Here are some things you **CAN** do:

- Ensure you're using strong, unique, and at least 14-character passwords or passphrases for each account. This might sound daunting but think of it like having a unique key for every door in your house.
- Utilize Multi-Factor Authentication (MFA) on every account where it is available.
- Verify that user accounts which don't need administrator access do not have administrator roles. Check with your IT support team if you don't know what this means – it is important!
- Hover over every link to see where it would take you before you click on it.
- Verify the authenticity of an email before clicking a link, opening an attachment, responding, or providing any requested information.
    - Determine the sender's telephone number from a source other than the email (like the company website for example).
    - Call and verify.
    - Be particularly careful when replying to emails on your mobile phone—it can be difficult to see the actual email address of the sender.
- Stay vigilant and be aware of common tactics used by attackers, like creating a sense of urgency, pretending to be unavailable for a call, or asking for help in a suspicious way. If something doesn't feel right, trust your instincts, and double-check before taking any action.
- Patch all your systems. Check with your IT support team if you don't know what this means—it is important!
- Review business practices to discover any risks and identify any changes to make.
- Educate ALL employees on their security responsibilities.

- Have a business continuity plan, an incident response plan, and a routine to test your backups regularly.

- If anything seems not right, reach out to your IT support team immediately!

This list is **NOT** all-inclusive. This is just the new minimum recommendation for what you **MUST** be doing. This list might also have included implementing intrusion detection and response solutions, email spam and security solutions, reviewing all accounts daily for use and rights, and more.
We want to express our sincere gratitude for your additional diligence and heightened awareness. We understand that keeping up with your daily work while staying vigilant against these attacks can be challenging, but we applaud your efforts. By being extra cautious, we can work together to better protect ourselves and our business partners during this unprecedented era of cyber threats.

We all have a very big stake in what happens in our industry, and we all need to be part of shaping the future. We all need to evolve and adapt—this means changing both our individual behaviors and our company practices. It's time to embrace new technology and updated security protocols to enhance and protect every single transaction.

Finally, we want to let you know that many of our industry partners, underwriters, vendor partners and ALTA have provided excellent resources for reviewing and implementing cybersecurity measures. Be sure to take advantage of these resources to keep your systems secure and your customer information safe. We urge you all to work with your IT security providers to address these issues as soon as possible.

You'll find information and resources developed by our work group on **ALTA's website** to support your efforts.