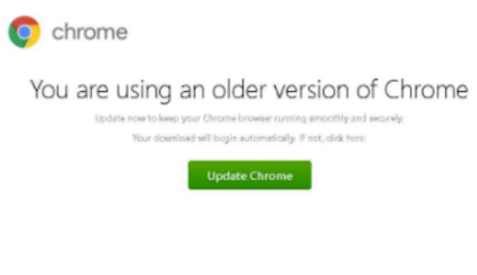
October 31, 2024

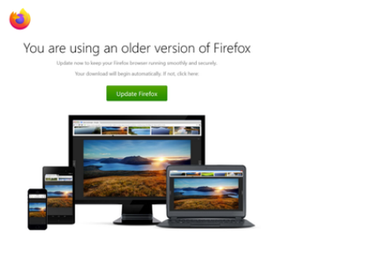
Dear Salt Lake County employees,

The SLCo IT team has recently become aware of a new cybersecurity threat that could turn into a potential attack on the County's network.

What is The Cybersecurity Threat?

Legitimate websites on the internet have become compromised with malicious code that appears as a "browser update" pop-up message and can appear on any web browser. Some fake update messages may also appear as updates for other applications such as Java.





When website visitors click to install the fake update, malware is then downloaded to their computer and gives the attacker access to everything on their computer by communicating with the attacker's website.

What Websites Have Been Compromised?

Too many websites have been compromised to create a comprehensive list. Instead, employees should be cautious when viewing any website and be suspicious of any update messages in their browsers.

What Steps Should Employees Take to Stay Safe?

The SLCo IT team is working to block access to the attacker's website. While they work on their end, employees should:

- Not install the update if a similar pop-up message about updating their browser or other applications appears.
- Contact the IT Team's Service Desk at 385-468-0700 if this pop-up appears on a County-owned computer.

What Do Legitimate Updates Look Like?

If your browser needs to be updated, you will not receive a message like the fake browser pop-up. Google Chrome, Mozilla Firefox, and Microsoft Edge automatically install updates unless the default settings have been changed.

We appreciate your help in ensuring Salt Lake County's data stays secure. Please reach out to the IT Team's Service Desk at 385-468-0700 if you have any questions.

Sincerely,

Zach Posner
Chief Information Officer