who have conducted transactions via email should obtain the Spirion application from the [U]Tech Software Center. Use Spirion to scan both hard drive and email to cleanly remove any confidential data such as CCNs or Social Security Numbers that may be stored "in the clear" on a workstation.

Visit the Information Security Office at: **securityaware.case.edu**

UNIVERSITY TECHNOLOGY
CASE WESTERN RESERVE
UNIVERSITY

[U]Tech Service Desk | help@case.edu | 216.368.HELP (4357) | help.case.edu