



CAUTION



Cyberattacks Targeting Arkansas's Construction Industry

1. Construction has become *the* top hotspot for costly cyberattacks

With high-value financial transactions, complex supply chains, fragmented workforces, and lagging cybersecurity, **construction has become cybercriminals' favorite target**. Two analyses, one from ReliaQuest and another from NordLocker, ranked construction as the most targeted industry for cyberattacks. Attacks on construction firms, their partners, and their customers often range from **hundreds-of-thousands of dollars to a few million**.

Construction

226

Transportation

167

Wholesale Trade

138

Manufacturing

116

Retailers

105

Note: Cyberattack incidents remediated by ReliaQuest, by industry, avg. per year (2022–2023)

2. Million-dollar attacks are happening right here, right now in Arkansas

Hackers don't just target contractors. They also target their partners and clients. In late 2025, a cyberattack manipulated an otherwise real invoice from a real Arkansas-based construction company to **scam the Pine Bluff School District out of \$3.2 million**. These attacks — on both contractors and their clients — are more common than you might think. According to Microsoft, **600 million cyberattacks take place every single day**.

Fake Construction Invoice Fuels \$3.2 Million Cyberattack on Arkansas School District

3. The good news: Construction firms and their partners *are* fighting back

Fighting back starts with fundamental cybersecurity safeguards: strong passwords, multi-factor authentication, security-awareness training. Often, though, it takes advanced cyber protections to prevent advanced cyber threats — and that's when you need a local, trusted cybersecurity partner.

- ✓ Strong passwords + MFA
- ✓ Security awareness training
- ✓ Local cybersecurity partner

PREPARE TODAY, OR BE A VICTIM TOMORROW