UCDAVIS

INFORMATION SECURITY OFFICE

Top 9 Cybersecurity Habits you need to adopt today

The University is committed to protecting the confidential and personal information that it holds. Information security has a direct financial, operational, and reputational impact on the University and its mission.

Security is everyone's responsibility!

The Information Security Office (ISO) seeks to provide a secure technical environment that protects UC Davis' information assets and minimizes disruption to business processes. However, technology alone is not always enough. All members of the UC Davis community have an obligation to safeguard information – both the campus' and their own.

The 9 Cybersecurity habits you need to adopt today

Incorporate these habits into your online life to help protect your information, your family and your work. They'll also reduce your risk of getting scammed!

1 Phishing – don't take the bait! Always think twice before clicking on links or opening attachments.

- Navigate to web pages by a legitimate path instead of clicking on a link in a message.
- Contact the sender by a separate means to confirm they sent an unexpected attachment.

2 Verify requests for private information (yours or other people's), even if they look like they're from someone you know.

3 Use passwords that can't be easily guessed, and protect your passwords.

- Make them long and strong.
- Never reveal your password to anyone.
- Use different passwords for UC and non- UC accounts.
- Click "no" when websites or apps ask to remember your password.

4 Enable multi-factor authentication.

- Multi-factor authentication adds an additional layer of protection for your accounts.
- With MFA, you use a separate verification to your username and password to login.
- For more info, go to https//movetoduo.ucdavis.edu

5 Protect your stuff! Lock it up or take it with you when you leave.

- Password protect all of your devices.
- Secure your area and lock your computer screen before leaving them unattended–even just for a moment.
- Take your phone and other portable items with you or lock them up.

6 Keep your devices up to date.

- Ensure all devices, apps, browsers, and anti-virus software are set to update automatically.
- Restart your devices periodically.

7 Back up critical files.

- Store copies of critical work files on a drive that gets backed up regularly.
- For your personal files, save a backup copy of anything critical on a separate hard drive, data stick, etc., and store it securely.
- Test your backups periodically.

8 Delete sensitive information when you're through.

- Follow UC Davis' records retention schedule.
- Better yet, don't store it in the first place if you don't need to. If you don't have it, it can't be stolen!

9 If it's suspicious, report it!

- If you think you've experienced a security incident, report it immediately to UC Davis Information Security Office or IT Express. Report any attempted or successful unauthorized access, disclosure, or misuse of computing systems, data or networks, including hacking and theft.
- If a device you use for work has been lost or stolen, whether it was UC Davis-issued or personally-owned:
- Report it to IT Express.
- Change your UC Davis email password immediately.
- For personally-owned phones, notify your carrier.
- **Contact IT Express:** itexpress.ucdavis.edu, 530-754-HELP (4357)
- **Report a security incident:** cybersecurity@ucdavis.edu