To: All Agents and Offices of WFG National Title Insurance Company
From: WFG Underwriting Department
Date: March 2, 2026
Bulletin No. NB 2026-02
Subject: Increased Cyber-Security Risk

Not to be political, but many Cyber Security Professionals are warning of heightened risk of retaliatory cyber attacks on U.S. critical infrastructure and financial institutions following the recent combat operations against Iran.

While we are all regularly battling business email compromise (BEC), fraudulent payoff alterations, data theft/extortion, and Ransomware, having a nation-state and its proxies engaging in the attacks dramatically increases the risk level.

Those same professionals have also suggested we might see an increase in attacks targeting our Software as Service Closing Systems, E-recording systems and County Interfaces.

Consistent with WFG's Agent 3.0 philosophy of sharing our best ideas with our agents, we are providing the guidance and specific steps given us by Bruce Phillips, SVP & Chief Information Security Officer, MyHome, a Williston Financial Group Company™. See his recommendations on the following page.

One interesting statistic– over 90% of successful cyber-attacks begin with a Phishing attack. So please refresh your staff training on not clicking on just any email or link.

Information Bulletins are designed to provide our agents with information we think will help in managing their business or just being better title professionals, but which does not rise to the level of being an underwriting mandate and are not within the scope of the agency agreement.

From: Bruce Phillips
SVP & Chief Information Security Officer
MyHome, a Williston Financial Group Company™

Over the last 24-48 hours, the United States and Israel have launched major, coordinated combat operations against Iran, striking leadership, missile, and air-defense targets across the country. Iran has responded with widespread missile and drone attacks across the region. In parallel, we are seeing the cyber domain emerge as an active front—reports of a near-total internet blackout within Iran following cyberattacks on media and government platforms, along with renewed activity and threats from Iran-aligned cyber groups targeting U.S. and allied organizations. The conflict remains fluid, and we should anticipate attempts to exploit U.S. businesses—especially those with high-value financial workflows and sensitive customer data.

Why this matters to our business
Our operating model—high-velocity wires, multi-party coordination, reliance on SaaS platforms/eRecording/county interfaces, and custodianship of sensitive documents—presents an attractive attack surface for business email compromise (BEC), fraudulent payoff alterations, data theft/extortion, and disruptive malware. We also carry interconnected vendor and county dependencies that can amplify operational impact if a third party is degraded or taken offline.

Immediate priorities (next 72 hours)

1. **Wire & transaction integrity**
    1. Enforce out-of-band callbacks (known numbers only) for all payoff, proceeds, and last-minute changes; two-person verification and VP approval for any exceptions.
    2. Run company-wide mailbox rule sweeps; block external auto-forwarding; increase monitoring for look-alike domains contacting escrow teams.
2. **Identity & access hardening**
    1. Enforce phishing-resistant MFA (no SMS/voice fallback) for finance, operations, IT admins, and anyone with wire authority.
    2. Tighten conditional access (geo-fencing, impossible-travel, legacy protocol blocks); audit and revoke unnecessary OAuth app consents.
3. **Backup & recovery readiness**
    1. Validate last known-good, **offline/immutable** backups for title plant, imaging, escrow accounting, policy production, and payroll.
    2. Rehearse manual closing contingencies and high-level recovery runbooks.
4. **Vendor & county dependencies**
    1. Obtain same-day attestations from Tier-1 vendors (MFA, EDR, DDoS protection, incident status, RTO/RPO).
    2. Pre-stage alternates (paper instruments, overnight checks) if any platform or county portal is degraded or geo-blocked.
5. **Detection & response focus**
    1. Elevate alerting for: new inbox rules, anomalous MFA prompts, OAuth grants, spikes in eDiscovery/SharePoint/OneDrive downloads, unusual SFTP/API pulls, and ransomware precursors (EDR tamper attempts, VSS deletions).
    2. Confirm 24×7 escalation paths and decision authority for wire holds, portal cutovers, and public communications.

What success looks like this week

1. No unauthorized wire movements: all payoff changes validated out-of-band.
2. 100% phishing-resistant MFA coverage for privileged, finance, and escrow roles.
3. Verified, restorable offline backups for all critical systems.
4. Tier-1 vendors affirmed and contingency workflows pre-approved.

We will continue to monitor the situation and adjust controls as needed.