TO: Philip Carson

FROM: IT Staff

SUBJECT: 20 – Social Networking Policy

You asked us to create a policy regarding social network use within the corporation. While social networks like Facebook may be useful for communication, they constitute a large security flaw.

A large amount of information can be gleaned from a person’s social network. If a person were to get access to it, they may be able to infer details about the corporation itself. They could learn about the corporation’s personnel hierarchy and use that to decide whom to target next. Furthermore, they could gain more information about you to use with social engineering attacks.

Social networking systems also introduce vulnerabilities in our computer systems. If a person could be tricked into downloading a virus or other malware from a site like Facebook, it could possibly cause quite a lot of damage to our systems. Furthermore, social networking sites in the past have been vulnerable to cross-site scripting attacks, which could give a hacker access to your cookies, credentials for other websites, and access to your own machine.

If you use such social networking sites for your own personal use at home, we request you do not post any corporate information nor personal information that could introduce vulnerabilities related to company security.

While at work, however, we recommend that access to social networking systems be disallowed for all users.

Sincerely,

The IT Staff