UCSF **Benioff Children's Hospital**
Oakland

"INFORMATION
SECURITY AWARENESS"

Two-Factor Authentication

Use a texting authenticator on your Gmail, Facebook, and Banking accounts. It's a free "setting" that you just need to enable!

Public Networks

Don't do sensitive work on public or untrustworthy Wi-Fi networks.

Piggybacking

Don't hold the door open for people that might not have proper entry badges.

Social Engineering

Be careful with people who reach out to you with an email or phone call that you aren't expecting. They might be manipulating you in order to gain access to your private information or company IT resources.

HTTPS

If you are doing anything sensitive online, check for the HTTPS in the web address bar; it means the site is encrypted (but even an encrypted site can be malicious!).

Online Advertisements

Don't click on advertisements, but go directly to your vendor's site instead.

"INFORMATION
SECURITY AWARENESS"

Anti-Virus

Use an anti-virus program like Windows Defender or Symantec, and remember to always apply patches when Microsoft or Apple gives you the option!

Webcams

Cover your webcams! Any teenager can use a free program called Metasploit to hack into your webcam, and spy on you.

"INFORMATION SECURITY AWARENESS"

MAC Filtering

In your home router configuration (typically 192.168.1.1 in the web browser), use MAC filtering to blacklist unknown devices or to whitelist permitted devices.

UCSF Benioff Children's Hospital
Oakland

"INFORMATION
SECURITY AWARENESS"

Phishing

Always look at the destination in a link you are considering "clicking." If you are going to wellsfargo.com, and the link shows, "wellsfargo.interweb.com", then it's probably malicious!

"INFORMATION
SECURITY AWARENESS"

Trojan Viruses

There are many free tools on the internet, but many of them are dangerous! If you are downloading "Free" software, assure that it's from a major vendor like Adobe, Apple or Microsoft – if you don't recognize the vendor, then don't install it!

Exposed Passwords

Don't share passwords or leave written passwords out in the open.