

Forum:[Hack Forums](#)

Thread: [Florida DMV Database Breached Through Stolen Police Account — ShinyHunters Claims 200K Records](#)

XtremeDiscount - September 12, 2026, 1:17 pm

Florida DMV Database Breached Through Stolen Police Account — ShinyHunters Claims 200K Records

Florida has confirmed that its DAVID driver database was breached after attackers gained access using compromised credentials belonging to a police department employee.

The Florida Department of Highway Safety and Motor Vehicles says the credentials belonged to a Plant City Police Department user and had been improperly stored on the employee's personal electronic device.

The ShinyHunters extortion group previously claimed responsibility for the breach and says it stole more than 200,000 Florida driver records.

According to ShinyHunters, the group accessed records from the DAVID system and downloaded driver information, HTML pages and images. As proof of access, the hackers reportedly shared a screenshot of Jeffrey Epstein's DMV record containing personal and vehicle information.

Interestingly, Florida's investigation doesn't completely match ShinyHunters' version of how the breach happened.

ShinyHunters claimed it exploited a password-reset vulnerability that allowed access to multiple DAVID accounts, while Florida says the intrusion originated from compromised credentials belonging to a single police department user.

Florida says the breach was discovered on September 4 and was quickly mitigated. Officials say there is no indication that access is still ongoing.

The state has not confirmed ShinyHunters' claim that more than 200,000 records were stolen, so that number currently comes from the attackers themselves.

Pretty crazy that access to a database containing sensitive driver information could potentially come down to credentials being stored on someone's personal device.

What do you guys think?

Should government and law enforcement database accounts even be allowed to authenticate from personal devices?

Source:

BleepingComputer — September 11, 2026

<https://www.bleepingcomputer.com/news/security/florida-confirms-dmv-database-breached-via-stolen-police-account/>

m1000 - September 12, 2026, 1:23 pm

Well that sucks. It really amazes me how a single stolen login credential from nobody more than a department employee could result in something as catastrophic as this. \$20 bucks says the employee got fired. Another \$20 bucks says the employee proceeded to shit their pants.

Tyr - September 12, 2026, 6:37 pm

bro my boy who lives near there tells me this is all insider shit via corrupt police going on in florida rn you'll see some news come up this year or next about it

shady ass cops

(Sep 12, 2026 01:17 PM)XtremeDiscount Wrote: [\[CITE\]](#) Florida DMV Database Breached Through Stolen Police Account — ShinyHunters Claims 200K Records

Should government and law enforcement database accounts even be allowed to authenticate from personal devices?

no lol.. im surprised you are asking if this could ever or would ever work man

(Sep 12, 2026 01:23 PM)m1000 Wrote: [\[CITE\]](#) Well that sucks. It really amazes me how a single stolen login credential from nobody more than a department employee could result in something as catastrophic as this. \$20 bucks says the employee got fired. Another \$20 bucks says the employee proceeded to shit their pants.

\$20 says they will be picked up by an APT group in the future and make bank with them

Prepper - September 13, 2026, 4:32 pm

All government agencies regardless if it is federal or at the state or local level should be provided government issued devices that are locked down and secured.

Personal devices are for personal use only, any attempts to perform official tasks on personal devices should result in immediate termination if confirmed and if any breach is confirmed as a result prosecution should be pursued.

XtremeDiscount - September 13, 2026, 6:35 pm

(Sep 13, 2026 04:32 PM)Prepper Wrote: [\[CITE\]](#) All government agencies regardless if it is federal or at the state or local level should be provided government issued devices that are locked down and secured.

Personal devices are for personal use only, any attempts to perform official tasks on personal devices should result in immediate termination if confirmed and if any breach is confirmed as a result prosecution should be pursued.

I agree, crazy how these leaks happen.