

October 4, 2026

Humans Are Reviewing Your AI Prompts and are Horrified

Microsoft is the latest AI vendor to admit that they have hundreds or thousands of people reading your prompts and looking at your pictures. ***If you thought anything you ask AI is private - even for corporations, you are fooling yourself.*** Like we have seen with social media, reviewers are being bombarded with lewd or explicit photo editing requests. OpenAI is doing the same thing. Faces are uncensored and many of the requests are sexual in nature and likely not consensual. Credit: [404 Media](#)

Please check out our blog at [HTTPS://TCPS-BLOG.COM](https://TCPS-BLOG.COM)

You can also find copies of the weekly newsletter at <https://cybersecurity-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://cybersecurity.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.

Security/Privacy Alerts

Humans Are Reading Your AI Prompts and are Horrified

Microsoft is the latest AI vendor to admit that they have hundreds or thousands of people reading your prompts and looking at your pictures. ***If you thought anything you ask AI is private - even for corporations, you are fooling yourself.*** Like we have seen with social media, reviewers are being bombarded with lewd or explicit photo editing requests. OpenAI is doing the same thing. Faces are uncensored and many of the requests are sexual in nature and likely not consensual. Credit: [404 Media](#)

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 Pricing - Clear as Mud

While there are some AI services that are priced on a fixed price per month like an end user's access to Claude or ChatGPT, almost all advanced AI services are priced based on the unit of work done. Each service calculates this differently, of course. Below is a link to an interesting chart that may help, showing the cost per million input tokens and output tokens (priced separately and differently) for a wide range of companies. This, of course, is not sufficient to figure out your AI spend, but if you don't have unlimited pockets, you need to consider what you are going to allow and what you are going to prohibit. Details at [Layer3Labs](#)

As Pressure Builds on AI's Actions, People are Speaking Out and FTC Investigates

As the president invited all of the AI company CEOs (and donors to his campaign) to the White House to discuss AI safety, the noise around AI is getting too loud for politicians to ignore. The FTC (which can't really fine people according to the Supremes, but can get companies to voluntarily agree to consent decrees) has opened, according to Reuters, a "sweeping" probe into Anthropic, OpenAI and other AI labs to uncover the potential dangers their technology poses to consumers, according to a source. Note that unlike the meeting at the White House and the AI/SI executive order, there was no announcement by anyone, other than a leaker, that this investigation started a couple of weeks ago and no one knew about it until it was leaked (probably on purpose to reduce the heat) to the media. You can learn more about the actions that law enforcement can and likely will take at the link. I don't think this self-regulation thing is going to actually work. While new laws MAY be needed, it is fair to say that Section 5 of the FTC Act (causing consumers' harm) and the equal laws at the state level are extremely powerful if politicians choose to use them. Credit: [Gary Marcus](#)

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.

Status of the CMMC Provider Ecosystem

Every month we get an update on CMMC from the CyberAB. Here are this month's stats:

- 117 C3PAO organizations
- 564 C3PAO applicants
- 1179 Certified assessors
- 2199 Certified professionals
- 2362 Organizations that are third party assessed at Level 2
- 151 Level 2 assessments in process

So, there is no shortage of assessors and the reality is that companies are not ready to be assessed. Credit: CyberAB

Reference

Nothing to report

Software and Hardware to Check Out

Nvidia Releases “Open Agent Safety Platform”

They claim this software, which they are open-sourcing, combines software and an out-of-band DPU-based chip with a reference system design that they claim will secure agents from going rogue. Is this really just a PR stunt that no one will adopt or is this going to be a standard that is adopted widely. Your guess is as good as ours. Credit: [CSO Online](#)

Important Issues/Patches

Nothing to report

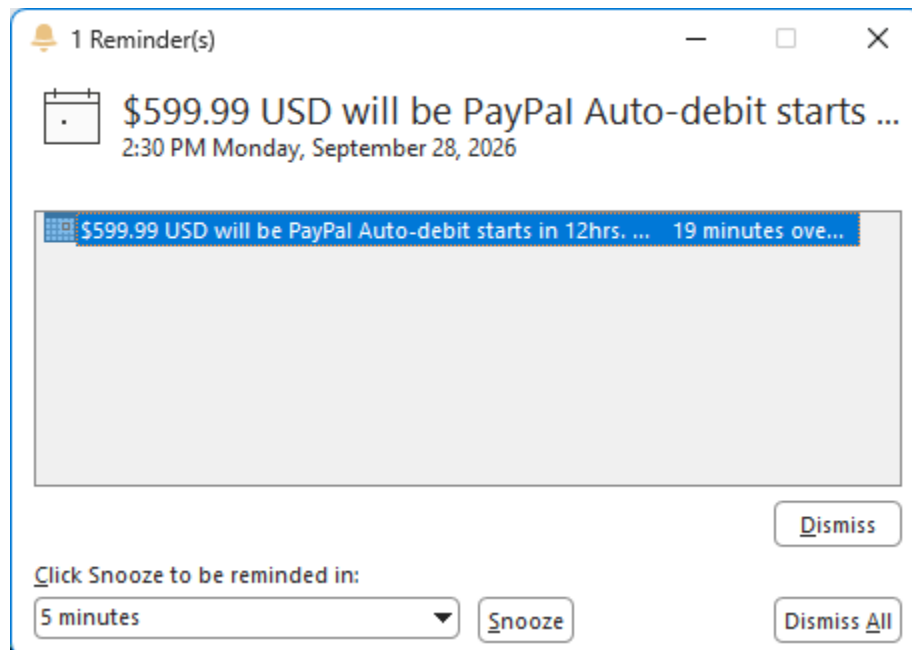
Legislative and Legal Activities

Nothing to report

Education

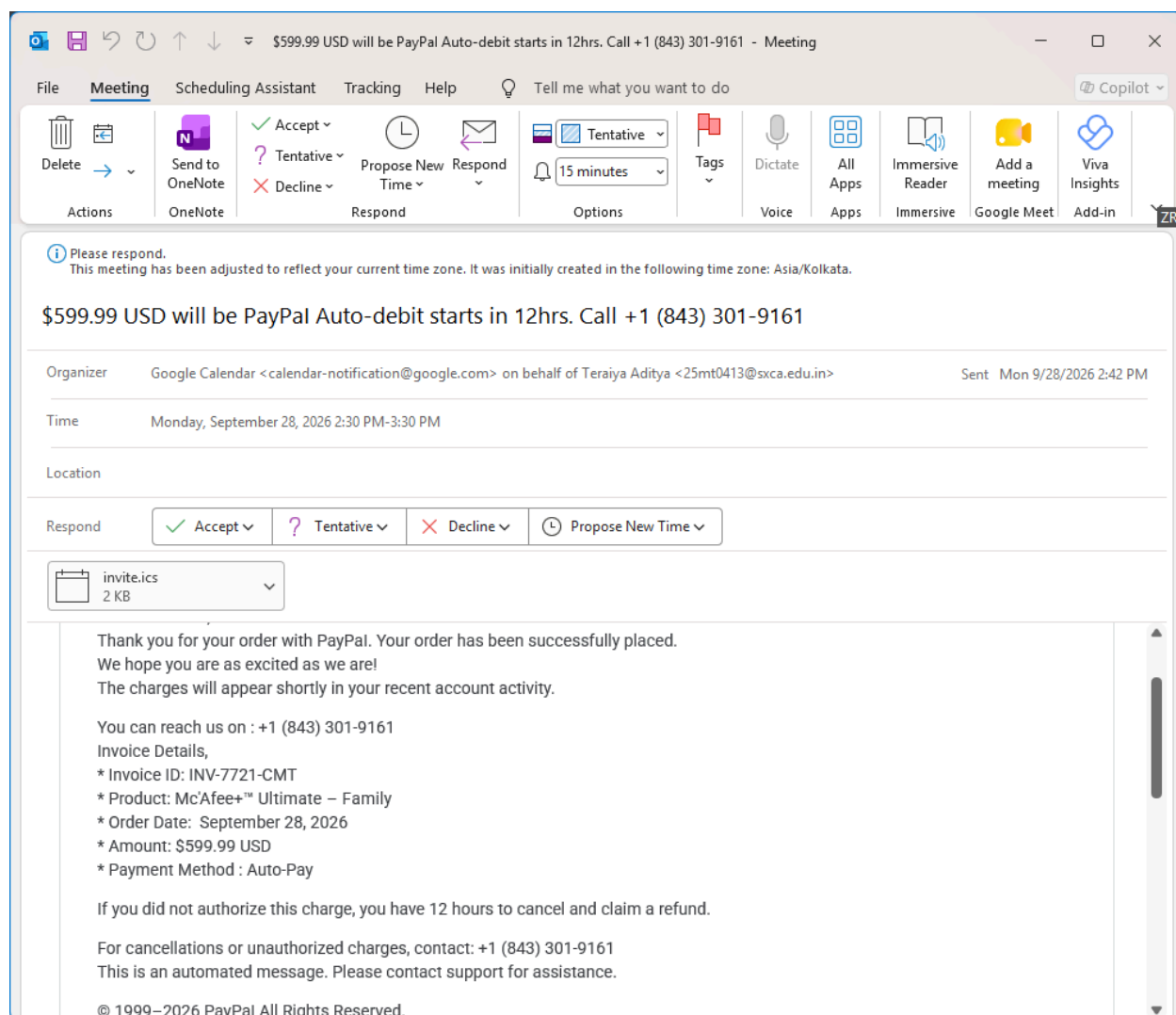
Payment Scams Now Showing Up at Meeting Invites

As software gets better at filtering out scam emails like “you are about to be billed for \$399 for Norton Antivirus - call this number in the next 12 hours to cancel” - which is a scam. You didn’t order it and you won’t be billed. But when you call the hackers they are going to ask you for the credit card info that it was billed to “for security purposes”. Recently, they have shifted to sending meeting invites with a similar scam. The anti virus software doesn’t filter those. Here is an example.



It just pops up and you go CRAP! and maybe fall for the bait.

If you open the meeting invite you will basically see the same scam as you used to see in emails.



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.

FBI Sort of Admits That the ShinyHunters Hack is Real

The FBI has reportedly told its agents and support staff that their personal information was stolen in a recent cyberattack. Publicly, it is crickets. They have declared a cyber incident, whatever that means to them, besides having to change their undies. The internal memo said that names, addresses, job titles and socials were exposed. Needless to say, for an FBI agent and their family, having their address exposed is not good. However, the media is saying that medical information like blood and urine samples (I assume they mean the results and not the liquids) and psychiatric reports were also stolen. ShinyHunters says that they stole between 2-3 terabytes of data but they don't plan to release it; they just want to call attention to themselves. Sure. We believe them. Credit: [Tech Crunch](#)

Month's Long Breach at Pentagon Announced

The government is alerting several million current and former defense personnel that their information was stolen during an almost year-long romp through files at the Defense Manpower Data Center. This was data that was in an unspecified file sharing system (is this related to the recent announcement from Kiteworks that told customers to turn off their servers? I don't know but it could be) that DMDC uses. Besides the usual name, birth, sex and race, it says other information about their military service was stolen. The data was NOT ENCRYPTED. Good job DoD. The breach includes data on 2.8 million living people and 300,000 dead ones. DMDC has records on about 60 million people so the fact that - at least for now - data on just 3 million appears to have been taken over close to a year says the attackers were dribbling out the data to avoid being detected. Credit: [Tech Crunch](#)

Is AI out of control

The answer probably depends on who you talk to, but for a lot of people, the answer is yes. Here is what people are saying and why. Learn more [here](#).

What is really in the White House AI agreement?

First of all, it is purely voluntary. Nothing in the very short one page memo has any way to enforce it. It is totally voluntary and, of course, open to interpretation. There are 4 points which include robust internal controls and doing some sort of wave of the hand external assessments. There is zero detail on anything. Learn more [here](#).

Can AI recover its reputation? Does it care?

Possibly, but it is going to be damn tough. There is an awful lot of distrust of AI right now and I don't think it is going to get any better anytime soon. The more we look, the more bad things that these AI agents have done. Unfortunately, we get to deal with the fallout. Learn more [here](#).

Security News for the week ending October 02, 2026

This week's news: millions of California cars can be hacked by bluetooth, Apple and AT&T say some iPhone 18 Pro Max phones need to be physically replaced, bipartisan backlash to license plate readers, Chinese open-weight models catching up to US and AI hallucinates even in court. Learn more [here](#).

Are You Ready for AI?

Can you really avoid using AI - not really. I assume if you are avoiding AI, you are no longer using Google or Bing search engines. Since everyone else is using it you get to deal with the rogue and illegal behavior of everyone else. This includes hackers, who were early to the party. If you need assistance, please contact us.

Mitch

www.CyberCecurity.com

www.TurnkeyCybersecurityAndPrivacySolutions.com

Mitch@CyberCecurity.com

720-891-1663