VCU

GENERAL GUIDANCE FOR AUTHENTICATION INTO IT SERVICES USED BY VCU (SUCH AS SOCIAL MEDIA ACCOUNTS)

PASSWORDS:

1. PASSWORDS MUST BE AT LEAST 12 CHARACTERS IN LENGTH (VCU'S INFORMATION SECURITY OFFICE RECOMMENDS 16 CHARACTERS MINIMUM) WITH AT LEAST 1 UPPERCASE, 1 LOWERCASE, AND A SPECIAL CHARACTER OR NUMBER.
2. PASSWORDS SHOULD BE UNIQUE AND NOT REUSED IN OTHER PLACES WHEN POSSIBLE.
3. IF SUPPORTED, MULTI-FACTOR AUTHENTICATION (MFA) MUST BE IMPLEMENTED (E.G., RECEPTION OF ONE-TIME TOKEN VIA TEXT MESSAGE OR OTHER MFA APPS SUCH AS DUO).
4. PASSWORDS SHOULD BE CHANGED PERIODICALLY (E.G., ANNUALLY OR WHEN AN ADMINISTRATOR LEAVES).
5. PASSWORDS SHOULD NOT BE RECORDED AND STORED ON ELECTRONIC DOCUMENTS WITHOUT ENCRYPTION, AND PHYSICAL STORAGE SHOULD BE AVOIDED IF POSSIBLE.

IF PASSWORD MANAGEMENT IS NEEDED, VCU'S INFORMATION SECURITY OFFICE RECOMMENDS USING KEEPASSXC.

DON'T BE A PHISHING VICTIM

HOVER YOUR MOUSE OVER LINKS TO SEE ITS ACTUAL DESTINATION, AND NEVER SUBMIT YOUR USER NAME AND PASSWORD OVER EMAIL.

FOR MORE DETAILS VISIT HTTP://PHISHING.VCU.EDU, AND GO TO VCU IT SUPPORT CENTER OR CALL 828-2227 TO REPORT A PHISHING SCAM.