

Related Resources

Passwords

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

Tips: <https://www.microsoft.com/protect/yourself/password/create.msp>

Password Checker: <https://www.microsoft.com/protect/yourself/password/checker.msp>

Safely Using the Internet and Email

Helpful pointers to keep in mind when publishing or even entering information on the web, from the US Computer Emergency Readiness Team (US-CERT):

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

Tips and resources for safe use of social networking sites from US-CERT:

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

A catalog of many reported email schemes: This site contains images and text of “phishing” emails, so that people can compare email they have received:

<http://www.millersmiles.co.uk/archives/current>

Laptop Security

Measures you can take to protect your laptop from theft or unauthorized access, from OnGuardOnline and US-CERT:

<http://www.onguardonline.gov/laptop.html>

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

More Good Practices

The National Cyber Security Alliance's “Top Eight Cyber Security Practices”:

<http://www.staysafeonline.org/practices/index.html>

OnGuardOnline's “STOP · THINK · CLICK: 7 Practices for Safer Computing”:

<http://onguardonline.gov/stopthinkclick.html>

Identity Theft Resources

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

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

Information from the Federal Trade Commission about how to protect against and limit damage from identity theft:

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

October is National Cyber Security Awareness Month!

The goal of National Cyber Security Awareness Month is to raise awareness about the many technology-related threats we face each day, and 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
- Online computer security training and tutorials
- How to report computer security incidents
- Excellent UCSC and non-UCSC resources
- And more...

http://its.ucsc.edu/security_awareness/

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

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

National Cyber Security Awareness Month

October 2007



http://its.ucsc.edu/security_awareness/



UC SANTA CRUZ

Top 10 List of Good Computing Practices

http://its.ucsc.edu/security_awareness/top10.php

- 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); 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 Guidelines: <http://security.ucsc.edu/policies/password.shtml>
- 2. Be cautious when using the Internet.**
 - Don't provide personal or sensitive information online unless you are using a known, trusted, secure web page.
 - Just opening a malicious web page can infect a vulnerable computer. Be cautious about clicking on unknown or unsolicited web links. When in doubt, look up the web site on your own and go there independently.
- 3. Practice Safe Emailing.**
 - Don't open email attachments or click on web site addresses in emails unless you really know what you're opening.
 - Delete spam and suspicious emails; don't open, forward or reply to them.
- 4. Secure your area before leaving it unattended.**
 - Lock windows and doors, and never share your access code, card or key.
 - Be sure to lock up portable equipment and sensitive material before you leave your work area (take keys out of drawers).

Top 10 List of Good Computing Practices, cont.

http://its.ucsc.edu/security_awareness/top10.php

- 5. Secure your laptop computer at all times: keep it with you or lock it up securely before you step away.**
 - At all times: 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 or <option><Apple><eject> 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_awareness/top10.php

- 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 Safe Emailing

Key indicators that an email isn't legitimate:

- 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 look legitimate or doesn't seem match where the email says the link will take you.
- It is an unsolicited or unexpected email with an attachment, or it has an attachment with a name that doesn't make sense or match what it is supposed to be.
- It asks you to send money or to provide financial account information.

How to protect yourself:

- Don't click on links or open attachments in unsolicited or unexpected email.
- Don't open, respond to or forward spam email.
- If you are uncertain about an email or phone call, contact the sender using a method you know is legitimate to verify that the message is from them.
- Remember that any unsolicited call or email asking you to disclose financial account information, your social security number, your password, or other personal or private information is suspicious – even if it appears to be from a company you are familiar with.