# Digital Portfolio Project

**Author:** CENSORED

**Due Date:** 12/6/19

**Class:** ISMN-5730

1. **Administrative Controls:**

**ADMINISTRATIVE – DETERRENT – POLICY:**

**DESCRIPTION:**

**ADMINISTRATIVE – PREVENTATIVE – USER REGISTRATION POLICY:**

**DESCRIPTION:**

**ADMINISTRATIVE – DETECTIVE – CONTROL NAME:**

**DESCRIPTION:**

**ADMINISTRATIVE – CORRECTIVE – TERMINATION:**

**DESCRIPTION:** Termination is the corrective procedure that is employed when a company policy/rule is violated by an employee. By firing the employee, the company is avoiding a lot of liability that might ensue if they were to keep them in their employment. While the action that the employee does may not always seem reasonable to fire them over, it is usually due to them violating a part of a contract they sign when they were hired by the company. A good example of this happening in the real world is the Edward Snowden case; after leaking important classified information from the NSA (and more importantly, violating many contracts and laws) he was terminated from working with the Central Intelligence Agency (CIA).

**ADMINISTRATIVE – RECOVERY – CONTROL NAME:**

**DESCRIPTION:**

**ADMINISTRATIVE – COMPENSATING – CONTROL NAME:**

**DESCRIPTION:**

1. **Technical Controls:**

**TECHNICAL – DETERRENT – CONTROL NAME:**

**DESCRIPTION:**

**TECHNICAL – PREVENTATIVE – PASSWORDS:**

**DESCRIPTION:** Passwords are used to help authenticate a user based on what they know to help secure accounts. These are helpful in preventing attacks like social engineering and unauthorized data mining but are still susceptible to attacks. Some attacks that a system entirely dependent on password-based logins may be susceptible to are passwords crackers, keyloggers, shoulder surfing and malicious software. With 2-Factor Authentication (2FA) this can help protect a web-based service and its’ users from being open to outside attacks. The example I’m providing below is a web portal for Comcast employees to login to use employee tools; while it is open to the Internet for anyone to find, you need a password (and form of 2FA, in this case the CABLE or CORPHQ NT ID) in order to access the system, which will help prevent unauthorized access to the employee tools.



**TECHNICAL – DETECTIVE – LOGS:**

**DESCRIPTION:**

**TECHNICAL – CORRECTIVE – CONTROL NAME:**

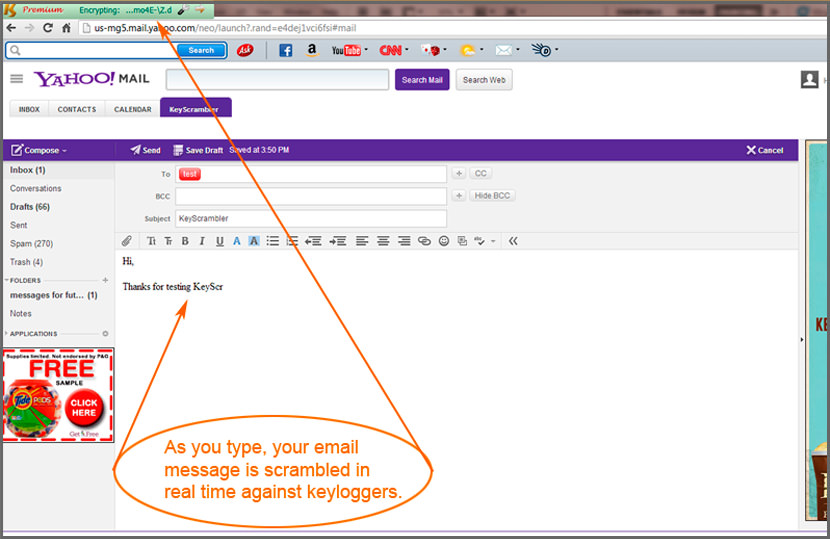
**DESCRIPTION:**

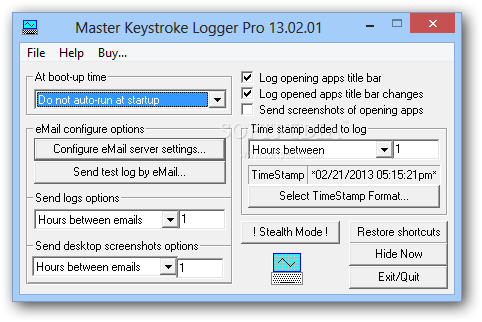
**TECHNICAL – RECOVERY – CONTROL NAME:**

**DESCRIPTION:**

**TECHNICAL – COMPENSATING – KEYSTROKE MONITORING:**

**DESCRIPTION:** Keystroke monitoring is a way of monitoring what all employees are doing without constantly having to supervise them. Using software that accomplishes this will help management prevent malicious activity and misuse of company resources. There is software that exists that can obfuscate key strokes and make this software effectively useless; programs such as KeyScrambler (<https://www.qfxsoftware.com/>) can encrypt all keystrokes into random characters so that it is impossible to determine what the user is typing. The two pictures I am providing below relate to this; the first is a screenshot of KeyScrambler being used and the second is a screenshot of a keystroke monitoring program.





1. **Physical Controls:**

**PHYSICAL – DETERRENT – CONTROL NAME:**

**DESCRIPTION:**

**PHYSICAL – PREVENTATIVE – CONTROL NAME:**

**DESCRIPTION:**

**PHYSICAL – DETECTIVE – CCTV:**

**DESCRIPTION:**

**PHYSICAL – CORRECTIVE – CONTROL NAME:**

**DESCRIPTION:**

**PHYSICAL – RECOVERY – CONTROL NAME:**

**DESCRIPTION:**

**PHYSICAL – COMPENSATING – CONTROL NAME:**

**DESCRIPTION:**