Consumers Put Digital Convenience Ahead of Safety on Laptops and Mobile Devices

AARP Launches “Watch Your Wi-Fi” Campaign to Increase Awareness of Risks on Free Public Wi-Fi

WASHINGTON, DC—A new survey of internet users shows that the freedom and convenience of public wireless networks may come at a cost. Nearly half failed a quiz about online and wireless safety, and the survey results indicate that thousands nationwide are engaging in activity that could put them squarely in the sights of hackers looking to steal their personal information.

An AARP Fraud Watch Network 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. “A free Wi-Fi network at an airport, hotel or coffee shop is convenient,” said Doug Shadel, a fraud expert and AARP Washington state director. “But without a secure network, Americans risk oversharing, leaving themselves vulnerable to attacks by con artists and hackers.”

In response to these threats and need for greater awareness of the risks of cyber scams, AARP is launching the “Watch Your Wi-Fi” campaign to educate Americans about the risks of free public Wi-Fi and how they can protect themselves. Starting in August, AARP state offices nationwide will be offering free forums on cyber security in multiple locations.

The survey results unveil a high incidence of risky online behaviors:

- 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.

Nearly half of survey respondents (45%) failed a quiz about online and wireless safety. Approximately 40% of respondents were not aware that:

- It is NOT okay to use the same password on more than one site even if it contains a complex mix of letters, numbers and symbols.
- Even if you are not using the Internet, if you’re in a location with a public Wi-Fi network, you should disable your wireless connection.
- It is NOT safe to access websites with sensitive information, such as banking or credit cards, while using a

public Wi-Fi network, even if the website is secured by https.

More than 8 in 10 (84%) people surveyed 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.

“The Fraud Watch Network’s “Watch Your Wi-Fi” campaign is giving people the information they need to stay connected without sacrificing their personal security,” said Shadel.

A newly launched FWN cyber scam website features “**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.

Consumers may also visit the new website to learn about three scams frequently associated with public Wi-Fi, including the “man-in-the-middle attack,” an “evil twin” ruse, and the “war driving attack.”

For additional information, including a video demonstrating the risks of unsecure Wi-Fi, visit the AARPFraud Watch Network.

Survey Methodology: Alan Newman Research completed a total of 800 interviews (559 by landline and 241 by cell phone). Respondents were screened for being age 18 or older and accessing the internet at least a couple of times per month. A total of 11,700 records were dialed. The total sample of 800 respondents yields a maximum statistical error of ± 3.5% at the 95% level of confidence. This means that in 95 out of 100 samples of this size, the results obtained in the sample would be within ± 3.5 percentage points of the results obtained had everyone in the population been interviewed. Interviews took place April 2 through April 11, 2015

# # #

About AARP:

AARP is a nonprofit, nonpartisan organization, with a membership of nearly 38 million, that helps people turn their goals and dreams into real possibilities, strengthens communities and fights for the issues that matter most to families such as healthcare, employment and income security, retirement planning, affordable utilities and protection from financial abuse. We advocate for individuals in the marketplace by selecting products and services of high quality and value to carry the AARP name as well as help our members obtain discounts on a wide range of products, travel, and services. A trusted source for lifestyle tips, news and educational information, AARP produces AARP The Magazine, the world's largest circulation magazine; AARP Bulletin; www.aarp.org; AARP TV & Radio; AARP Books; and AARP en Español, a Spanish-language website addressing the interests and needs of Hispanics. AARP does not endorse candidates for public office or make contributions to political campaigns or candidates. The AARP Foundation is an affiliated charity that provides security, protection, and empowerment to older persons in need with support from thousands of volunteers, donors, and sponsors. AARP has staffed offices in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. Learn more atwww.aarp.org.

CONTACT:
Mark Bagley, 202-434-2560, media@aarp.org, @AARPMedia