Security Tip of the Week

Pharming

Take these simple precautions to protect yourself from pharming:

- Before clicking on a link in a browser window, place your mouse over the link and check the link's address that's displayed in the bar at the bottom left of the window
- Confirm that a website has a valid certificate of authority, from a service such as VeriSign, which matches the site's name before you enter any personal data.
- Only use a secure web site when submitting credit card or other sensitive information via the web browser. The beginning of a secure web site address should read "https". The 's' on the end of http signifies it is a secure site.
- Avoid completing forms in email messages that ask for personal financial information.
- Change the default password that came with your wireless router to your own unique, strong password.
- Make sure your browser is up to date and security patches are applied.
- Regularly check bank, credit card, and debit card statements to ensure all transactions are legitimate.

If you believe that you have been a victim of pharming, notify the Internet Fraud Complaint Center (IFCC) of the FBI by filing a complaint at www.ifccfbi.gov

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)