UNIVERSITY of CALIFORNIA, Office of the President – Information Technology Services

THE FACTS: Computer Security

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 Office of the President seeks to provide a secure technical environment that protects UC's information assets and minimizes disruption to business processes. However, technology alone is not always enough. All members of the UCOP community have an obligation to safeguard information – both UC's and their own.

EIGHT HIGHLY EFFECTIVE HABITS FOR CYBERSECURITY

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. **Always think twice before clicking on links or opening attachments.**
   - Whenever possible, go to web pages by a path you know is legitimate instead of clicking on a link in a message.
   - If an attachment is unexpected, contact the sender by a method you know is legitimate to confirm they sent it.
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.
   - Use multi-factor authentication when available
4. **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 second.
   - Take your phone and other portable items with you or lock them up.
5. **Keep your devices up to date.**
   - Ensure all devices, apps, browsers, and anti-virus software that aren't managed for you are set to update automatically.
   - Restart your devices periodically.
6. **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, CD/DVD, etc., and store it securely.
   - Test your backups periodically.
7. **Delete sensitive information when you are done with it.**
   - Follow UC's 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!
8. **If it's suspicious, report it!**
   - Report phishing and other suspicious cyber activity to your supervisor and the IT Service Desk (contact info on pg 2).

DON'T BE SHY: REPORT!

Suspicious Incidents and Security Breaches

If you think you've experienced a security incident, report it immediately to your supervisor or the UCOP Information Security Officer.

Report any attempted or successful unauthorized access, disclosure, or misuse of computing systems, data or networks, including hacking and theft.

Unusual Computer Activity

If you observe unusual activity on your computer, report it to the IT Service Desk. For example:

- Strange files you didn't create
- Unexpected windows or pop-ups
- Your web browser starts going to pages on its own, or your mouse starts clicking on things on its own.
- Also report spam and phishing emails!

THE FACTS: Computer Security

ENABLE MULTI-FACTOR AUTHENTICATION WHERE AVAILABLE

Multi-factor authentication (MFA - also called two-factor or two-step authentication) adds an additional layer of protection for your accounts. With multi-factor authentication, you use a one-time code or some type of additional validation in addition to your username and password to log in. This means an attacker needs more than just your password to break in.

When it's offered by a UC service you use for work, or a service that you use for personal activities (e.g. Google, LinkedIn, etc.), enable multi-factor authentication to protect your accounts and the information accessible by those accounts.

KEEP UP TO DATE

One of the most important things you can do to protect your computer, the information on it, and UCOP's network is to keep your software up to date. If your software isn't current, your computer is vulnerable to attack and may spread damage throughout the network or expose sensitive information without your knowledge. UCOP IT manages some software updates for UCOP-issued devices, but not everything. It's up to you to make sure all other software and your personal devices are up to date.

PHISHING – DON'T TAKE THE BAIT!

Phishing is one of the most common sources of infected computers, stolen passwords, and data breaches.

Phishing is any scam designed to trick you into clicking on a harmful link or file; trick you into revealing sensitive information or your password; or trick you out of money - typically via deceptive emails, texts, posts on social networking sites, pop-ups, or phone calls.

It is no longer safe to assume that a message is legitimate just because it looks like it's from someone or an organization you know.

How to Protect Yourself:

- Always be suspicious of unknown links and attachments, regardless of who they appear to come from.
- Never share your password with anyone.
- Never give private information (yours or other people's) to anyone you don't know or who doesn't have a legitimate business need for it -- in person, over the phone, via email, text, direct message (DM), Facebook, Twitter, etc.
- If you can't verify the legitimacy of a message, DELETE IT!
- If you're not sure about a message you receive at work, forward it to the IT Service Desk for assistance (ServiceDesk@ucop.edu).

Be suspicious about any message or phone call that:

- Asks you for your password
- Includes an unknown or unexpected link or attachment
- Asks for financial information or money
- Asks you to update or confirm your account information, and you didn't initiate the communication
- Asks you to go to a login page by clicking on a link
- Requires urgent, immediate action; or threatens you with a penalty if you don't act
- Tells you your computer is compromised (Contact the IT Service Desk if you think your work computer might be infected or compromised! Contact info is below.)
- Is not addressed to you, personally
- Uses poor grammar or spelling
- Sounds too good to be true

LOST OR STOLEN DEVICES

If a device you use for work has been lost or stolen, whether it was UCOP-issued or personally-owned:

- Report it to the IT Service Desk.
- Change your UCOP email password immediately.
- For personally-owned phones, notify your carrier.

GETTING HELP

Ask the IT Service Desk: ucop.service-now.com, ServiceDesk@ucop.edu, 510-987-0457

Visit the UCOP IT Security website:
http://ucop.edu/information-technology-services/initiatives/ucop-information-security/index.html

Learn about Information Security Services:
http://ucop.edu/information-technology-services/services/ucop-it-services/it-policy-security/information-security.html