Best Practices for Information Security

Suzanne Dmytrenko, Information Privacy Officer

Email: suzanne@sfsu.edu. Ph: 415-338-2823

Mig Hofmann, Information Security Officer

Email: mig@sfsu.edu. Ph: 415-338-3018

Best Practices for Information Security

1. Do not store any personally identifiable information on your computer

- Do not store any personally identifiable information (such as Social Security Number, date of birth, Driver’s License Number, credit card information and home addresses) on your computer or removable media (such as disks, tapes, USB drives)

Best Practices for Information Security

2. Follow Clean Desk Policy

- Do not leave any personally identifiable information (such as Social Security Number, date of birth, Driver's License Number, credit card information and home addresses) on your desk

Best Practices for Information Security

3. Create complex password choices

- 8 characters or longer
- Use upper/lower case letters and
- Include numbers and special characters when permitted
- Examples:
- 8 character password: iAe2W4S
- Or a longer pass phrase: Iamexcited2work4sfsu

Best Practices for Information Security

4. Regularly change passwords

- Change on a Monday so you have all week to remember
- Change all passwords at the same time
- Use different passwords for home versus work
- If you must write down passwords, secure them in a locked drawer or encrypt in a PDA
- Do not share passwords

Best Practices for Information Security

5. Delete/archive unnecessary information

- Shred papers and destroy CD/DVDs that contain confidential information (use cross-cut shredder)
- Delete or move information off-line that is no longer needed
- Old computers should have data completely erased before being discarded or sent to the swap shop. Contact the DoIT Help desk for information on completely erasing data

Best Practices for Information Security

6. Password protect computers and use password protected screen savers

- All computers should have login passwords
- Lock your computer when you leave your office (on a PC, press Ctrl+Alt+Delete and select “Lock Computer”; on a Mac activate your screensaver and require a password be entered before the screen unlocks
- Set your computer to automatically lock after 15 minutes of inactivity

Best Practices for Information Security

7. Do not use external e-mail or instant messaging (IM) services for SFSU business

- SFSU has spam and anti-virus filters for e-mail
- SFSU e-mail is upgraded and patched regularly
- SFSU e-mail is stored on SFSU servers, not 3rd party

Best Practices for Information Security

8. Set automatic updates for your computer

- Your computer should be set with Windows/MacOS automatic updates option enabled
- Operating system firewalls should be enabled

Best Practices for Information Security

9. Anti-virus and anti-spyware software

- Anti-virus and anti-spyware software on your computer should be configured to update definitions at least once a day
- Computers should be scanned daily for new viruses/spyware missed by active protection
- Viruses/spyware are commonly distributed by websites, screen savers, game software, and other “free” programs

Best Practices for Information Security

10. Do not click links in unsolicited e-mails, instead:

- Type the URL address in the browser
- Follow a link from a trusted Web page
- Use a previous bookmark

Best Practices for Information Security

11. Tips for securing laptops & other mobile devices

- Store all passwords, account names, access codes, login instructions, and authentication tools separately from laptops (not in the pockets of the carrying case)
- Lock up laptops when not attended (cable lock during the day, in a locked drawer or cabinet when you leave for the day)
- Keep laptops out of sight when temporarily stored in a car, hotel room, or home
- When traveling, always keep laptop in your possession
- Record make/model & serial number of your laptop/PDA
- If a laptop/PDA is stolen or missing contact the issuing department immediately

Best Practices for Information Security

12. Relaying confidential information securely

- Send faxes of confidential data to a secured fax machine (i.e. in a locked room) or to an attended fax (where someone is waiting on the other end to receive the fax)
- Send e-mails of confidential data encrypted. Saving confidential data into a Word, Excel, or zip file does not encrypt it. Using the password functionality of Word, Excel, winzip is not sufficient protection of the data. For e-mail a utility such as PGP should be used for proper encryption

Best Practices for Information Security

Q & A