Published on *University of Colorado* (https://www.cu.edu)

your campus

Feature Articles

Stay Cybersecure While Traveling: Avoid Public USB Charging Risks

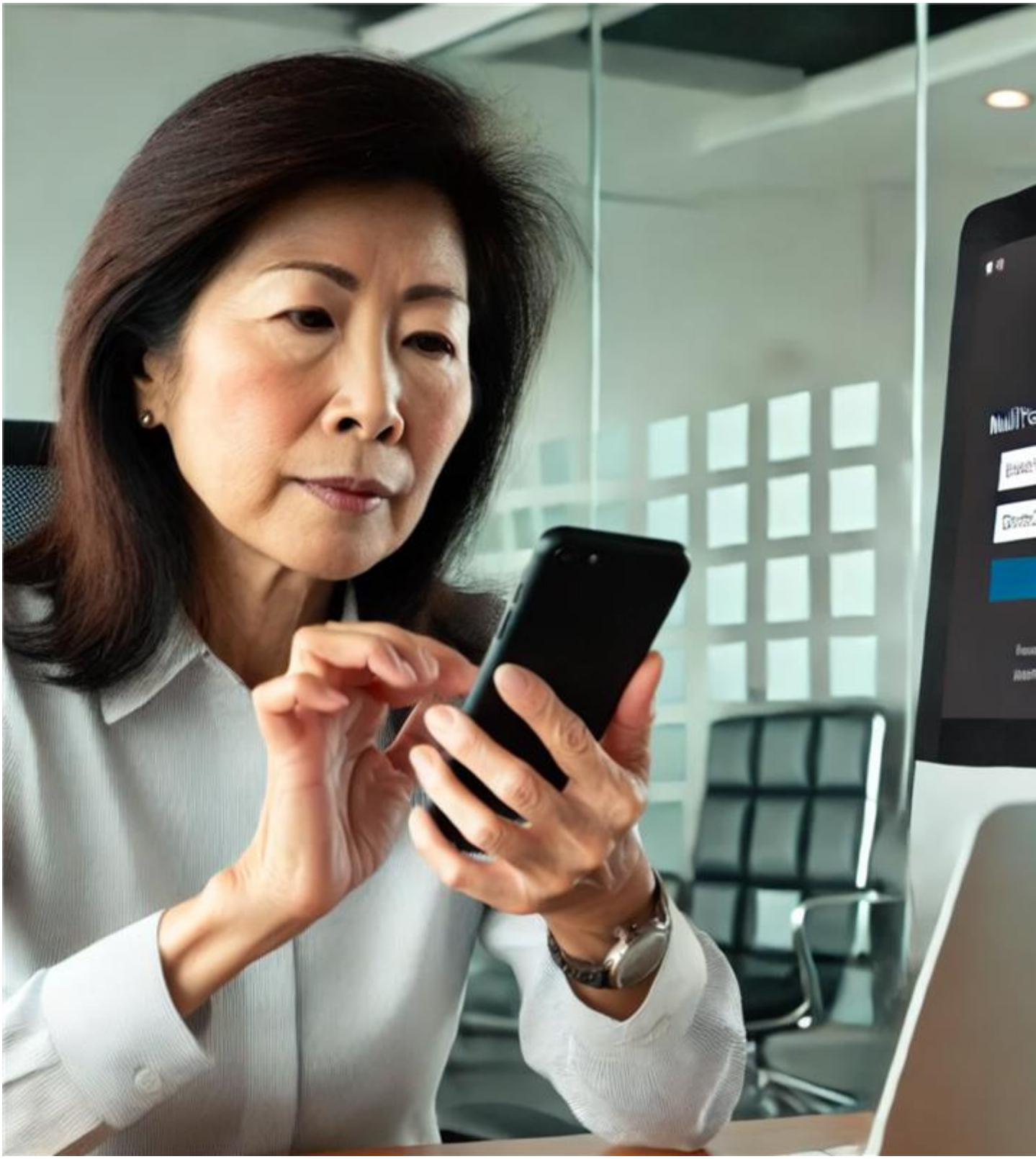
Both the FBI and TSA have issued warnings against plugging phones or devices directly into public USB charging ports, especially in airports. Cybercriminals can exploit these seemingly convenient charging stations to access your device while it charges. Learn more [1].

Are Your Taking These 10 Steps to Keep Data Safe?

Adopt these simple yet crucial steps to keep our confidential data safe. Read More [5] [6]

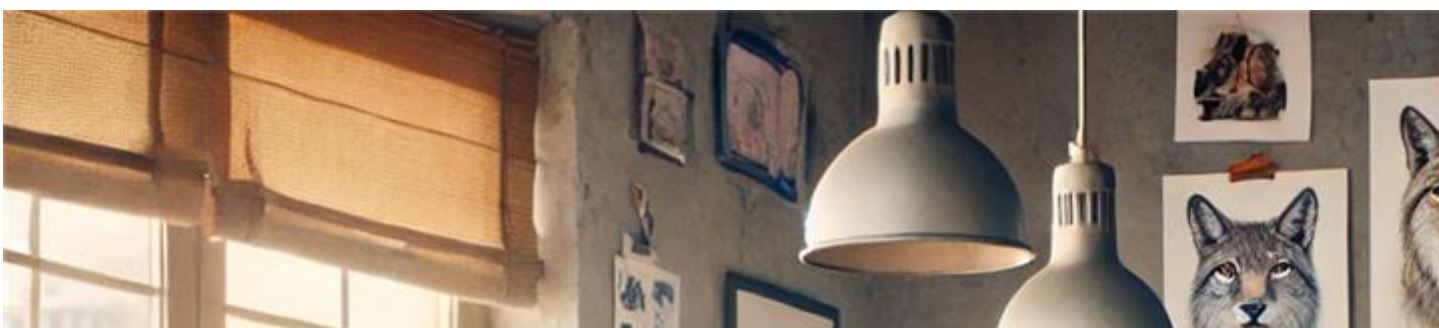
Can Your Passwords Withstand Cybercrime?

Strong and secure passwords are essential for protecting personal and sensitive university data. Read More [7]



MFA: Added Protection from Cybercrime

MFA is a crucial security feature designed to verify your identity before granting access to accounts. Read More [8]



Using AI at CU

Explore your campus resources when using artificial intelligence. Read more [9]


****
***
login

Avoid Being a Phishing Scam Victim

Before clicking any links or downloading attachments, assess the email's legitimacy. Read more [10]

Keep Your Family Secure Online

Kids are especially vulnerable to cybercrime. Teach them good security behaviors. Read more [11]

Top Policies and Standards

Custom text

Top Policies, Standards, Guidelines to Know

IT Security Program [12]
Serves as the core for the university's information security activities and provides general guidance.

Systemwide Security Baseline Standards [13]
Provides guidelines for selecting and specifying security controls for organizations and information systems.

Data Classification [14]
Provides guidelines for classifying university information and helps determine minimum security requirements necessary to keep it safe.

Collection of Personal Data from Students and Customers [15]

Source URL:https://www.cu.edu/department/184268/university-colorado-process-data-classification-and-system-security-categorization

Provides requirements for the collection of personal data from students and other customers of the university, and for detecting warning signs associated with identity theft.

Links

[1] https://www.cu.edu/security/stay-cybersecure-while-traveling-avoid-public-usb-charging-risks [2] https://www.cu.edu/security/information-security-course-compliance-faqs [3] https://www.cu.edu/security/reporting-incident [4] https://www.cu.edu/security/about [5] https://www.cu.edu/security/are-you-taking-these-10-steps-keep-data-safe [6] https://www.cu.edu/security/top-three-social-media-scams [7] https://www.cu.edu/security/can-your-passwords-withstand-cybercrime [8] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime [9] https://www.cu.edu/security/explore-resources-using-artificial-intelligence-cu [10] https://www.cu.edu/security/avoid-being-phishing-scam-victim [11] https://www.cu.edu/security/keep-family-secure-online [12] https://www.cu.edu/ope/aps/6005 [13] https://www.cu.edu/security/systemwide-baseline-security-standards [14] https://www.cu.edu/data-governance/resources-support/data-classification [15] https://www.cu.edu/ope/aps/7003 [16] https://www.cu.edu/ope/aps/2006 [17] https://www.cu.edu/ope/aps/6002 [18] https://www.cu.edu/security/security-guidance-software-service [19] https://www.cu.edu/security/policies

Retention of University Records [16]

Establishes universitywide records retention policy and records retention schedules to comply with state law and align with best practices.

Electronic Communications [17]

Establishes electronic communication as the official means of communication and related parameters for use.

Security Guidance for Software as a Service (SaaS) [18]

Provides security guidance for departments and teams who are considering SaaS options for their technology needs.

Visit the Policies [19] webpage for an expanded list.