Case Studies

U.S. Military E-mails Sent to Mali

A typo can lead to a cybersecurity incident. Over the span of a decade, millions of emails containing Controlled Unclassified Information (CUI) intended for the .mil email domain were mistakenly sent to the .ml email domain—the country identifier for Mali. Adversaries take advantage of human error in a practice called typosquatting, whereby they create legitimate looking websites for domains containing common typos.

Deepfakes Boost Social Engineering Tactics

The evolution of artificial intelligence (AI) tools makes it possible to readily create realistic fake audio and video of people, known as deepfakes. In one case, social engineers used emails and deepfake audio of a company's director to convince an employee to transfer $35 million. Always verify any suspicious contact using legitimate means.

Bogus Search Results to Scam You

Have you considered how the top results get there when using a search engine? Search engine optimization (SEO) techniques influence the results you get—and scammers use this to their advantage. Some travelers seeking airline customer service have been scammed by bogus phone numbers at the top of their search results. Be sure to evaluate the source of the information before clicking to ensure it's a legitimate site.

Contractor Sentenced to 45 Months in Prison

Daniel Hale is a former Air Force airman, National Security Agency (NSA) employee, and National Geospatial-Intelligence Agency (NGA) contractor. Hale used his legitimate access to classified national defense information to demonstrate his opposition to war and the use of drone warfare. He misused his access to take classified information and share it with journalists, resulting in the documents being published and publicly available.