# Daily Threat Intelligence Briefing

Today's threat briefing contains live links that connect you to the original source articles. You can see the real URL by hovering your mouse over the links and checking that they match the source articles. These links were taken straight from the website of the source article. Tyler Technologies has not checked these sites or links for security.

## News from Friday, June 26, through Sunday, June 28, 2026
## (Reported on Monday, Jun 29, 2026)

### Government

**Russian Intelligence Services Continue to Target Commercial Messaging Applications**
Read more at CISA

**Proposed US law would make AI risk reporting a legal obligation**
Read more at CSO Online

**Malware-Laced USBs Breach Japanese Military Networks**
Read more at GovInfoSecurity

### Financial Institutions

**Spoofed Fraud Call Nearly Costs Credit Union Member Thousands**
Read more at CUtoday

**FCC phone ID plan could end burner phones**
Read more at AOL

### Healthcare

**High-Severity Vulnerability Identified in OHIF Viewers DICOM**
Read more at HIPAA Journal

**Colorado Health Network; Kentucky Mountain Health Alliance Announce Data Breaches**
Read more at HIPAA Journal

**Minnesota Epilepsy Group; Campbell University; City of Middletown Announce Data Breaches**
Read more at HIPAA Journal

### Other

**Amazon Q Flaw Enabled Cloud Credential Theft via Malicious Repositories**
Read more at Security Week

**Malware authors subvert AI detection systems**
Read more at CSO Online

## News from Friday, June 26, through Sunday, June 28, 2026
## (Reported on Monday, Jun 29, 2026)

**Chinese Framework Powers 200,000 Scam Sites**
Read more at Security Week

**Data breach exposes up to 14.2 million email logins at six ISPs**
Read more at Bleeping Computer

**$3 Million Reportedly Stolen in Polymarket Hack**
Read more at Security Week

**Clean GitHub repo tricks AI coding agents into running malware**
Read more at Bleeping Computer