GENERAL SECURITY TIPS

Since your login accounts provide access to various services, it's vital to keep your account secure. Login accounts would include your U.C. Berkeley CalNet identity, your Haas computing account, as well as your personal logins (Google, Apple ID, etc.)

Protect your password

Never share your account information with anyone. Do not share your password or post it anywhere.

Use a strong password / passphrase

Do not use dictionary words or family or department names. It is best to use a combination of alphanumeric and special characters. Also, changing your passwords regularly, like once a year, would be helpful.

Protect confidential information

Most student information is confidential. Please do not store any private or confidential information on your computer or in unlocked areas. As a rule of thumb, protect the data as if it were your own personal data.

Please see the Campus Data Classification standard at: (https://security.berkeley.edu/data-classification-standard). For any inquiries about this, you may contact the Haas Helpdesk.

Protect your property

Never leave your laptop, phone or personal property unattended. If you need to temporarily leave the device unattended, remember to lock the screen.

Screen Lock

Most Haas-issued computers have password-protected screen locks. Remember to lock these screens whenever you need to leave the machine unattended. If possible, turn off your computer at night (unless it is backed up at night and must be left on) or whenever you do not need to use it.

Tip: If you need to step away from your computer, lock your screens quickly by pressing:

Windows OS: Windows Key + L

Mac OS: Control + Shift + Eject

Update system patches, security fixes, and anti-virus software

System updates and patches help keep systems up-to-date against malware and viruses, so applying them is always recommended. Haas-issued computers are patched regularly and should be relatively secure.

If you have a personal computer, always make sure to check for the latest patches and security fixes. Configure your computers to have updates downloaded automatically. This also includes phones and tablet devices which are potentially vulnerable to exploits.

Use secure and supported applications only

Insecure applications such as certain BitTorrent clients can cause trouble for your computer and leave the University and your personal networks open to attack.

Don't open suspicious email attachments

Many viruses, trojans and worms are spread through email attachments. If you receive suspicious or unexpected items in your inbox, even if it appears to be originating from a member of your contact list, do not open it. Reach out to your contact through a separate email to verify that they sent you the unexpected message or attachment. Contact Haas Help Desk or your network administrator to report the suspicious email.

Backup your data

Protect your information by making sure your data is backed up regularly. You can consider backing data up through several means, including cloud storage and external or accessory hard drive solutions.

Find more security tips and best practices at the U.C. Berkeley Security Basics page.