Identifying and Protecting Yourself from Scareware and Malvertising Tactics:

Malvertising is not a new internet scam, but with the growing prevalence of smartphone usage, the tactics employed have evolved significantly.
It is crucial for consumers to be aware of the potential threats they may encounter while browsing on mobile devices.
Malvertising, as the term suggests, is a form of malware that can deceive users into sending money for fraudulent antivirus software.
This specific type of online scam is known as scareware, which instills fear in unsuspecting individuals through urgent messages claiming their systems are infected.
Alarmingly, scareware is becoming more common than ransomware.

While navigating certain websites, you may encounter pop-up ads that falsely claim you have downloaded a virus (or multiple viruses) and urgently need to install the antivirus software they promote.
Another common scam involves notifications that your smartphone battery is outdated and requires an upgrade.
These pop-ups can be aggressive, making them difficult to dismiss, and may even cause your device to beep loudly or vibrate, inducing panic.
Ironically, following the prompts of these pop-ups can lead

to the actual download of a virus that could compromise your device's files and applications.
In essence, these pop-ups mislead users about a nonexistent virus to entice them into downloading malicious software, often accompanied by alarming sounds and vibrations to reinforce the perceived threat.

If you encounter such a scam, do NOT follow the prompts.
Instead, immediately close the browser tab.
If necessary, navigate to your device's settings, locate the browser app, and clear its cache.
You may also need to force stop the app to resolve the issue.
When using a laptop or desktop, minimize the browser window and utilize a task manager to terminate the browser's activity.
As previously mentioned, this type of malware can be aggressive, often causing your device to emit loud beeping or vibrations to create a sense of urgency.
If a task manager does not suffice, you can restart your computer by pressing Ctrl-Alt-Del simultaneously.

To enhance your protection, ensure that your browser app has the pop-up blocker feature enabled in its settings.
This simple precaution can significantly reduce the likelihood of encountering scareware.
By taking these proactive measures, you can decrease the risk of identity theft and becoming a victim of ransomware.
I hope this information proves useful in helping to safeguard

your online experiences.