Information Security Awareness Training:  
Reminders for Computer Users

Protect confidential information, including all patient information.

There’s no excuse for being lax when it comes to “good computing practices.”

<table>
<thead>
<tr>
<th>Your Account is Only As Secure As Its Password</th>
<th>Report Security Incidents/Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Don’t let others watch you log in.</td>
<td>• Such as: Lost or stolen computer, network hacked</td>
</tr>
<tr>
<td>• At home, change your password often.</td>
<td>• UCSD Health – Information Security Help Desk: 619-543-HELP</td>
</tr>
<tr>
<td>• Don’t write your password on a post-it note.</td>
<td>• or 619-543-7474</td>
</tr>
<tr>
<td>• Don’t attach it to your video monitor or under the keyboard.</td>
<td>• UCSD Campus – Computer Incident Response Team, <a href="mailto:security@ucsd.edu">security@ucsd.edu</a> and blink.ucsd.edu/technology/security/services/cirt.html</td>
</tr>
</tbody>
</table>

Password Construction

• It can’t be obvious or exist in a dictionary.
• Every word in a dictionary can be tried within minutes.
• Don’t use a password that has any obvious significance to you.

UCSD Health Password Standard

• Eight character minimum and should contain at least one of each of the following characters:
  − Uppercase letters (A-Z)
  − Lowercase letters (a-z)
  − Numbers (0-9)
  − Punctuation marks (!@#$%^&*()_+)
• Some systems have limitations
• Password construction - pick a sentence that reminds you of the password. For example:
  − If my car makes it through 2 semesters. I’ll be lucky: incomit2s.lbl
  − Only Bill Gates could afford this $70 textbook: oBGcat#
  − Just what I need, another dumb thing to remember!: Jw1n.adtr!

Password Construction: Vanity Plate

• I feel great: if33lgr8!
• Dance of the red shoes: RED.$hoes$
• Dolphins Fan: d0lf1n'sfan

Password Construction: Compound Words

• Used every day and are easy to remember.
• Spice them up with numbers/special characters.
• Misspell one or both of the words and you’ll get a great password.
  − Friendship: Fr13nd+ship
  − Lifelong: L1f3l0ng
  − Teddybear: T3ddy^Bare

Take Precautions with Physical Security of Devices

• Review information on device/data security at blink.ucsd.edu/technology/security

Back-Up Important/Original Data Files & Programs

• You are personally responsible for University data entrusted to you.
• Only save work to the assigned secure network drive.
• If you use a mobile computing device, the computer must have current anti-malware software installed, be current on patches, and must be encrypted with a strong password or passphrase.
• Encrypt any back-up disks or flash-drives.

Avoid Phishing Emails - Recognize when not to open an email attachment

• How to identify phishing scams: blink.ucsd.edu/technology/security/user-guides/phishing.html
• If it’s suspicious, don’t open or reply to it! Delete it!
• Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, *.scr, *.pif)

When Sending Confidential Information by Email

• Confirm the recipient’s address.
• Use the confidential message footer.
• Encrypt the email and email attachments. Learn about email encryption here blink.ucsd.edu/technology/email/encryption/index.html

Anything Done Under Your Log-In is Your Responsibility!

• Log off when you leave a workstation.
• Do not share log-ins, User IDs, or your password.
• IS support staff can help when there is a problem logging-in. Call 3-HELP! Don’t log in for others.
• Use auto log-off (@ 15 minutes) and password protected screen-savers when possible.
• Access only the “minimum necessary” information needed to do your job.

Protect Against Viruses and Worms

• Use a virus scanner and keep it updated.
• Use a firewall when connecting to the internet.
• Don’t install unlicensed software.
• Don’t install something you are not sure of.
• Be careful about what internet sites you visit.

Encrypt Files on Portable Devices

• Laptops, flash-drives, USBs, CDs, etc.
• Use the encryption capabilities built into your operating system or install an encryption program.
• Avoid keeping ePHI and other restricted information on your computing devices, unless absolutely necessary for UCSD Health business.

Wipe Drives Before Getting Rid of Computer Equipment

• Simple erasure is not enough. Degauss the device.
• Contact IS before recycling unneeded computers, or use “DiskWipe” software.

Questions? Call the UCSD Health – Information Security Help Desk, 619-543-7474 or 3-HELP.