

## Key Points

- Sidejacking attacks involve hackers or criminals stealing cookies, usually via wireless networks. They then use the information from these cookies to surreptitiously log in to the victims' Web-based accounts.
- This form of man-in-the-middle attack has been around for a while and is also known as session hijacking.
- Prevention strategies involve encrypting the cookies themselves and the entire browser session via HTTPS, logging out of Web sessions when done, regularly clearing cookies from browsers, and treating all open public networks as untrustworthy.

# Sidejacking Explained

## Cookies Are Bad For Your Security Health

BY CARMİ LEVY

*Sidejacking is nothing new, but it is of growing concern to IT security administrators. In such an attack, a hacker intercepts a cookie—typically used to retain user-specific information such as username, password, and session data—and then uses the information it contains to gain access to a Web-based service.*

This form of attack, once referred to as session hijacking, is a variation of the man-in-the-middle attack and is a growing threat as the Web becomes a more capable application delivery platform. The popularity of wireless networks, especially unsecured public hotspots, makes it relatively easy for attackers to locate and pursue victims. The increased reliance on Web services by end users further raises the stakes for identity theft.

The majority of Web sites, services, and applications now use cookies to increase convenience—for example, obviating the need for users to re-authenticate every time they connect to a Web site. Because cookies contain the security equivalent of an entire set of keys

to the house, however, they are prime targets for this type of attack.

### ■ WHAT'S THE RISK?

Given the growing reliance on Web-based services, the impact could be significant. A hacker could use information stolen during a sidejacking attack to subsequently log in to a user's Web-based email account or online application suite.

“Ultimately, the risk is that your user's data is compromised, which in turn affects your reputation with them,” says Robert Hanson, applications development manager with QTS ([www.qualitytech.com](http://www.qualitytech.com)). “If your end users are the general public, this typically means loss of users and a lot of bad press. If your users are

business clients, compromised data not only affects your relationship with your client but could also mean a loss of revenue or possibly even a lawsuit.”

Companies not running secure Web services for remote employees put themselves at greater risk compared to those that implement secure VPNs and end-to-end encryption. Wi-Fi hotspots are another area of vulnerability.

“The risk in public wireless networks is very high,” says Marcos Santiago, information security analyst with Scotiabank

Canada ([www.scotiabank.com](http://www.scotiabank.com)). “At this point, I would not recommend connecting to a public, unknown wireless network at all, unless it is absolutely necessary.”

### ■ WHAT CAN YOU DO?

To reduce the risk of sidejacking-based attacks, Santiago recommends either encrypting the cookies or encrypting the entire browser session by delivering everything over HTTPS. Advise users to avoid simply closing the browser session when they are finished working. Instead, they should log off of the Web session from within the app itself. They should also clear cookies from all browsers regularly.

Hanson says organizations looking for even stronger protection against sidejacking should keep track of users' IP addresses, browser types, and versions to ensure they don't change during the course of a session. **P**

## Keep Your Defenses Up

Although corporate networks are somewhat less exposed to sidejacking, Marcos Santiago, information security analyst with Scotiabank Canada ([www.scotiabank.com](http://www.scotiabank.com)), warns IT against becoming complacent, as it's possible for disgruntled employees to use similar techniques on colleagues. He says detection is difficult, even on a monitored network, because once the cookie has been compromised, an attacker logging in looks just like any other user. IT security must focus on traffic sniffing to identify the signature of a sidejacking attack before the attacker has a chance to actually steal the cookie.