Computer Security Self-Test: Questions & Scenarios

Rev. Sept 2015

Scenario #1:

Your supervisor is very busy and asks you to log into the HR Server using her user-ID and password to retrieve some reports. What should you do?

a) It’s your boss, so it’s okay to do this.

b) Ignore the request and hope she forgets.

c) Decline the request and remind your supervisor that it is against UC policy.

See next page for answer

Scenario #1:

Answer: C.

User IDs and passwords must not be shared.

If pressured further, report the situation to management, the ITS Support Center (http://its.ucsc.edu/get-help/index.html) or the Whistleblower Office (http://whistleblower.ucsc.edu).

Scenario #2:

You receive the following email from the Help Desk:

Dear UCSC Email User,

Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.

**Name (first and last):*
**Email Login:*
**Password:*
**Date of birth:*
**Alternate email:*

Please contact the Webmail Team with any questions. Thank you for your immediate attention.

What should you do?

Scenario #2:

Answer:

This email is a classic example of “phishing” – trying to trick you into “biting”. They want your information.

Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password or other private information. You should never disclose your password to anyone, even if they say they work for UCSC, ITS, or other campus organizations.

If you receive phishing or spam in your Google email, report it to Google: http://its.ucsc.edu/google/security.html#spam

Scenario #3:

A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card.

What should you do?

Scenario #3:

Answer: Delete the message.

This one has four big risks:

1. Some attachments contain viruses or other malicious programs, so just in general, it’s risky to open unknown or unsolicited attachments.
2. Also, in some cases just clicking on a malicious link can infect a computer, so unless you are sure a link is safe, don’t click on it.
3. Email addresses can be faked, so just because the email says it is from someone you know, you can’t be certain of this without checking with the person.
4. Finally, some websites and links look legitimate, but they’re really hoaxes designed to steal your information.

Scenario #4:

Real-life Scenario:

One of the staff members in ITS subscribes to a number of free IT magazines. Among the questions she was asked in order to activate her subscriptions, one magazine asked for her month of birth, a second asked for her year of birth, and a third asked for her mother's maiden name.

Q: What do you think might be going on here?

See next page for one possible answer

Scenario #4:

Possible answer:

All three newsletters probably have the same parent company or are distributed through the same service. The parent company or service can combine individual pieces of seemingly-harmless information and use or sell it for identity theft. It is even possible that there is a fourth newsletter that asks for day of birth as one of the activation questions.

Note: Often questions about personal information are optional. In addition to being suspicious about situations like the one described here, never provide personal information when it is not legitimately necessary, or to people or companies you don't personally know.

Scenario #5:

Real-life Scenario:

We saw a case a while back where someone used their yahoo account at a computer lab on campus. She made sure her yahoo account was no longer open in the browser window before leaving the lab. Someone came in behind her and used the same browser to re-access her account. They started sending emails from it and caused all sorts of mayhem.

Q: What do you think might be going on here?

Scenario #5:

Possible answers:

The first person probably didn't log out of her account, so the new person could just go to history and access her account.

Another possibility is that she did log out, but didn’t clear her web cache. (This is done through the browser menu to clear pages that the browser has saved for future use.)

Scenario #6:

Two different offices on campus are working to straighten out an error in an employee's bank account due to a direct deposit mistake. Office #1 emails the correct account and deposit information to office #2, which promptly fixes the problem. The employee confirms with the bank that everything has, indeed, been straightened out.

Q: What's wrong here?

Scenario #6:

Answer:

Account and deposit information is sensitive data that could be used for identity theft. Sending this or any kind of sensitive information by email is very risky because email is typically not private or secure. Anyone who knows how can access it anywhere along its route.

As an alternative, the two offices could have called each other or worked with ITS to send the information a more secure way.

Scenario #7:

Real-life Scenario:

In our computing labs and departments, print billing is often tied to the user's login. People login, they print, they (or their department) get a bill. Sometimes people call to complain about bills for printing they never did only to find out that the bills are, indeed, correct.

Q: What do you think might be going on here?

Scenario #7:

Possible answer:

Sometimes they realize they loaned their account to a friend who couldn't remember his/her password, and the friend did the printing. Thus the charges. It’s also possible that somebody came in behind them and used their account.

This is an issue with shared or public computers in general. If you don’t log out of the computer properly when you leave, someone else can come in behind you and retrieve what you were doing, use your accounts, etc. Always log out of all accounts, quit programs, and close browser windows before you walk away.

Scenario #8:

The mouse on your computer screen starts to move around on its own and click on things on your desktop. What do you do? *<Select all that apply>*

a) Call your co-workers over so they can see
b) Disconnect your computer from the network
c) Unplug your mouse
d) Tell your supervisor
e) Turn your computer off
f) Run anti-virus
g) All of the above

See next page for answer

Scenario #8:

Answer: B & D.

This is definitely suspicious. Immediately report the problem to your supervisor and the ITS Support Center: itrequest.ucsc.edu, 459-HELP (4357), help@ucsc.edu or Kerr Hall room 54, M-F 8AM-5PM

Also, since it seems possible that someone is controlling the computer remotely, it is best if you can disconnect the computer from the network (and turn off wireless if you have it) until help arrives. If possible, don’t turn off the computer.

Scenario #9:

Which of the following passwords meets UCSC’s password requirements?

A. @#$)*&^%
B. akHGksmLN
C. UcSc4Evr!
D. Password1

Scenario #9:

Answer: C. UcSc4Evr!

This is the only choice that meets all of the following UCSC requirements:

- At least 8 characters in length
- Contains at least 3 of the following 4 types of characters: lower case letters, upper case letters, numbers, special characters
- Not a word preceded or followed by a digit

Scenario #10:

You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log in to your account and fix the problem.

WELLS FARGO

What should you do?

Scenario #10:

Answer:

Delete the email. Better yet, use the web client (e.g. gmail, yahoo mail, etc.) and report it as spam or phishing, *then* delete it.

Any unsolicited email or phone call asking you to enter your account information, disclose your password, financial account information, social security number, or other personal or private information is suspicious – even if it appears to be from a company you are familiar with. Always contact the sender using a method you know is legitimate to verify that the message is from them.

Scenario #11:

A while back, the IT folks got a number of complaints that one of our campus computers was sending out Viagra spam. They checked it out, and the reports were true: a hacker had installed a program on the computer that made it automatically send out tons of spam email without the computer owner’s knowledge.

Q: How do you think the hacker got into the computer to set this up?

Scenario #11:

Answer:

This was actually the result of a hacked password. Using passwords that can't be easily guessed, and protecting your passwords by not sharing them or writing them down can help to prevent this. Passwords should be at least 8 characters in length and use a mixture of upper and lower case letters, numbers, and symbols.

Even though in this case it was a hacked password, other things that could possibly lead to this are:

- Out of date patches/updates
- No anti-virus software or out of date anti-virus software
- Clicking an unknown link or attachment
- Downloading unknown or unsolicited programs on to your computer

Phishing and Spam Quiz

SonicWALL has a fun, informative quiz to test how well you distinguish between email schemes and legitimate email. Check it out at:

http://www.sonicwall.com/phishing/

Would you like to:

(please click on an option)

Start again

Finish & go to the certificate

Go to the main Computer Security training page