Union County College
Important information for accessing Email, remote file access and Handling of PPI information
Last Updated: 5/9/2018

Introduction

It is the goal of the IT department to ensure that all users are aware of the security risks of using email and the internet in public locations. This document provides basic guidelines for Union County College (UCC) users on how to maintain basic security.

Scope

Checking Email and Webmail

- Avoid using public computers (any computer that is not personally or UCC owned) and if you do, make sure NOT to save your username or password.

- Always hit the “Logout” button when you are finished using your email, closing the browser may not log you out.

- Do not open email links or attachments from anyone you do not know, immediately delete them.

- Union County College will never ask you for your password through an email, if you receive an email requesting login information, immediately delete it. if you are unsure please forward the email to techsupport@ucc.edu for clarification on whether the email is legitimate.

- Do not click links or attachments on any emails that look suspicious, if you are unsure please forward the email to techsupport@ucc.edu for clarification on whether the email is legitimate.

- If you do click on something and realize you shouldn’t have, immediately report it to the helpdesk: techsupport@ucc.edu so we can look into the issue and see if your data is at risk.

Remote Access outside of UCC

- When accessing email or working on UCC files outside of the College, it is highly recommended to use the UCC VPN https://sslvpn.ucc.edu/ as this will encrypt all transmitted data over the internet and will allow you to use UCC internal data resources.

- Avoid using public Wi-Fi, which is any Wi-Fi network that yourself or UCC does not have control over. If it is necessary, use the UCC VPN.

Personal Owned Equipment

- When using a personal computer for accessing UCC information such as email access or data, always use VPN.
- Be sure to have antivirus software installed and updated at all times in order to protect all personal and UCC owned data

Mobile Devices

- Always make sure to have a password locking your mobile device.
- Always make sure you have a utility set up such as “find my iPhone” or “android device manager” that will allow you to remotely wipe your device if it is lost.

Handling of Personal Identifiable Information (PII)

UCC Faculty, Staff and students should not have PII information stored on any electronic device such as a computer (including shared drives on the servers), discs, USB drives (thumb drives), mobile devices, email or any other type of digital format other than designated servers indicated below. PII information consists of the following:

- Social Security number
- Driver's license number or State identification card number
- Username and password pair
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (NJ Identity Theft Law; C.56:8-161 Definitions relative to security of personal information)

In addition to the identifiers above, other identifiable personal/private information includes (but is not limited to):

- Medical records
- Educational records
- Financial records
- Studies or surveys using personally identifiable data

PII should only be stored within the following servers which have the proper security measures needed to protect the information:

- Colleague
- Recruit
- Image now

If you have any questions or concerns, or have clicked on a suspicious link and/or provided your college login credentials, please contact the IT Department at techsupport@ucc.edu or at extension 4357 (HELP).