Jehiel Benedict F. Russel

**1. Malware**

A school computer containing no confidential information was hooked to the network containing the personal information of over 15,000 students. This computer was breached with malware designed to steal sensitive data. Names, addresses, phone numbers, dates of birth and Social Security numbers were all part of the database that was potentially exposed to this malware. It is uncertain if any of this information was accessed, but the malware was found to have been on the breached computer for approximately five years.

1. **What should be the very first course of action?**

Step 1: Disconnect from the internet.

Step 2: Enter safe mode.

Step 3: Refrain for logging into accounts.

Step 4: Delete temporary files.

Step 5: Check your activity monitor.

Step 6: Run a malware scanner.

Step 7: Fix your web browser.

Step 8: Clear your cache.

1. **Should the public be informed about the situation? If so, how will their trust be regained?**

Yes, the public should be informed because in the first place that’s their data and information, and the school must be the liable of the malware breach to their system. For me to regain the trust of the public they must prove that the situation will never be happened again, and they must upgrade their system in to more secured system and detect a possible malware.

1. **What steps should be taken to prevent similar attacks in the future?**

Step 1: Protect Vulnerabilities

Step 2: Watch out for social engineering.

Step 3: Practice safe browsing.

Step 4: Layer your security.

1. **What are the ethical issues of this situation?**

The ethical issues of this situation are computer crime and breach of privacy.

1. **How should students be dealt with if they were the people initiating the attack?**

For me, it is better for them to be expelled, because we don’t know what their next intentions and things will be will just be happening all over again if we don’t teach them a lesson that they deserve.

### 2. Breached Password - 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 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."

1. **What should be the very first course of action?**

Step 1: Change your password immediately.

Step 2: Use different password in every account.

Step 3: Report immediately if someone is attempting to shoulder surf you.

Step 4: Hide or temporarily delete your information.

Step 5: Backup your files or information.

1. **Should the public be informed about the situation? If so, how will their trust be regained?**

Yes, before it gets worst and the perpetrator will be caught in no time, and the public are aware of what really happen and what is the cause of the incident. To regain the trust of the public the school must tightened their security and won’t let anyone enter a room without permission.

1. **What steps should be taken to prevent similar attacks in the future?**

Step 1: When entering passwords, codes, PINs and other credentials, always protect the keyboard, so its invisible to people and cameras around you.

Step 2: While entering passwords or credentials, never say them out loud.

Step 3: If your work in public places, install a protection on your device to obscure the visibility of the display.

Step 4: Never write down any password.

Step 5: Use multi-factor authentication, single or two-factor authentication.

Step 6: Use different passwords on each account and pick a strong password.

1. **What are the ethical issues of this situation?**

The ethical issues of shoulder surfing is breaching privacy and stealing confidential information.

1. **How should students be dealt with if they were the people initiating the attack?**

The situation must be immediately reported and the perpetrator must be fine on the damage he caused.