The Privacy Podcast - Ep.2: Website Pricing Tactics and the Dangers of Using Wi-Fi While Traveling

Audio is available at http://www.theprivacyblog.com/

Speaker: Lance Cottrell, founder of Anonymizer

Transcript:

This is Lance Cottrell and you're listening to The Privacy Blog Podcast, brought to you by Anonymizer. Welcome to our podcast for November 2012. In this episode, I will be talking about how websites can charge you more for the things you buy compared to someone who lives somewhere else, and other dubious tactics. After that, I'll talk about some of the dangers of using the Internet while on the road – which many of you are likely to be in November and December.

[Part 1: Website Pricing Tactics]

So what's up with getting charged different amounts than people in other places? Well I've been talking about the issue of geo-blocking and geo-pricing for years, but the issue seems to be getting wider attention lately. Geo-blocking is the practice of denying access to a website or other Internet service based on the location of the user. Geo-pricing is when the price of things on an online store are different for people in different places. More generally there is a concept of website clocking, where a site changes its content in some way based on any information they can gather about who's visiting.

In the lead up to the holiday shopping season, geo-pricing may be particularly relevant. The practice of geo-blocking is probably the best known however because it's the most obvious. If you have a Hulu account for example and try to access it while outside the United States, you'll find your access has been denied (and that's pretty obvious). If you've visited an online store while you were out of the country and the prices were 10% higher for you than when you were at home, how would you really know?

A paper published at choice.com.au showed markups averaging between 30%-80% for various software and technology purchases in Australia vs. in the United States. Our internal research has shown hotels varying by over one hundred dollars a night and similar differences in airfares based on what country you're coming from. We've even seen this used by companies against their competitors. They'll set up their websites to show wrong prices *only* to their competitors to trick them into competitively pricing against the wrong price. You might systematically make all of your prices look, say, 10% higher than they really are. If your competitor prices against those prices, you'll get all the business because everyone will come to your site because you really have the low price. So how does all this work?

Well there's several ways for them to see who you are and target you. The first and most commonly used is your IP address. Every computer has an IP address and every IP address is registered and tracked in a big public database. So it's easy to see who owns it. Additionally, there are a number of businesses that have built massive databases of the physical location of every block of IP addresses. They do this in some pretty clever ways. For example, many partner with major e-commerce providers, online stores which share billing and shipping information for their transactions, along with the associated IP addresses. Since people tend to have billing addresses and shipping addresses where their computers are, if you look at where they overlap, the most common ones are going to be the real location of that address.

Even behavior can identify the locations of blocks of addresses. If you look at your search history and the history of all the people in your neighborhood, the vast majority of the location specific searches would be local. So would all the map requests, right? If you are looking up hairdressers and you live in New York, you are unlikely to be looking up hairdressers in Cincinnati very often. They're going to be in New York. By looking at the most frequently requested search and map locations and comparing it to the IP addresses, you know where those IP addresses are with *very* high accuracy. We've seen this happening in practice. When IP addresses start being used by people in a particular area, very quickly we see the search engines starting to provide geographically targeted results and advertising to those IP's. Now tools like Anonymizer Universal hide your IP address by replacing it with one of ours.

It's often well worth your while to cross check prices from your real location against those you'll see when going through Anonymizer. Just make sure you clear out your cookies and history between those visits. Otherwise, they may still know who you are and be careful to show you the same information each time.

Now lots of other things can be used besides IP addresses to target you. A recent relatively benign example was when Orbitz was shown to be targeting Mac users vs. PC users. So when you were searching for hotels, Mac users were generally shown the most expensive hotels at the top of their list, whereas Windows PC users would be shown more mid-priced hotels. Now Orbitz says this is because Mac users ended up choosing hotels that were 30% more expensive on average and they just wanted to show you what you were likely to want anyway – but it just shows how easy it is do this kind of targeting and how many different kinds of things can be targeted.

So clearly your operating system can be used against you. So can your choice of browser. Turns out the kind of people who tend to use Safari may be different than Internet Explorer, different than Firefox, different than Chrome. There are demographic patterns to that. If your computer is set up for a language other than English, that language preference can be seen and targeted. Simple behavior and history can have a huge impact. If you visit an online store directly (just type it into the address bar on your browser) you may see different prices than if you go there from a price comparison site like Pricewatch or Frugal or PriceGrabber. The site you visit can see the site you're coming from. There's a header called a referrer that shows the site you were on before you visited the next site and it even includes things like the search terms you use. So, if you go to a store having searched for "fine wrist watches" you may get very different prices than if your search was for "cheap wrist watches" (even if they're showing you exactly the same wrist watches). Now you can make this easier for yourself by using different browsers with different settings and wiping your cookies between them, and trying different search terms and different discount sites – to try to work out where you're going to get the best price. A small amount of time doing that can be handsomely repaid when you're shopping for gifts this holiday season.

[Part 2: The Dangers of Using Wi-Fi While Traveling]

It's a dangerous thing anytime you step away from your home network. When you are away from home travelling or even at your local coffee shop, you can be vulnerable to some pretty nasty attacks. I'm going to assume that your home network is either wired or WPA protected wireless. Not an open Wi-Fi or a Wi-Fi using WEP. If not, please go fix that, I'll wait…

(Musical Interlude)

All right, so the big problem with Internet on the road is that it's almost always on open Wi-Fi or on shared wired networks. Now you can spot open wireless networks because the icon for those networks will *not* have a lock associated with it. With wired networks at hotels, I always assume any wired connection is shared and vulnerable unless I have personally confirmed that it's secure – which is pretty non-trivial for the average user. So with either open Wi-Fi or shared wired networks, you're vulnerable to having your traffic intercepted. That means that anything you send or receive from the Internet can also be seen by anyone else on the same network. If that data is encrypted, you are probably fine, but most of the websites and a lot of other activity is *not* encrypted. Even if it's encrypted, they can see where you're going and what sites you're visiting.

Now the data they can intercept includes things like everything you do on social networks. In most cases, your authentication token is in a cookie that's passed "in the clear" to the website. This makes it easy to automatically grab it and allows the attacker to log in as you. There's a Firefox plug-in called Firesheep, which completely automates this process for the attacker. You can even call it "point and hack". We have a video showing how this works with Facebook at Anonymizer.com. In "The Lab" section of " The Knowledge Center", look for "Video 2" (or I'll put a link to that in the blog post for this podcast).

The nastiest attack is called the "Evil Twin" attack. So imagine, you're in Dave's Coffee Shop, how do you know you're connecting to their Wi-Fi? Most people just look for a network called "Dave's Coffee Shop". Unfortunately, anyone can set up a network called "Dave's Coffee Shop". If an attacker has a stronger signal than the real network because they are closer to you or they're using some kind of a booster, you'll connect to the attacker's Wi-Fi instead of the real network. This is often called the "Evil Twin" network. The attacker will generally then just pass your data through to the real "Dave's Coffee Shop" network so that it looks completely normal to you – including the login page, splash screen, and everything else that you are used to seeing. Now with an "Evil Twin" attack, not only can the attacker monitor everything you do, they can also modify the communications. They can jump in and pretend to be your bank's website when you visit your bank, insert extra codes or links into web pages, and conduct any other kind of man-in-the-middle attack. So this does *not* mean you need to swear off public networks for good. You just need to take some precautions.

A VPN like Anonymizer Universal can protect you against any of these attacks. While the attacker will be able to sniff the connection, all they'll get is the fully encrypted data pipe between you and Anonymizer (not any of your sensitive content or information about where you're going). Anonymizer Universal authenticates that VPN connection, so an attacker can't pretend to be Anonymizer either. When I need to go use public Wi-Fi or any other un-trusted network, I first quit any program that accesses the Internet – like web browsers and email programs. Then I launch Anonymizer Universal (if it's not already running). After that, I connect to the Wi-Fi. As soon as I've gone through whatever log in or agree to the terms, or whatever else and have a working Internet connection, I immediately activate Anonymizer Universal's VPN. As soon as that's up and secure then I can launch all my software again.

Well that's it for our November 2012 podcast. I'd really like to hear back from you. Let me know what you'd like to get from these podcasts -what topics I should cover, what I could improve, and what you'd wish I would do differently. Until the next podcast, I invite you to continue the conversation on theprivacyblog.com. Thanks for listening!