SAFE SURFING

BY GIRIDHARA RAAM M, MARKETING ANALYST, MANAGEENGINE

Browsers have become an integral tool many of us use several times throughout the day, both for work and personal reasons. Since cloud computing has become the new norm, a simple vulnerability in your browser or a phishing attack can pave the way for cybercriminals to take control of your browsers and, in some cases, access corporate data. As Paul Herbka, senior product manager at GCI General Communication said, "Security in IT is like locking your house or car—it doesn't stop the bad guys, but if it's good enough they may move on to an easier target."

Why is browser security so important?
Most industries rely on web applications, with the average employee spending 21 hours of their work week online. Unfortunately, not all browser use at work is carried out on enterprise-approved platforms. According to a survey conducted by International Data Corp (IDC), 30-40 percent of internet

access in the workplace is spent on nonwork-related browsing. On top of this, a staggering 60 percent of all online purchases are made during work hours.

This increased nonwork-related browsing activity has led many IT security teams to focus on browser and port security. Proper browser security management can not only help enterprises defend against web-based threats, but it can also improve employee productivity by only allowing users to access approved sites.

"PROPER BROWSER SECURITY MANAGEMENT CAN NOT ONLY HELP ENTERPRISES DEFEND AGAINST WEB-BASED THREATS, BUT IT CAN ALSO IMPROVE EMPLOYEE PRODUCTIVITY."

Escaping web-based cyber-attacks
There are many types of cyber-attacks, but most of them, including web-based trojans and cryptomining malware, hide within browsers. Phishing has proven to be a prominent technique used by cybercriminals to breach corporate networks. A simple phishing email with a malicious attachment could cause chaos if downloaded or opened, as they commonly contain worms, trojans, ransomware, cryptominers, or other dangerous files.

Even enterprises that are careful about keeping their network applications up to date often forget about updating the add-ons installed in their browsers. These add-ons can easily become outdated, leaving the door open for browser-based takedowns like man-in-the-browser and boy-in-the-browser attacks.

Users browse different webpages based on their jobs' demands. Some webpages may look legitimate, but can actually automatically download malicious content straight to the user's device and spread across the network through open, vulnerable ports. To top this off, phishing and malicious websites aren't the only web-based threats to worry about; there's also cryptojacking, cross-site scripting, outdated JavaScript takedowns, and more.

If IT admins have the right browser security options for monitoring add-ons, then they can easily avoid things like malicious extensions, cross-site scripting, and outdated browser vulnerabilities.

Preventing data leaks in browsers
There are several ways web browsing can lead to corporate or personal data leaks. One of the biggest risks is users uploading confidential documents to third-party sites. Employees can also take screenshots of internal corporate webpages through a browser or execute print page options to export confidential data.

Autofill, while convenient for users, can also cause problems. For example, if a user has enabled autofill in their browser, cybercriminals can use phishing to steal users' autofilled data when they fill out forms on third-party websites.

Aside from traditional USB-based attacks and hard drive theft, browsers have become the primary entry point for all other data leaks. Simply disabling the autofill option or preventing file uploads on all end user devices can greatly benefit corporate data security.

Preventing cyberslacking
Adding to concerns over browser and data security, enterprises need to reign in cyberslacking and prevent employees from wasting company time and resources. That means restricting employees from visiting unwanted websites, downloading unwanted software, and adding anonymous extensions to browsers.

According to a survey conducted by Staff Monitoring, cyberslacking accounts for 30-40 percent of lost productivity. Another report from Interaction states that with 41 percent of UK-based employees admitting to nonwork-related internet surfing during work hours exceeds three hours per week, finding the right browser security and management tool can be a huge advantage for any business.

How browser security benefits your business
Center of Internet Security (CIS) states that browser security is a critical security control for effective cybersecurity. Here are some ways establishing browser security can benefit your organisation:

- Secures corporate data
- Reinforces cloud computing security
- Avoids browser-based cyber-attacks altogether
- Monitors your users and their browser behaviour
- Improves employee workplace productivity

Proper browser security procedures not only add an extra layer of security to your enterprise, but they also give you total control over your network browsers to prevent cyberslacking and increase productivity.