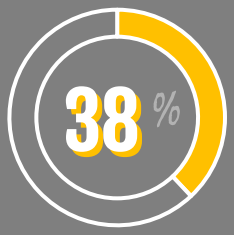
BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY I EMPLOYEE MANAGEMENT RELATIONS I THREAT ASSESSMENT & MANAGEMENT

Concerning ONLINE BEHAVIOR

INSIDER THREATS (InT) ON NETWORK SYSTEMS

Advances in network detection capabilities, including User Activity Monitoring (UAM), endpoint security, and User and Entity Behavioral Analytics (UEBA) bolstered by Artificial Intelligence (AI) tools, provide increased insight into concerning online behavior and enable the identification of previously difficult-to-detect behaviors and anomalous activities. These advanced analytic tools and capabilities bridge the gap between "human sensors" that observe physical offline behaviors and the corresponding concerning online behaviors bringing into focus the "whole person," identification of additional Potential Risk Indicators (PRI), and evidence of escalating behaviors used by multidisciplinary teams for complete contextualized risk analysis.



Concerning online behaviors and user agreement violations led to 38% of FY23 information security incidents within federal agencies[1].

TRENDS IN CONCERNING NETWORK BEHAVIOR

BEHAVIOR	RISK	DETERRENCE / MITIGATION
Expressing emotional distress online: Individuals may perform online searches, post online chats, or use AI tools to research psychiatric conditions/symptoms, and solicit advice.	Individuals with concerning behaviors associated with undiagnosed or untreated psychiatric conditions may struggle to cope with stressors which can contribute to increased risk.	Provide direct leadership engagement/support, when indicated, to the individuals to ensure they have resources for treatment of the expressed concerns and continue to monitor for escalating behaviors.
Using pornography/ sexting/fantasy forums: Individuals may use multiple avenues to circumvent system controls to mask their behavior while engaging in sexual content at work.	Sites that facilitate sexual content viewing can be foreign-based and may contain malware or harvest information that can lead to network/data compromise and render an insider vulnerable to blackmail and/or coercion.	Directly address the behavior with the individual. Ensure organizational policies include concrete language about illicit content, specifically regarding new technologies and software. Provide proactive education to the workforce about the inherent risk involved in accessing these sites.
Profanity, slurs, and angry comments: Individuals may write/post/text expressing their views about current affairs, work, or their home lives using derogatory, angry, and/or ominous language.	While expressing anger or personal views is typically protected, individuals who express *direct threats* toward a target or show escalation from *anger to action* may be showing signs of leakage of a plan to engage in violence, espionage, or sabotage.	Focus on addressing stressors and any grievances. Support the individual by connecting them with resources for managing anger (e.g. EAP). Use a trusted third party to communicate with and help the individual. Refer any direct threats or escalation to security and/or law enforcement.
Inappropriate use of AI tools: Users may engage with relational AI "chatbots" during the workday for role play, connection, and/or "therapy." Other concerning use is uploading sensitive information into AI tools (e.g., NIPRGPT) to facilitate work.	While the government is promoting the use of AI tools to improve efficiency, it's important this is done within a safe framework. Some commercial AI tools have platforms with foreign connection that may scrape for sensitive data or use data for leverage or compilation.	Ensure organizational security policies address integration of AI capabilities (e.g., ChatGPT, NIPRGPT, chatbots). Coordinate UAM and Security Operations Center (SOC) actions to enhance risk evaluation and management. Educate the workforce on emerging risks associated with these platforms and consequences for violations of policies.

Coming in November, DCSA is introducing a new podcast focusing on topics from the BTAC Bulletin.

1. Cybersecurity and Infrastructure Security Agency (CISA) (2023) *Computer Emergency Readiness Team Incident Report data FY 2023*

DITMAC DOD Insider Threat Management and Analysis Center

E-Mail Contact: dcsa.quantico.dcsa.list.ditmac-sme@mail.mil