Browser Extension and Security FAQ

07/24/2024 12:39 pm EDT

1. What are third-party browser extensions?

Third-party browser extensions are small software modules that are used for customizing a web browser. These extensions are installed by individual users into the browser on their computers and are utilized at users' own risk. Further, such extensions are not affiliated with DrChrono and DrChrono does not have visibility into which extensions any user may use. Browser extensions request permissions from users. Depending on which extensions you have added to your browser, each extension requests its own permissions in accessing, reading, and even changing the information in your browser/computer.

2. What browser extensions should you look out for?

We have learned that if you are using any of the following browser extensions, the information of your patients could be at risk of exposure or misuse and you should cease using them immediately:

- Hover Zoom
- Speak It!
- Super Zoom
- "SaveFrom.net" Helper
- FairShare Unlock
- PanelMeasurement
- Branded Surveys
- Panel Community Surveys

Note: Any browser extension/plug-in you utilize has the potential to read information from your browser and any sites you visit (including DrChrono). The above listed have been found to sell your data to third parties. You should still exercise caution in any extension you install.

We recommend using DrChrono from your browser with no extensions installed.

3. How can you protect PHI from these browser extensions?

If you have one (or more) of these extensions enabled in your browsers, we recommend completely removing all of these extensions immediately as disabling the extensions may not be sufficient. Additionally, at this time, there may be other browser extensions not listed here with security and privacy problems. As such, the best practice is to only access the DrChrono service from supported browsers that have all plugins and extensions removed.

Here are some articles that may help you:

Uninstall an extension in Google Chrome

Disable add-ons (extensions) in Firefox

4. What is DrChrono doing about the situation?

Security and privacy are important. DrChrono has communicated to practices so they can be aware of what we've learned and proactively take steps to protect themselves. DrChrono is also analyzing our services to identify if there are measures we can take that would mitigate or lower these kinds of risks to practices regardless of their browser choice or choices about extensions. Please visit the following link to learn more about our current security measures https://www.drchrono.com/ehr-emr/security-policy/. And, in general, DrChrono regularly works to

enhance and improve its product and inform its user community to help and enhance and improve the protection of practices and patients.

5. How is encryption handled for data in transit?

All communications between the browser/Apple devices and the DrChrono server are made using TLS protocol with a strong cipher and key exchange. All communication between you and the DrChrono server is secured by using AES 256-bit encryption.

6. How is encryption handled for data at rest?

DrChrono encrypts all our data at rest including the database (and its backups) via whole disk encryption using AES 256-bit encryption algorithms. Our data center is both physically and electronically secured. Our servers are isolated from the Internet by using a firewall which is a hardware and software system that blocks access by unauthorized parties.