Information Security Awareness Training

Reminders for UCSD Health Science Computer Users

Protect confidential information, including all patient / personnel information.

There's no excuse for being lax, when it comes to "good computing practices".

Your Account is Only As Secure As Its Password

- Don't let others watch you log in, e.g., "shoulder-surfers"
- At home change your password often.
- Don't write your password on a post-it note.
- Don't attach it to your video monitor or under the keyboard.

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.

UCSDHC / UCSDHS Password Standard

- Eight character minimum and try to 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

Passwords & Pass-Phrase Construction

- Pick a sentence that reminds you of the password. For example:
- I feel great: if33lgr8!

Password Construction: Use Compound Words

- Used every day and are easy to remember.
- Spice them up with numbers / special characters.
- Mis-spell one or both of the words and you'll get a great password.
- Friendship: Fr13nd+sh1p

Take Precautions with Physical Security of Devices

- Review information on device / data security at:
- http://blink.ucsd.edu/go/secureinfo

Back-up Important / Original Data Files & Programs

- When possible, save all work to the network drive.
- If you store original data on local drives / laptops, you are responsible for creating back-up disks.
- Store back-up disks off-site and in a secure location protected from theft and environmental risks
- Password protect or encrypt the back-up disk

Report Security Incidents / Breach

- Such as: Lost or stolen computer; network hacked
- Healthcare: 619-543-2145;
- UCSD Hot Line: 1-877-319-0265
- Campus Security: security@ucsd.edu

Should You Open the E-mail Attachment?

- If it's suspicious, don't open or reply to it! Delete it!
- What is suspicious?
  - Not work-related
  - Attachments not expected
  - Attachments with a suspicious file extension(*.exe, *.vbs, *.bin, *.com, *.scr, *.pif)
  - Web link
- Unusual topic lines; "Your car?" "Oh! Nice Pic!" "Family Update!" "Very Funny!"

When sending confidential information by E-mail …

- Confirm the recipient's address
- Use the confidential message footer
- Encrypt it, if possible
- E-mails to patients requires patient consent (form D-819) described in the e-mail policy # CEP 18.1

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
- Use auto log-off (@ 15-minutes) and password protected screen-savers when possible
- Access only the "minimum necessary" information needed to do your job. Log-in activity can be monitored

Protect against Malware, e.g., 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 Electronic Media Devices

- Portable devices = Laptops, PDAs, memory sticks, etc.
- Laptop theft is our #1 risk!
- Use the encryption capabilities built into your operating system or buy an encryption program.
- Better yet, avoid keeping ePHI and other confidential information on your portable device, memory cards or PDAs if at all possible and delete files when finished.

Wipe drives before getting rid of computer equipment

- Simple erasure is not enough. Sanitize or degauss the device to DOD standards.
- Contact Information Services before recycling unneeded computers, or use "DiskWipe" software.
- Destroy unreadable drives to prevent access to files

Questions? Call the UCSDHC Information Security Help Desk (619-543-7474) or (3-HELP).

Updated: 4/1/2005 kn, x-19152