Protecting Your Privacy

Web Site Security

(NAPSA)—Four simple steps can take you a long way toward protecting the information on your computer.

It's important because, according to research from Secure Enterprise 2.0 Forum, there has been a significant increase in the number of Web attacks lately. The report indicates that social networks, wikis and community blogging services and sites are the most popular social media targets for hackers. As social media sites become increasingly popular, hackers work harder and smarter to exploit their vulnerabilities.

Attackers focus on gaining unrestricted access to data on the computer to use for financial or identity theft. Cyber criminals are also known to implant malicious code by exploiting well-known security weaknesses in software.

To protect themselves, Web site users should consider the following when online:

1. Assess the "value" (to you) of the information stored online:

• Ask yourself whether the information on any of your Web sites could be used for malicious purposes.

• As a general rule, it's never a good idea to put any information online you wouldn't want the entire world—including your worst enemy—to see.

2. Isolate accounts:

• Avoid cross-linking your account details. Don't publicly list your e-mail address or link your MySpace page to your Facebook page. This will minimize the chances an attacker can compromise several of your accounts by infecting one.

• Use different passwords. Too often, hackers use information from one account to compromise another.

Protect yourself from hackers: Regularly check that all programs on your computer are up to date and secure.

3. Secure your online logins:

• Use secure, unique passphrases for logons and each Web site you log on to. All of them should be as long as possible and contain UPPER CASE, lower case, symbols and numbers (although the numbers 0, 1, 3, 5 are less secure as people use them as numb3r r3plac3m3nts a11 t00 0ft3n).

4. Secure your computer against malware and exploits:

• Use a reputable security solution that includes browser protection such as Check Point's ZoneAlarm Extreme Security (make sure that "Enable Virtualization" is turned on) or ZoneAlarm ForceField, which works well alongside other security solutions.

• Ensure you have the latest Microsoft Updates and your Automatic Updates are turned on in Windows.

• Before installing unknown software, look for reviews about it at reputable sites such as CNET or PC World.

Following these tips can help you keep your account from being compromised or used to infect others.