Security Tip of the Week

Wireless Security

- Use encryption to scramble communications over the network. If you have a choice, use WiFi Protected Access (WPA) as it is stronger than Wired Equivalent Privacy (WEP).

- Use anti-virus and anti-spyware software, as well as a firewall on both your computer(s) and router.

- Change the identifier on your routerfrom the defult so a hacker can't use the manufacturer's default identifier to try to access your network.

- Most wireless routers have a mechanism called identifier broadcasting. Turn it off for your router won't send a signal announcing its presence.

- Change your router's pre-set password for administration to a passphrase or series of letters, numbers and symbols that only you know. The longer the password, the tougher it is to crack.

- Allow only specific computers to access your wireless network using MAC address filtering

- Turn off your wireless network when you aren't using it

- Don't assume that public "hot spots" are secure. You should assume other people can access any information you see or send over a public wireless network.

For more information on this week's tip visit www.rochester.edu/it/security/securitytipofweek.

Need Help? Contact University Information Technology
Online: www.rochester.edu/it ▫ Email: UnivITHelp@rochester.edu ▫ Phone: 275-2000 (5-2000)