

Related Resources

PASSWORDS

UCSC's Password Standards:

<http://its.ucsc.edu/policies/password.html>

Helpful tips from Microsoft for creating strong passwords, plus a checker to test password strength:

<http://www.microsoft.com/security/online-privacy/passwords-create.aspx>

SAFELY USING THE INTERNET & EMAIL

Cautions about putting information online or entering information on the web, from US-CERT:

<http://www.us-cert.gov/cas/tips/ST05-013.html>

Safer use of social networking sites, from US-CERT:

<http://www.us-cert.gov/cas/tips/ST06-003.html>

LAPTOP SECURITY

Protecting your laptop from theft or unauthorized access, from OnGuardOnline and US-CERT:

<http://www.onguardonline.gov/topics/laptop-security.aspx>

<http://www.us-cert.gov/cas/tips/ST04-017.html>

MORE GOOD PRACTICES

The National Cyber Security Alliance's "Stop.Think.Connect." campaign to help keep you safe online: <http://www.staysafeonline.org/tools-resources/stop-think-connect>

OnGuardOnline's "7 Practices for Computer Security":

<http://www.onguardonline.gov/topics/computer-security.aspx>

IDENTITY THEFT RESOURCES

Tips for identify theft victims, from the California Office of the Attorney General:

<http://caag.state.ca.us/idtheft/tips.htm>

How to protect against and limit damage, from identity theft, from the Federal Trade Commission and the California Office of Privacy Protection:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

http://www.privacy.ca.gov/identity_theft.htm

Cyber Security Awareness

An important key to effective cyber security is each of us taking active measures to learn how we can better protect our computers, our information and ourselves.

Many cyber security threats are largely avoidable. The "Top 10 List" and other resources in this brochure offer practical cyber security tips and pointers for safer computing.

UCSC's Information Technology Services (ITS) Security Awareness Website also offers a wide range of information and resources:

- The Top 10 List of Good Computing Practices included in this brochure
- Information about protecting sensitive data
- Computer security training and tutorials
- Campus security requirements
- How to report computer security incidents
- Excellent UCSC and non-UCSC resources
- And more...

→ its.ucsc.edu/security ←

If you are ever in doubt about a cyber security issue, contact the ITS Support Center:

- Online: itrequest.ucsc.edu
- Phone: 831-459-HELP (4357)
- Email: help@ucsc.edu
- In-person: 54 Kerr Hall, M-F 8AM-5PM



UC SANTA CRUZ

Cyber Security at UC Santa Cruz



its.ucsc.edu/security

Top 10 List of Good Computing Practices

<http://its.ucsc.edu/security/top10.html>

- 1. Use cryptic passwords that can't be easily guessed, and protect your passwords.**
 - Good, cryptic passwords use a mixture of upper and lower case letters, numbers, and symbols; are at least 8 characters in length (or longer if they're less complex); and are difficult to guess and easy to remember (so you don't have to write them down).
 - Don't share your passwords or private account information.
 - For additional information and tips, see UCSC's Password Standards: <http://its.ucsc.edu/policies/password.html>
- 2. Beware of scams.**
 - Don't respond to requests for your password.
 - Only click on links and open attachments from trusted sources.
 - Don't give private information to anyone you don't know or who doesn't have a legitimate need for it.
- 3. Protect information when using the Internet and email.**
 - Don't log in or enter personal or sensitive information online unless you are using a trusted, secure web page.
 - Don't send highly sensitive information via email or instant message (IM).
 - Be extremely careful with filesharing software: Improperly configured filesharing software can allow others access to your entire computer. And don't illegally download or share copyrighted files.
- 4. Secure your area before leaving it unattended.**
 - Lock windows, doors, and drawers; lock up portable equipment and sensitive materials.
 - Never share your access code, card or key.

Top 10 List of Good Computing Practices, cont.

<http://its.ucsc.edu/security/top10.html>

- 5. Secure your laptop computer at all times: keep it with you or lock it up securely before you step away.**
 - In your office, at coffee shops, meetings, conferences, etc. – Remember: laptops are stolen from cars, houses, and offices all too frequently.
- 6. Shut down, lock, log off, or put your computer to sleep before leaving it unattended, and make sure it requires a password to start up or wake-up.**
 - <ctrl><alt><delete> or <Windows><L> on a PC; Apple menu on a Mac.
 - Contact your computer support person or the ITS Support Center if you need help changing your computer's security settings.
- 7. Make sure your computer is protected with anti-virus and all necessary security "patches" and updates, and that you know what you need to do, if anything, to keep them current.**
 - Contact your computer support person or the ITS Support Center for assistance.
- 8. Don't keep sensitive information or your only copy of critical data, projects, files, etc., on portable devices, unless they are properly protected. These items are extra vulnerable to theft or loss.**



Top 10 List of Good Computing Practices, cont.

<http://its.ucsc.edu/security/top10.html>

- 9. Don't install or download unknown or unsolicited programs to your computer.**
 - These can harbor computer viruses or even open a "back door" giving others access to your computer without your knowledge.
- 10. Make backup copies of files or data you are not willing to lose – and store the copies very securely.**

More about Scams

How to protect yourself:

See #2 of the Top 10 List. Also:

- If you can't verify the legitimacy of a link or attachment, don't click on it or open it. This includes links online, in texts, tiny URLs, etc.
- Don't open, respond to or forward spam email.
- Be suspicious of any unsolicited phone call, email, instant messages (IM), text, etc. asking you for your password, financial account information, social security number, or other personal or private information – even if it seems to be from a company or person you are familiar with.
- Don't download unfamiliar software or plug-ins from the Internet.

Key indicators that an email isn't legitimate:

- It asks you for your password, money or financial account information.
- It says there is a problem with your account and has a link where you can go to fix things.
- It is an unsolicited or unexpected email with an attachment, or it has an attachment with a suspicious name or extension (.zip, .exe).
- It's not addressed to you personally.
- The sender isn't specified, isn't someone you know, or doesn't match the "from" address.
- It has spelling or grammatical errors.
- It has a link that doesn't seem match where the email says the link will take you.