Case Studies

When the average person thinks of network security within a school, they often think of the student trying to hack into the system to change their grade, to see if they can take over their friend's computer, or to put a prank up on the school website. In light of the current network dangers these may be some of least of the school system worries.

All of the following cases are based upon real situations. Read all of the case studies below and for answer the following questions for ***each*** of the three case studies:

- What should be the very first course of action?
- Should the public be informed about the situation? If so, how will their trust be regained?
- What steps should be taken to prevent similar attacks in the future?
- What are the ethical issues of this situation?
- How should students be dealt with if they were the people initiating the attack?

Breached Passwords

There are many ways for people to get passwords. What they do once they have them can be devastating. The important first step in data security is for everyone to take password security seriously. Choosing good passwords, not posting it on your computer, making sure no one is looking when you are typing it in are all simple steps in password security.

Brute force

Hackers used brute force password cracking program to break into the district's computers and initiated a batch of bogus transfers out of the school's payroll account. The transfers were kept below $10,000 to avoid the anti-money laundering reporting requirements. The hackers had almost 20 accomplices they had hired through work at home job scams. Over $100,000 was successfully removed from the account. Two days later a school employee noticed the bogus payments. Unfortunately, unlike consumers who typically have up to 60 days from the receipt of a monthly statement to dispute any unauthorized charges, organizations and companies have roughly two business days to spot and dispute unauthorized activity. This is because school organizations that bank online fall under the Uniform Commercial Code. Due to this law, the district was able to get less than $20,000 of the transfers reversed.

Shoulder surfing

A former student “shoulder surfed” (physically observed) the password of an employee while still in high school. After graduating, he used this information to get into the district’s student information system. From there, he gained access to a different district’s payroll data including birth dates, social security numbers, and bank account information of 5000 current and former employees. This information was then used for identity theft purposes including requesting and using credit cards, creating checks and altering bank account information. The perpetrator was caught and arrested after attempting to use a fake check at a local store. At a cost of $62,000 the district gave all of the affected employees fraud prevention and resolution services. According to the district superintendent, the district suffered “damage to our reputation with the public and our employees. Hundreds of hours were spent investigating the extent of the compromised data and developing the plans and procedures to protect staff from further exposure to fraud.... answering employee questions and preparing internal and external communications. It is impossible to measure lost productivity as employees worried about their financial security and work to change bank account and payroll information."

Key logger

A group of students installed a keystroke-tracking program (this could also fall under malware or student hacking) on computers at their high school to grab the usernames and passwords of about 10% of the students, teachers, parents, and administrators that use the system. The students then used this password information to access the system to change grades for themselves and others. They did not seem to do anything else to the system while they had access.

Source: Wikibooks.org, “Information Security in Education/Case Studies”