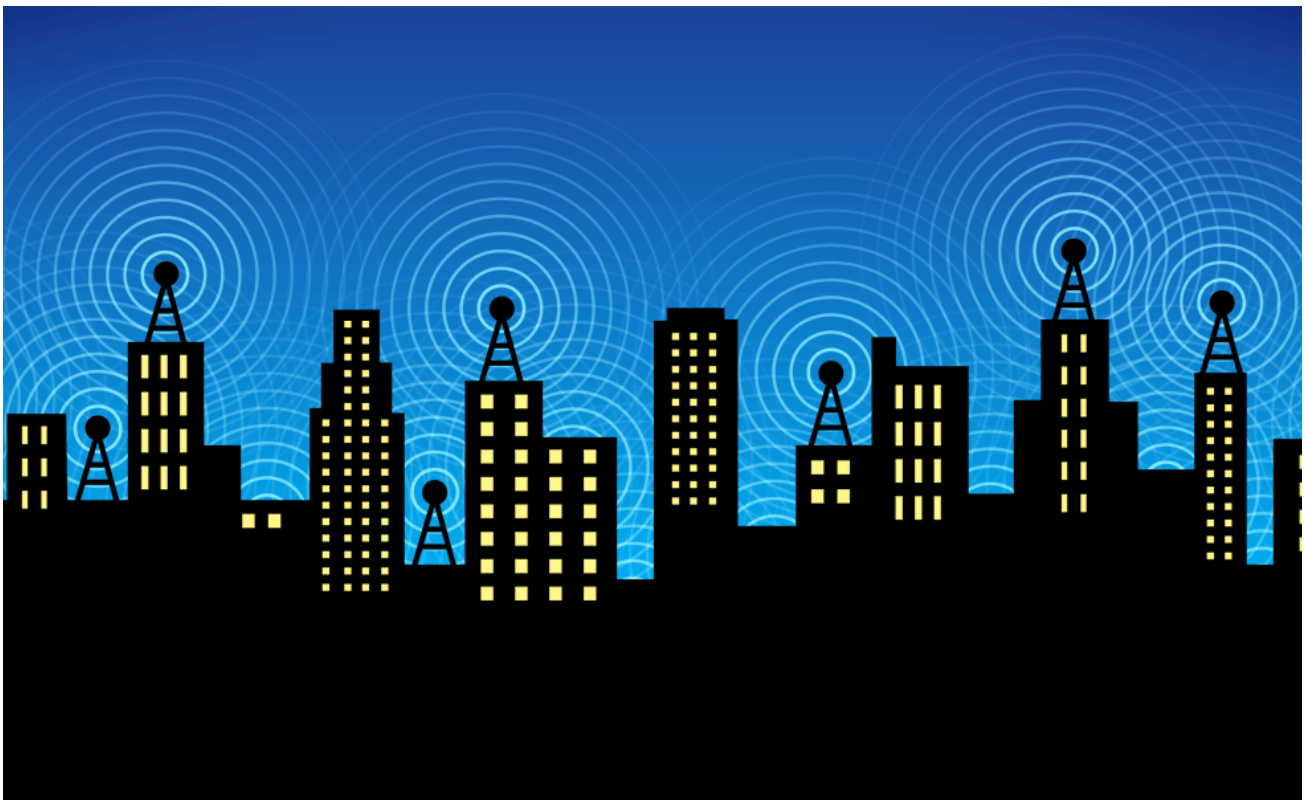


How Captive Portals Interfere With Wireless Security and Privacy

BY GENNIE GEBHART AND JACOB HOFFMAN-ANDREWS | AUGUST 9, 2017

If you have ever wanted to use the wifi at a coffee shop or library, you have probably had to click through a screen to do it. This screen might have shown you the network's Terms of Service and prompted you to click an "I agree" button. Depending on where you were, it might have asked you for

information about yourself, like your email, social media accounts, room number (in a hotel), account number (in a library), or other identifying information. Sometimes you even have to watch a short video or ad before wifi access is granted.

These kinds of screens are called captive portals, and they interfere with wireless security without providing many user benefits.

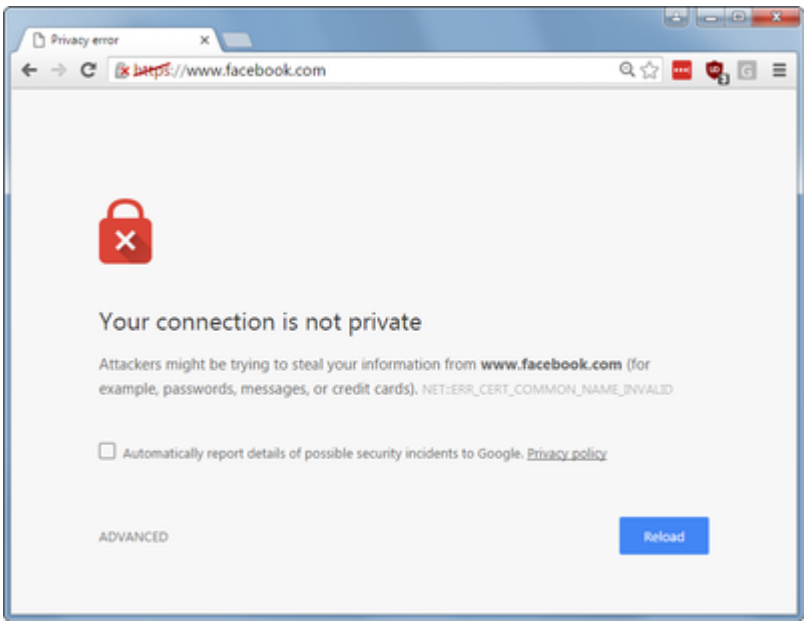
One example of a captive portal. In addition to getting the user's agreement to Terms of Service, other captive portals might ask for login information, social media accounts, email addresses, or other information.

Security and Privacy Problems for Users

Captive portals are to blame for a number of security issues, especially when it comes to HTTPS websites. HTTPS is meant to prevent traffic interception, alteration, and impersonation by a third party. But captive

portals work by doing exactly that: they intercept and alter the connection between the user and the site they are trying to visit. On an unencrypted HTTP connection, the user would not even notice this. But for sites secured with HTTPS, the web browser detects something or someone hijacking the connection (similar to a man-in-the-middle attack). This causes "untrusted connection" warnings about fake certificates for websites that users otherwise expect to be safe.

Those copious unexplained "untrusted connection" warnings on a network with captive portals—essentially false-positive warnings about websites that are actually safe—can train users to adopt the dangerous habit of ignoring security warnings.



A security warning caused by a captive portal interfering with an HTTPS connection might look like this. *Source: Captive Portal, Why Do I Get Those Certificate Warnings?*

And that's not the only inaccurate lesson captive portals teach users about

wireless security. The illusion of security that a log-in window may provide can lead users to inaccurately believe that wireless networks with captive portals are safer than those without.

On top of that, captive portals may not play nicely with devices and softwares that don't have web browsers. This can all be confusing and cumbersome for people trying to use the network.

Despite all this, businesses and organizations have several incentives to use captive portals. Chief among these is user authentication—that is, giving administrators some idea of who is using the wireless network and when. Captive portals that require information about you tie your online activities to a specific login or identity. In addition to monitoring the network, this can help an organization harvest emails for marketing campaigns, or collect social media information to sell to third parties—all trading user privacy in exchange for network access.

Organizations might also use captive portals to display a Terms of Service page. However, that is not the only way to make sure users see and agree to an access policy. The Open Wireless Movement, for example, offers an alternative. Posting a Terms of Service in a physical space, like in a library, can also be an option.

For Network Admins: If A Captive Portal Is Necessary, Follow These Best Practices

If you administer a network and must use a captive portal, you can follow best practices to mitigate some of the security and privacy problems described above.

First, let's look at the problem of copious security warnings. The captive portal should reject connections on port 443 for hostnames it does not recognize. This will generate a "CONNECTION_REFUSED" error rather than the "Connection not private" error that would result from serving an invalid certificate, and will avoid desensitizing users to the risky behavior of clicking through that type of warning. Of course, even better is to pass through HTTPS connections without interference, if that meets your needs.

Second, there's the challenge of authenticating network users. In many cases, access to a restricted network may require a complex login flow that is not currently supported by wifi's simple shared password model. In general, such networks are better off using the more sophisticated WPA2 Enterprise model. In cases where that's not feasible, the network can minimize captive portal harm by: (1) using a valid certificate on a domain name rooted in the public DNS, (2) not interfering with captive portal detection, (3) ensuring the login works in a restricted captive portal login environment (e.g. don't require a logged-in Facebook account), and (4) rejecting HTTPS connections to external domains during the login process, rather than serving an incorrect certificate.

Finally, take advantage of existing device and OS features. Device and OS vendors have come up with ways to minimize the harms of captive portals, by sending an innocuous request on first connection to a network. If that request is interfered with, the OS will open up a special, limited browser to interact with the likely captive portal screen. Unfortunately, some captive portal software interferes with these detection methods by treating the "innocuous request" differently. Instead, best practice is to simply let the captive portal detection software do its job.

Toward More Open, Privacy-Protective Wireless

For most networks, captive portals are an unnecessary barrier between users and a wireless connection. Instead of providing access benefits, they only make users less safe. As we collectively move away from captive portals in our businesses and public spaces, we can move toward more open, more privacy-protective wireless access.