

## **Tip of the Month - June 2012**

### **Protect Yourself Against Hackers**

Computer hackers are on the loose worldwide. Big and small companies as well as individuals are easy targets. The mighty Google's recent revelation that its servers have been attacked by hackers, and that Chinese, US and European human rights activists have been adversely affected is proof that hackers are cause for concern. They take delight in discovering the vulnerabilities in your computer system and are indiscriminate agents of destruction.

Enticements to open a malicious email attachment or visit a malicious email attachment or visit a malicious website abound. Once opened, hidden codes allow a remote user to quietly take and retain control of your computer until it is detected or removed.

Here are a few things you can do to help protect your computer from hackers:-

1. Adobe Acrobat Reader and Flash Player are not always safe to use; however if you have to use them for your work please ensure you have the latest version appropriate to your work.
2. Install and update anti-virus and anti-malware software, checking for regular system patches from your vendor (e.g. Apple or Microsoft). Use common sense when opening attachments.
3. Never use an account with administrative privileges for ordinary work, particularly email or online activities such as web surfing.
4. Program your computer to "go to sleep" after a short period of inactivity and require a password to wake it up again.
5. Activate the firewall built-in to your system. Check your documentation or online help for instructions on how to do this.

6. When a new version of an operating system comes out, delete the old one first before installing the new. This ensures you have a “clean” system going forward.
7. Consider purchasing an email digital ID. When you send an email this will allow the recipient to authenticate your identity and allow you to encrypt the contents of your message.
8. Run a proper “scanning” program on a regular basis.
9. Remember, hackers like to look for “security holes” through which they can gain entry without much trouble. These holes frequently exist in the programs and plug-ins that we install on our sites.
10. New software vulnerabilities are found all the time and sometime attacks are devised before software vendors even become aware of the vulnerabilities or patch them. Your best defenses are caution and vigilance.

For more information on this and any other data protection concern you may have, please email us at [dataprotection@bahamas.gov.bs](mailto:dataprotection@bahamas.gov.bs) or visit our website [www.bahamas.gov.bs/dataprotection](http://www.bahamas.gov.bs/dataprotection).

**Remember “Privacy is the Best Policy”**