October 25, 2026

Governments Hack People with Zero-Click Spyware in Ads

Citizen Lab says government spyware makers are using global advertising networks to hack devices with no clicks required by using malicious ads. An Israeli company, Discover-Tech, lets spyware makers use its ad network to insert zero-click spyware-laden ads into target's phones. In case you were wondering why I am a fan of ad blockers. Credit: **Tech Crunch**

Please check out our blog at HTTPS://TCPS-BLOG.COM

You can also find copies of the weekly newsletter at
https://cybercecurity-mitch-tanenbaum-blog.com/SNU

We have a YouTube Channel with a lot of videos. Check it out at:
Turnkey Cybersecurity and Privacy Solutions, LLC - YouTube

As part of our YouTube channel we have a demonstration of our AI capabilities. The CyberPulse Scoop is an AI driven cybersecurity interview. Click on PODCASTS once you are in our YouTube channel and then on CyberPulse Scoop.

If you received this email from a friend and want to receive it directly, please send an email to Mitch@CyberCecurity.com.

Thanks for your interest. If we can provide any assistance, please let us know.

Video Blogs

We also have a video and audio blog, including an RSS feed at **https://cybercecurity.us**. Not only are there audio and video versions of the weekly security news updates there, with extended commentary, but there are also other blogs about subjects of interest. Please check it out and let us know what you think.

This week there is a new video discussing the risk of using AI agents to do your online banking. Check it out.

Security/Privacy Alerts

Governments Hack People with Zero-Click Spyware in Ads

Citizen Lab says government spyware makers are using global advertising networks to hack devices with no clicks required by using malicious ads. An Israeli company, Discover-Tech, lets spyware makers use its ad network to insert zero-click spyware-laden ads into target's phones. In case you were wondering why I am a fan of ad blockers. Credit: **Tech Crunch**

AI Alerts

Check out our Certified AI Governance Leader Course at AIGIP.AI. If you are a government employee, check out our AI Governance for Govies at the same site.

Want to stay on top of the news about AI - Check out our news feed on the AIGIP web site at https://aigip.ai/news/latest-ai-news

AI Firms Are Scared (you know what) That They May be Held Liable for Their Software
As I have said before, there are no laws that address who - if anyone at all - is liable when an AI agent hacks a third party. AI companies like Meta and Anthropic are attempting to paint over the damage without taking any responsibility legally for what happened. That could, to some extent, change overnight if states or better yet the feds (much less likely unless something really bad happens), choose to. Still software makers are worried. Credit: **Dark Reading**

CMMC Q&A

I get to listen to hours and hours of webinars every week, so you don't have to.
We are seeing the agencies beginning to get on board and their view of the universe is CMMC Level 2 third party assessment (eventually) for everyone. If you are not already on board this train, the train has already left the station. If you need assistance, please contact us.

**** REMINDER** NEW SPRS/PIEE System Access Requirements**
This is not a change to CMMC, but PIEE is now requiring that you log in at least every 34 days to keep your account active, so make sure you put this on your recurring task list.

DoD Form DD2345 (Militarily Critical Technical Data) is Becoming More Commonly Required
The form is often required when you get access to export controlled technical information and the process is very detail oriented. You mess up one detail and your application gets bounced and you get to start over. There is now an online process where you enter your data and it may take up to 120 days to get approved (and hopefully not rejected). The output of that process is a government signed DD2345 form which you would provide to the requesting prime or agency. Until you have that signed form, if it is required, you cannot get access to the data. There are some thoughts to consider especially if you are a virtual organization. Contact us if you need assistance and plan well in advance.

Reference

Nothing to report

Software and Hardware to Check Out

Microsoft to Treat AI Agents as Insider Threats
Microsoft keeps adding stuff to Microsoft 365 E7 ($99/month/user). This feature allows you to box in AI agents from outside of the agent. Hopefully, something it won't be able to deactivate. They are calling it guardian agents and they monitor and control other agents. Credit: **CSO Online**

Important Issues/Patches

Two Critical Flaws in PHP; Releases EMERGENCY Patches
The emergency patches were released this week to address critical issues. They have not released the details in advance of the release of the patches. The bugs are rated 10.0 on the CVSS scale. Credit: **Bleeping Computer**

Signal Bug Could Keep Your Mic and Camera On After Hangup

A bug in the library used by Signal to manage phone calls could prevent a call from ending, possibly leaving both audio and video active after you thought the call ended. This vulnerability has a score of 9.3 out of 10. It appears that Signal may have forced a patch as my Signal instances have been updated. A proof of concept is available and the library in question is open source, so likely it is used elsewhere and the exploit complexity is considered low.   Look for these versions or higher. Android 8.27.0, iOS 8.30.0 and Windows/macOS/Linux 8.29.0. Credit: **The Register**

Oracle Tries to Compete with Microsoft - And Failed - This Month
As you probably already know, Microsoft patched around 1,400 bugs in this month's patch Tuesday. Oracle, always trying to compete, only patched 1,200 some-odd bugs, failing to beat Microsoft's very high bar. Seriously, if you are an Oracle user, patch now. Credit: **Security Week**

Legislative and Legal Activities

DHS Admits it Lied in Case of Person Who Gave Customs Phone Wipe Password
This case dates back to 2024 when the FBI asked Customs to hold Samuel Tunick. Customs told him he was suspected of kiddie porn, which was a lie. He was suspected of domestic terrorism because he was opposed to the Cop City project outside Atlanta. That distinction is important because it could trigger whether the border exception for not requiring reasonable suspicion and other factors was just a ruse. More briefings are due next month and we will watch this case. Credit: **404 Media**

Education

Personal Privacy and Cyber Tips
Law firm Morrison Foerster presented a great end-user level educational presentation on what you can do to protect yourself and your business. See it on YouTube **here**.

Breaches

Note: I could probably report on a hundred a week, but that would make for a very long report. I will, at least, mention a few of the high-profile ones. NOTE THAT THIS IS THE ONLY SECTION THAT I CAN FILL TEN TIMES OVER EACH WEEK.

Hack Exposes Millions of California Students' Data
The data was stolen from a non-profit that contracts with the state's Department of Education. The data stolen includes name, address, demographic information and disability status of ALL 7 million students enrolled over the last three school years. Credit: **Politico**

- -

Will you have to share your license to surf the web?
The protect the kids laws that are popping up in multiple states requires companies to figure out who a kid is. In order to do that, they have to know who everyone is. There are lots of different ways to do that, each of which has a different reliability level. Government issued IDs are one. It is unclear which one each site will choose, so you may have to furnish different IDs to different

sites or, you may have to ID yourself to use your phone at all and then the phone will share that data. Learn more **here**.

Preparing operational tech (OT) devices for post quantum is complicated
If you think that preparing your IT systems for the post quantum era is hard, that problem is nothing compared to getting your factories, critical infrastructure and other OT systems ready. Learn more **here**.

This week's tech insanity is not over
Actually last week by now. Between PHP and node.js, we thought that was enough of a challenge, but then we added Fortinet, Railway, Connectwise and more. Learn more **here**.

Security News for the week ending October 23, 2026
This week's news: Meta is on the hook for $25 billion, Norway proposes new Undersea cable between Canada and Europe that bypasses the US. is AI backlash becoming a workplace security risk, GoDaddy revokes 404,000 SSL certificates and ICE is creating a $100 million domestic secret police force. Learn more **here**.

With AI discovering bugs at AI speed, are you ready?
I don't think anyone was prepared for a bug that affected 70 percent of the web (the PHP bug), but this is only the start. Buckle in because the ride over the next few years is going to be "interesting". Those who are prepared will survive. If you need assistance or just a third party check, please contact us.

Mitch
www.CyberCecurity.com
www.TurnkeyCybersecurityAndPrivacySolutions.com
Mitch@CyberCecurity.com
720-891-1663