

College of Arts and Sciences
Information and Computer Security Tips
security.cas.sc.edu

Information Security

1. Protect all Social Security Number and credit card information

Avoid storing paper copies or computer files that include SSN or credit card information. If you must hold paper copies, store in a secure location.

2. Use strong passwords

Don't use passwords like "open", "password", or "123"
Change passwords for sensitive account often.

3. Be cautious of pop-up windows, banner ads, or email attachments

Your web browser or web plug-ins may be vulnerable to attack.
Watch out for PHISHING sites which masquerade as official sites to get confidential information.

4. Stay away from high-risk web sites

Don't visit unknown or suspicious web sites.

5. Never give personal information over the telephone to anyone who calls you

Demand a corporate number and call back.

6. When working from home, use the USC campus VPN connection

VPNs encrypt information that passes through the Internet.

7. Never save SSNs or business acct numbers in files on your office computer

SSNs and names are high-profile targets for identity theft.

8. Don't enable auto-login passwords for any web account on your notebook

If your notebook is stolen, your email or web accounts are compromised also.

9. Protect your Credit Card numbers

When at a check out counter, don't let the person standing behind you see your card.
When ordering on-line, your web browser should display an https://secure site URL.

10. Shred all paperwork that contains personal or business information

Paper copies disposed as trash could be used for identity theft.

11. Don't write passwords on sticky notes attached to your computer monitor

Anyone with access to your office space can see this information.

12. Secure notebooks in a file cabinet or desk drawer when not in use

A thief can steal a notebook from an open office in 10 seconds.

13. Be careful when sending email with attachments

Inspect attachments for any confidential information just before sending.

14. Heed all ZERO-DAY (urgent, high priority) threat announcements on the news networks (ZERO-DAY security threats are those released with no warning)

Install ZERO-DAY updates as soon as they are available, but confirm source!

Computer Security

1. Install Operating System Updates

Keep operating system patches up to date with auto-updates and know how to manually update.

2. Install Application Updates

Always keep programs such as Acrobat, QuickTime, etc. up-to-date.

3. Install and update Virus Protection

USC has a Trend Micro site license agreement. It includes scanners and anti-spyware functions. Macs use VirusScan. Both are available via VIP

4. Lock down your home wireless access point

Use WEP or WAP encryption and change the default SSID, default administrator password.

Contact the store or manufacturer for assistance.

5. Don't disable Microsoft Windows Firewall

If disabled, your computer is more vulnerable to attack.

6. Back up your files

Save critical files onto external drive

7. Verify update notices via email

Verify source for update email notices and ignore notices when links or attached executable files are embedded in the email.