Be careful computing in Wi-Fi hotspots

When you are on the move and computing in a Wi-Fi hotspot provided in a coffee shop, bookstore, campus, or airport you need to be wary of hackers waiting to access your network or steal your information. Most public wi-fi hotspots do not provide security protection for their users. Here are some tips to use hotspots safely.

1. **Hackers are able to capture network traffic with little effort and chance of being caught.** Make sure that sensitive data is encrypted during transport and not sent in clear-text.

    a. Only submit your credit card and other personal information to secure websites. How do you tell if your communications are protected (encrypted)? Web browsers use various methods to notify the user that the connection is secure such as:
        - changing http:// to https:// by adding an "s"
        - displaying a gold lock symbol 
        - changing the color of the address bar
        - notifying the user that browser session is encrypted
        - displaying a browser alert message when a site's security certification is invalid.

    b. Use a Web-based e-mail service that uses encryption for both logon and message transport. Many services only encrypt log-on information sending text in the clear. To verify that your text is encrypted, make sure you see https://mailprovider.com in the address bar after you log on.

    c. If you're sending sensitive files via e-mail consider encrypting them with the built in encryption features found in various compression utilities. This ensures the security of the data even if the e-mail is accidentally forwarded to unintended parties. Please note that you would have to notify the receiving party of the password and the preferred method to reverse encryption.

        1. Examples: Winzip and Stuffit Deluxe

    d. Be aware that most IM clients do not encrypt their communications. Your conversation could be intercepted and disclosed.
    e. One of the most effective means to safely send data over a wireless network is to use a secured network connection such as a virtual private network (VPN) service. There are many inexpensive (even free) consumer VPN services available to individual users. CABQ offers secure VPN services to staff using your login credentials.
    f. In order to really protect personal information, it is almost always wiser to use another form of transmission besides e-mail or IM (e-mail and IM are rarely secure).