Safe Computing – New Outline (5/11/10)

1. Safe Computing = taking measures to protect your PII and shared resources
   1. What are these things? (define PII, describe resources)
   2. Why should I care?
      1. PII is *your* stuff; compromised PII -> bad consequences, e.g., ID theft
      2. Although university does monitor for *some* breaches, there are no guaranteed safeguards. So (unlike h.s.) you are the first and last line of defense in protecting PII and shared resources
      3. If your computer or your account is found responsible for compromising shared resources, your account/network access will be suspended. You can get out of this (i.e., it’s not permanent and there are univ resources to help you get cleaned up & reinstated), but the ordeal will undoubtedly slow you down for a while.
   3. Questions to check understanding and ID theft video (with ?s) included above
   4. Foreshadow general structure of this unit: avoid getting tricked into giving stuff that you shouldn’t & secure stuff from attack
2. Many ways people try to trick you into giving away your PII and access to resources: Phishing and Social Engineering
   1. Phishing
      1. Introduce the term (perhaps with “respond to…” email)
      2. Results from study
      3. Email example “spearfish” (exemplifies “click to…” case)
      4. Phishing Phil exercise to introduce and practice best practices
   2. Social Engineering
      1. Introduce the idea that these scams set up situation of trust and then take advantage…
      2. Scenario of USB left on floor, clicking on untrusted links, opening attachments
      3. Go through best practices: What is trusted? What is expected? Good password management
      4. Exercise to check understanding?
3. Many ways people try to force their way in to steal your PII and shared resources
   1. What are the ways? Explain malware and bad consequences
      1. Hackers
      2. Viruses
      3. Spyware
   2. What preventative measures should you take?
      1. Back ups
      2. Run anti-virus
      3. Update software
      4. Use a strong password
      5. Install firewall
   3. What behaviors “during” (when you suspect)?
      1. Verify the source
      2. Use Phish Phil strategies
      3. See ISO alerts (sign up etc.)
   4. What behaviors “after” (if infected/compromised)?
      1. When your computer is infected
      2. When your ID is stolen
      3. …

Also, there was the suggestion of two kinds of scenarios under III: 1) a student who doesn’t do the preventative steps and gets in trouble and 2) a student who does but nevertheless must be cautious

Finally, regarding the social networking “topic” from the earlier outline, we tentatively decided to fold this in via scenarios (e.g., in social engineering because facebook instills a false sense of confidence, in PII as in how much information is safe to put on the web)