

## **SECURITY RISK ALERT: FACEBOOK Passwords**

**If your Facebook and online banking passwords are the same, please read below.**

As your trusted financial institution, we want to inform you of a recent Account Takeover computer malware that is targeting Facebook users. It is called the Ramnit worm. Account Takeover occurs when a criminal obtains electronic access to a specific website that requires your username and password. In this instance, the criminal is obtaining Facebook usernames and passwords.

### **Who was affected?**

We do not know what Facebook accounts have been attacked, however we do want to take this opportunity to remind you to use different usernames and passwords for social-based websites and financial accounts. Many individuals use the same passwords to access personal email and Facebook accounts as well as for remote access to corporate networks and online banking accounts. The same passwords or security challenge questions should never be used for social media, email and online banking access. If you have the same passwords setup, we recommend changing them immediately.

### **What can I do to protect myself?**

Below are a few safety tips we recommend for keeping your information safe:

- Review your accounts daily.
- Never use the same passwords or security challenge questions for social media, email and online banking access.
- Make sure you have anti-virus and anti-spyware software installed on your computer, keep them updated, and run a full system scan at least once a week.
- Keep your computer operating system up to date, and your firewall turned on.
- If you download anything from the Internet, such as music, movies or pictures, make sure you do so only from trusted websites. Downloads can be infected with spyware attached to the file.
- Be careful when using public computers to perform any type of personal transactions. Just logging into a website may give away passwords and other private information if spyware has been installed on that computer.
- Business customers should also have a process in place when an employee leaves the company, for example, changing online banking passwords.

### **Who can I contact with questions?**

We draw attention to this alert as a preventative measure, with the intent to keep you well informed of ways to protect your identity. As always, if you have any questions or concerns, or if you ever think your bank account information has been compromised, please contact Bank of Washington immediately at 636.239.7831.

Thank you,

Bank of Washington Customer Service