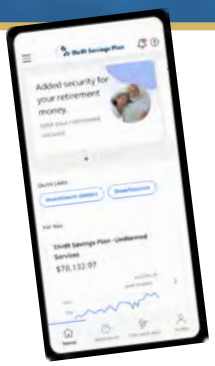
ARMY CRIMINAL INVESTIGATION DIVISION

CYBERCRIME PREVENTION

NEWS | JULY 2025

Authorized for widest release without restrictions.



Thrift Savings Plan (TSP) Fraud Tactics

The Thrift Savings Plan (TSP) manages nearly a trillion dollars in retirement savings for over seven million federal employees and service members. While convenient, mobile and online access increases your risk of cybercrime. Criminals are actively targeting TSP accounts for significant financial gain.

Recent Major TSP Fraud Incidents

April 2012: A cyberattack on a single TSP service provider workstation exposed the personal information (including Social Security numbers, financial account details, and bank routing numbers) of over 123,000 participants.

August 2022: A VA employee lost nearly $100,000 through a fraudulent hardship withdrawal due to system vulnerabilities and poor security practices.

March 2024: The State Department issued a warning about sophisticated phishing campaigns using malware to take over TSP accounts and redirect payroll deposits.

Phishing scams are rampant. Criminals impersonate TSP officials via email and social media, using urgent requests, "click-to-confirm" prompts, and malicious attachments to steal your login credentials.

Be wary of unsolicited investment opportunities. Per TSP.gov, TSP will never contact you about these or promote third-party counseling services. If you receive a call from anyone claiming to be a TSP representative, request a case number and then contact the Thriftline immediately.

Best Practices

Be Suspicious: Don't click on suspicious links in emails, text messages, or social media posts.

Secure Your Account: Never share your login information with anyone. Enable TSP's "account lock" feature as an added layer of protection and consider incorporating multi-factor authentication layer to mitigate risk of fraud.

Update Regularly: Keep your apps and devices updated with the latest security patches.

Log Out Completely: Fully exit your web browser after accessing your TSP account online. Doing so helps close your session completely and reduces the chance of someone gaining access through saved login data or browser history.

Download Safely: Only download the TSP mobile app from the official Apple App Store or Google Play Store.

Report Suspicious Activity: Contact the ThriftLine immediately at 1-877-968-3778 (PIN required) if you suspect any unauthorized activity. You can also report scams to the FBI's Internet Crime Complaint Center (IC3) at https://www.ic3.gov/.

If you are a victim of an email scam and affiliated with the Army, notify the Army Criminal Investigation Division via the Submit a Tip – Report a Crime website.

SCAN TO SUBMIT A TIP | REPORT A CRIME
OR VISIT https://www.cid.army.mil/Submit-a-Tip/

To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil