FRAUD WATCH NETWORK
AARP Real Possibilities

Protecting your future

Brought to you by AARP Iowa

The Hidden Perils of Free Public WiFi

By Mary Muehl, AARP Iowa Executive Council Member

It may be a nice convenience to access free public Wi-Fi, but if that Wi-Fi hotspot you use is provided by a con artist, you could wind up paying a steep price for the Internet connection.

According to a new AARP Fraud Watch Network report, nearly half of adults surveyed failed a quiz about online and wireless safety, while tens-of-thousands admit to engaging in activity that could put them squarely in the sights of hackers looking to steal their personal information.

The report, "Convenience versus Security," shows that among adults who access the Internet, a quarter (25%) use free public Wi-Fi once a week or more, and unveils a high incidence of risky online behaviors by the users:

- Among those who say they use free public Wi-Fi, more than a quarter of respondents (27%) say they have banked online via public Wi-Fi in the last three months.
- Similarly, 27% of those who use free public Wi-Fi have purchased a product or service over public Wi-Fi using a credit card.
- 26% of smartphone users do not use a passcode on their phones.
- 61% do not have online access to all of their bank accounts.
- Among those who have set up access to all or some of their online banking accounts, almost half (45%) say they have not changed their online banking passwords in the past 90 days. Experts say that online bank account passwords should be changed every 90 days.

The report also found that most respondents were not up to speed on the best protection scheme for home wireless networks: 84 percent did not know that the most up-to-date security for a home Wi-Fi network is not WEP — Wired Equivalent Privacy.

Experts advise using at least WPA2 wireless encryption for better protection against the same sort of eavesdropping that occurs on public Wi-Fi networks.

To help arm consumers with the information they need to protect themselves from cyber attacks, the AARP Fraud Watch Network has a new cyber scam website featuring "Four Things Never to Do on Public Wi-Fi:"

1. **Don't fall for a fake**: Con artists often set up unsecure networks with names similar to a legitimate coffee shop, hotel or other free Wi-Fi network.

2. **Mind your business**: Don't access your email, online bank or credit card accounts using public Wi-Fi.

3. **Watch your settings**: Don't let your mobile device automatically connect to nearby Wi-Fi.

4. **Stick to your cell**: Don't surf using an unknown public network if the website requires sensitive information - like online shopping. Your cell phone network is safer.

For additional information, including hackers' most common methods of attack and a video demonstrating the risks of unsecure Wi-Fi, visit the AARP Fraud Watch Network at aarp.org/fraudwatchnetwork.

In Iowa, a network of more than two dozen Fraud Watch Network volunteer educators are available to make presentations on scam protection in your community. If you belong to a group or association looking for speakers to talk about how you can protect yourself, your family and your neighbors from scammers, contact AARP. To schedule a free presentation for your community group, learn more about the Fraud Watch Network, or how to become a Fraud Watch Network volunteer, call the Iowa state office at 866-554-5378 toll-free or email ia@aarp.org.

Mary Muehl of Cedar Rapids is a member of the statewide AARP Iowa Executive Council. A retired educator with experience as a science teacher and curriculum consultant, Muehl is volunteer director of the AARP Iowa Fraud Watch Network Speaker's Bureau and one of the volunteers available to speak to groups about how to spot and avoid scams and identity theft. AARP Iowa Executive Council members work with staff and other volunteers to provide ongoing strategic direction for state activities in support of AARP priority issues. AARP has approximately 370,000 members in Iowa.