![Anchor Network Solutions, Inc. logo]

# CYBER CRIMINALS INCREASE EFFORTS DURING SUMMER MONTHS

**Cybercriminals don't take vacations.**

In fact, summer is a prime time for attacks. While teams are out of office and vigilance dips, cybercriminals ramp up efforts—targeting distracted individuals, organizations with lighter staffing, and unsecured networks.

## WHY IS SUMMER PRIME TIME FOR CYBERATTACKS?

- **Reduced security staffing:** Many businesses operate with fewer IT and security personnel during summer vacations, leading to slower response times and more overlooked threats.
- **Relaxed vigilance:** Whether on vacation or just in summer mode, people tend to let their guard down—perfect conditions for phishing and social engineering attacks.
- **More public Wi-Fi use:** Traveling employees and families using hotels, airports, or cafés often connect to unsecured networks.
- **Travel-themed scams:** Fake booking confirmations, vacation deals, or flight cancellations are common phishing bait.
- **Higher online activity:** From online shopping to booking getaways, summer means more digital behavior—giving attackers more opportunities.

## WHAT CAN YOU DO?

- **Stay alert:** Be cautious with unsolicited messages, especially those involving travel or urgency.
- **Verify before you click:** Always double-check links and sources before entering credentials.
- **Strengthen your defenses:** Tools like anomaly detection, behavioral analytics, and real-time alerts can help protect your organization.
- **Keep security top of mind:** Threats don't take time off—even if your team does.

### STATISTICS

**3.5k+ weekly attacks** on the education sector

**58%** increase in data-stealing malware attempts in 2024

**10%** of ransomware victims are in healthcare

**$200K** median ransom payment in 2024

**AnchorNetworkSolutions.com**