Is Your Web Browser Secure?
Presented by Derrell Crimm, CFP®

What comes to mind when you think of online security? Strong passwords? Multifactor authentication? To be sure, these are essential components of information security best practices. But there is one major area that is often overlooked: web browser security. In fact, many of us don't audit our browser security and privacy settings enough, if at all. But why is this so important?

Think of your web browser as the gateway to the rest of the Internet—and all the cyberthreats that come with it. If your browser doesn't have adequate security and privacy settings in place, you could be vulnerable to cyberattacks.

Common features and their risks
The following features are not considered dangerous in and of themselves, but they are commonly used by attackers as avenues of exploitation. It's important to **check your browser default settings**: these settings are often geared toward enhanced usability rather than information security.

JavaScript. This web scripting language is used to create the interactive effects that enhance the look, feel, and functionality of most websites you visit within your browser. **Risk:** Hackers can manipulate the JavaScript on a legitimate website to redirect you to a malicious site that will download viruses or attempt to harvest your personal information.

Java applets and ActiveX. Most likely, you've downloaded and enabled Java applets and ActiveX software components through your browser, as many websites will prompt you to install them so you can view all of the sites' content. **Risk:** Hackers can inject malicious code to vulnerable sites that could compromise your computer and put your sensitive information at risk when you run the applet or ActiveX on that particular site.

Plug-ins, add-ons, or extensions. These software components can be added to work with your browser to support certain features or functionality of different sites. **Risk:** Plug-ins, add-ons, and extensions have updates released regularly, which can leave outdated versions open to security holes. This makes them easier to exploit compared with other software and a prime target for cybercriminals.

Cookies. Have you ever visited a site and your e-mail or username is already populated? Or when revisiting a page, perhaps you've noticed that the online shopping cart has maintained your items from a previous visit? If so, it's all because of cookies. When you browse the web, some of your online activity and information you provide to sites is collected and stored in cookies, including your IP address, the last time you visited that site, and your e-mail address or username. **Risk:** Privacy issues are the main concern here, as some sites (especially advertising sites) use cookies to track your browsing habits without your knowledge.

Increase your security
So, what can you do to protect your information when you're online?

- Browsers give you the option to allow or deny sites to run JavaScript, and it is best practice to allow only trusted and secure sites to do so. Consider creating **allow and block lists** through either your browser's settings or a browser add-on/extension.
- If a website prompts you to install and run a Java applet, run only from a trusted and secure site.
- Allow cookies *only* for sites that you trust, especially if you're providing login or payment information. Best practice is to limit cookies to sites that are secure—look for the **https** before the URL. Similar to JavaScript, browsers include settings to allow or block cookies

from all or some sites. Every once in a while, clear your cookie cache, even if cookies are stored only by trusted sites.

Browser-specific settings
To find settings and help for a specific browser, simply visit the vendor's website. Here are links regarding settings for a few of the most popular browsers:

- Microsoft Edge
- Internet Explorer
- Mozilla Firefox
- Google Chrome

Other reminders and tips
Remember to keep your pop-up blocker setting enabled so that sites are not allowed to show pop-ups; many pop-ups are infected with adware and other malicious or unwanted programs. Further, keep your browser updated to mitigate vulnerabilities and security holes, as hackers can exploit outdated versions. Finally, audit your plug-ins, extensions, or add-ons to ensure that they're up to date.

Derrell Crimm
AC Financial Partners
1800 International Park Drive | Suite 10 | Birmingham, AL 35243
205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm@acfinancialpartners.com