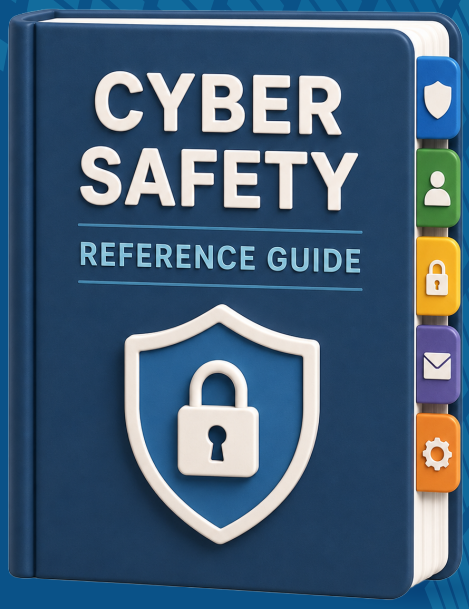
Intrada TECHNOLOGIES

# CYBER SAFETY QUICK REFERENCE GUIDE




Cyber threats often arrive disguised as everyday messages, calls, and pop-ups, which makes staying alert one of your strongest defenses. The tips below give you simple, practical steps to spot the warning signs and respond with confidence. Keep this guide close and lean on your Intrada team whenever something doesn't feel right—we're here as an extension of your own team. A few seconds of caution can prevent a costly mistake.

## Post this by your desk, or share it with your team.

1. Pause before you click. Hover over links to verify their destination.
2. Be wary of urgency. Messages that pressure you to act immediately are a red flag.
3. Confirm money requests. Verify payment or account changes by phone using a trusted number.
4. Don't trust caller ID. Voices and numbers can be faked—always call back to confirm.
5. Protect passwords and codes. Legitimate companies will never ask for them.
6. Close suspicious pop-ups. Don't call the number displayed or grant remote access.
7. Check sender addresses. Look for minor misspellings or unusual domains.
8. Use strong, unique passwords and enable multi-factor authentication whenever possible.
9. Trust your instincts. If something feels off, ask your IT team before taking action.
10. Report suspicious messages. Alerting others can help prevent additional attacks.



31 Ashler Manor Drive
Muncy, PA 17756

intradatech.com
800-858-5745

Exceeding Expectations.