October 2014

Fraud Alert!

C.A.S.E.
Churches Against Senior Exploitation

Weld County District Attorney Kenneth R. Buck
Assistant District Attorney Michael J. Rourke

Wi-Fi Hotspots, what you should know!

Did you know when you log-in to a public wireless hotspot you become a potential victim of identity theft? Coffee shops, hotels, and restaurants offer free public wireless access to you…and to hackers!

The FTC warns consumers that hackers can use unsecured public Wi-Fi to spy on your web browsing activity and gain access to your personal information.

Take these steps when logging into a Wi-Fi Hotspot…

- Verify the correct Wi-Fi network name from an employee, and confirm the address on your wireless menu when you log-in through your mobile device.
- Avoid using online banking and financial sites while logged into a public hotspot.
- Use a Virtual Private Network (VPN) - Frequent users of public Wi-Fi should consider using a VPN to encrypt their data. ***What is encryption?*** Encryption scrambles the data you send on the internet, making it unreadable. The FTC suggests use of encryption is one of the best ways to protect your online activity.
- Switch the settings on your smart phone, or laptop, so it doesn't automatically connect to a public wireless hotspot.
- Change your passwords frequently, and never use the same passwords for multiple sites. This is a good habit to use for all of your online activity!

Visit the FTC Consumer Information website for more detailed information on how to protect your identity on the internet: http://www.consumer.ftc.gov

Immediately report to your local police agency if you think you are a victim of crime.
To view other Fraud Alerts, go to www.weldda.com.