COM6655 Professional Issues Autumn 2021

Tutorial for week 8 (15th November): Computer Misuse

Scenario

“Good morning, class. This week's assignment is simple. See if you can get into the school's mainframe operating system. You've been reading all about password protection and its weaknesses. Now you're to see if you can beat the RACS Network. If you succeed in stealing a network user's password, you are to log in to their account; print a simple document with the username on top, as usual; and log off. You are not to add, delete, or modify any of the user's files. Otherwise, there are no rules. Anything goes, even social engineering."

Social engineering is a confidence game that hackers use on unwary timesharing users to steal their passwords. It involves the use of intimidation, pretence, and outright lying.

Dr. Peter Proctor's class, called Computer Security and Privacy, is one of Lagonda University’s most popular, due in large part to Dr. Proctor's challenging assignments.

Last week, he demonstrated social engineering. He called a fellow faculty member and said, “Sorry to interrupt your busy schedule. This is Karl Oberfest, systems administrator. I need your password to check your account. Afterwards you can change it ... OK, thanks."

Florence Porter and Ann Galen are two of the top students in the class. They generally work together to solve the assignments. This time, though, Florence decides to do it alone. They are sitting side by side at two terminals in the student computer lab.

“Ann, I just can't seem to get logged in. I've tried and tried, but I get bounced off every time. I bet there's something wrong with this terminal."

"Oh, come on! You know better than that. It's got to be something you're doing wrong in your log-in procedure. Try again, only slower."

Florence bashes the keys once more. Again, she turns to Ann.

“I just can't get it. Ann, I know it sounds silly, but just log off and switch terminals with me and you try it. Please."

Ann and Florence switch places. Ann sees this on the screen:

```
RACS Network
USERNAME:>
```

Ann enters her username, "Galen." The screen now shows:

```
USERNAME:>Galen
PASSWORD:
```

Ann looks around. Florence has turned her back, a common courtesy to avoid seeing another's password. Ann enters her password carefully, one character at a time, and receives this message:

```
Access denied on try 1. Disconnected. Reconnect to try again.
```

Curious, she thinks. She knows she has two more tries after reconnecting. She tries again.

```
RACS Network
USERNAME:>Galen
PASSWORD:> ********
Welcome to RACS Operating System
```

"Florence! I got in. It was just a fluke."

"Yes, Florence? You got someone's password without their knowledge? Let's see your printout." Dr. Proctor is clearly surprised and pleased. The printout shows Ann Galen's name at the top.

"Ann, were you aware that your password was compromised? You didn't give it to Florence, did you?"

"Of course not! But how did she do it? I'm very careful about that!"

Florence explained. “I wrote a program that displays the system's prompts. Then I pretended that I had trouble logging in, remember? We switched terminals and you thought you were logging in. But you were really interacting with my program, not the system. It captured your password and placed it in a file in my account, then gave you the 'Disconnected' message and logged off. When you logged in a second time, you weren't in my account anymore, but in the system. It's called the charade technique. Slick, huh?”

Dr. Proctor reminded the class about the hazards of social engineering and congratulated Florence for a job well done. He further explained the charade technique and several other common methods for stealing passwords.

Professor Whitten has just been interrupted in the Introduction to Programming Techniques class. A hand in the back is raised and waiving.

"Yes, George?"

"My files on the RACS are gone. I didn't delete them. Did the University change the system, or what?"

"My files are gone too." "Mine, too..." "Mine, too..."

Adapted from Kallmam & Grillo, Ethical Decision Making and Information Technology, McGraw Hill.

In your breakout groups

- One member of your breakout group should be given the role of rapporteur – they should take notes and be prepared to speak on behalf of the group at the end of the tutorial.

Discussion points

- What are the key facts in this scenario?
- Who are the key stakeholders?
- What are the main ethical issues here? (i.e. should someone have done something, or not done something?)
- What are the legal issues here?