Ohio Attorney General's
Consumer Advocate
Newsletter
NOVEMBER 2015

When to Use or Refuse Free, Public Wi-Fi

Free, public Wi-Fi can be an easy way to connect online while on the go. However, it's important for users to understand how their personal information, such as credit card numbers and account passwords, could be compromised while connected.

Follow these cybersecurity tips to protect against hackers and malware and determine when to use or avoid public Wi-Fi:

- **Know the network.** Before connecting, evaluate the legitimacy of the network. Know that scammers often create unsecured networks with similar-sounding names of legitimate networks. Once the user connects to the fake network, the scammer can potentially access any personal information stored on the user's device. For example, if you are trying to connect to a coffee shop's Wi-Fi, first verify the shop's network name and password with the clerk.
- **Never disclose personal information.** Generally, it is safe to use free, public Wi-Fi for catching up on the news or getting an updated sports score. However, never log on to websites requiring a username and password; never conduct online banking or pay bills; and never submit credit card information while connected to free, public Wi-Fi. When using public networks, pretend someone is looking over your shoulder and watching everything you're doing.
- **Review your settings.** Never opt to have devices automatically reconnect to an unsecured network. While this sounds like a convenient feature, a scammer could create a Wi-Fi network so that your device connects automatically to the scammer's network. This could allow the scammer access to personal information stored on your device. If you see a duplicative Wi-Fi network, alert the establishment's staff immediately.
- **Use secure websites.** Websites beginning with "https," rather than "http" in the web address are your clue that they are secure. Some websites will also display a padlock symbol, indicating that the information you are submitting is encrypted. It is especially important to use secure websites when entering personal information, such as credit card numbers or passwords. Encryption scrambles the numbers and letters and makes it more difficult for scammers to read the information.
- **When in doubt, do not connect.** Most tasks can wait until you have access to a secure home network. Also, know that it is possible for computer viruses to spread through a Wi-Fi network, so even if your computer is clean there could still be a threat from other users' devices. It is better to pass up the opportunity for a few minutes of free Wi-Fi rather than risk disclosing personal information to a potential hacker.

In October, Attorney General DeWine announced a new cybersecurity awareness campaign to help Ohioans protect their personal information and stay safe online. The grant-funded program includes cybersecurity messages that will be posted in public transit systems in several Ohio cities and will be available to libraries and schools.

Additionally, the Ohio Attorney General's Office offers free presentations as part of its CHIPP (Cybersecurity Help, Information, and Protection Program) initiative. CHIPP presentations are customized according to the age of the audience, with junior high, high school, and adult versions available.

To schedule a CHIPP presentation or to report a scam or unfair business practice, contact the Ohio Attorney General's Office by visiting www.OhioAttorneyGeneral.gov or call 800-282-0515.

Pension Advances Might Come with High Risk

The sales pitch may be tempting: trade some or all of your future pension in exchange for a lump sum of cash. You may want to sign over future payments in exchange for immediate cash, especially in tight economic times, but be cautious. In many cases, pension advances carry significant consequences.

In a typical pension advance, the consumer must sign over future monthly payments for five to ten years. The pension advance company also may charge additional fees and require a life insurance policy that lists the company as the consumer's beneficiary. This would allow the company to obtain future pension payments, even after the consumer's death.

Before agreeing to a pension advance, review these consumer tips:

- Contact your pension administrator to confirm whether you are allowed to participate in a pension advance agreement. Laws and regulations prohibit some pensions from being signed over to such companies.
- Review all costs and get everything in writing. Obtain a written agreement listing the annual percentage rate (APR), interest rate, commissions, purchase price of any required life insurance policies, and any other costs associated with the deal.
- Review the terms and conditions, and understand the cancellation policies that would apply should you decide the pension advance is not in your best interest.
- Be aware of potential tax impacts, such as the lump sum payment bumping you into a higher tax bracket.
- Research the company by checking complaints filed with the Ohio Attorney General's Office and the Better Business Bureau. Conduct an online search for complaints using your favorite search engine. Type the company name along with words such as "complaint" and "scam."

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioAttorneyGeneral.gov.

Verizon and Sprint Customers May be Eligible for Refunds Under Cramming Settlements

Sprint and Verizon customers who experienced unauthorized third-party charges on their cell phone bills (a practice known as "mobile cramming") have until Dec. 31, 2015, to seek refunds under national settlements Attorney General DeWine announced earlier this year.

Verizon customers can download or submit a claim form at CFPBSettlementVerizon.com or request a claim form by mail by calling the Verizon settlement hotline at 888-726-7063.

Sprint customers can submit a claim or find a claim forms at sprintrefundpsms.com or call the Sprint settlement hotline 877-389-8787.

Sprint prepaid customers (Virgin Mobile, Boost Mobile, Sprint Prepaid, and Assurance Wireless) can file claims for a one-time $7 refund for unauthorized charges that were not previously refunded, according to the Sprint settlement site.

Cramming involves a company adding unauthorized charges to a consumer's phone bill. The scam has targeted landline telephones for more than a decade, and in recent years, it became more prevalent with wireless telephone bills.

A garden-variety example of cramming could begin when someone enters his or her phone number into a website to enter a contest, join a club, or receive information about potential romantic interests. While many scammers need personal information like a Social Security number, credit card, or other financial account number to commit fraud, a crammer generally would need only to obtain a person's telephone number to add charges to a phone bill, making it even easier to lure a victim into losing money. Text messages, e-mails, phone calls, and print advertisements also could be used to try to collect phone numbers for cramming.

Many consumers may have failed to notice bogus charges caused by cramming because crammers often use nonspecific-sounding names like "monthly charge" or "service fee" to describe the charges on the bill. Also, the charges are often small, usually ranging from $1.99 to $9.99.

Earlier this year, Attorney General DeWine, along with the attorneys general of the other 49 states and the District of Columbia, the Federal Communications Commission (FCC), and the Consumer Financial Protection Bureau (CFPB) announced national settlements with Verizon and Sprint to resolve allegations that the companies allowed consumers' cell phone bills to be crammed. Under the settlements, which are estimated to affect hundreds of thousands of Ohioans, Verizon and Sprint agreed to pay a total of $158 million, most of which will be used to reimburse consumers.

Sprint and Verizon were the third and fourth mobile telephone providers to enter into nationwide settlements to resolve cramming allegations. Attorney General DeWine announced similar settlements with AT&T in October of 2014 ($105 million) and T-Mobile in December of 2014 ($90 million).

Under the settlements, the phone carriers agreed to make several changes designed to make mobile cramming less likely, but there are a number of ways you can prevent being taken by this scam:

- Review your phone bill carefully each month for charges you do not recognize. Fraudulent charges could be either one-time or recurring. You may be able to request a more detailed bill from your provider online or over the phone if your bill usually contains few details about the charges.
- Keep a record of the services you have signed up for.
- Don't enter your telephone number into websites you do not trust.
- Watch out for unsolicited texts; this could be a sign that you are receiving a service you did not order.
- Read every part of the promotional material and any forms before signing up for services to be charged on your bill.
- Ask your telephone carrier if it will block third-party charges.
- If you are unsure about a charge on your phone bill, ask your provider before you pay it.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioAttorneyGeneral.gov.

Scam Alert: Beware When Using Mobile Payment Apps

Imagine having tickets for an upcoming concert or sporting event, but realizing at the last minute you aren't able to go. After trying unsuccessfully to sell to someone you know, you post the tickets for sale online.

A potential buyer contacts you immediately. The only problem is that the buyer says he can't withdraw funds from the bank or the ATM to cover the cost, so he suggests using a reputable mobile banking payment app to pay you.

You agree to send him the tickets and to receive payment using the mobile payment app. The buyer sends a payment transfer request through email using the app. You open the email, accept the funds, and then give away the tickets. A few days later, you receive an email stating the payment transfer was cancelled due to insufficient funds in the buyer's account. You realize you gave away the tickets and received nothing in return.

Scammers are using a loophole in some mobile payment apps to trick buyers into sending their items before the scammer's payment has cleared. In this scenario, the scammer initially transferred enough money into the account to send a payment transfer request to the seller. However, since the transfer did not occur in "real time," the scammer was able to obtain the tickets and then withdraw the money from the account before the funds actually transferred. As a result, the funds did not clear, and you are left without your money or your tickets.

Attorney General DeWine offers the following tips for avoiding such scams:

- Never conduct business using mobile payment apps with people you don't know.
- Before giving away the product or service, be sure the funds have officially cleared.
- Contact the bank's customer service number to report suspicious activity related to its mobile payment apps.

If you suspect a scam or unfair business practice, report it to the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioAttorneyGeneral.gov.