

INTERNET SECURITY

Best Practices



Following some simple steps to help enhance your internet security can help you get the most out of your Internet service. While EPB is not responsible for the internet security practices of our customers, we recommend working with your IT professional to ensure you are following recognized best practices for secure internet browsing. Use the following to help you get started.

- 1. Encrypt all data to add further protection in the event of equipment theft or malfunction.**
- 2. Establish and implement a password security policy that requires personnel to regularly change email and other system passwords.**
- 3. Limit employee access to and use of removable media such as USB drives and external drives.**
- 4. Use Spam filters on email systems.**
- 5. Install internet security software and update it regularly.**

We offer McAfee® LiveSafe™ security software to our customers as an add-on. McAfee® LiveSafe™ is a well-known security software that you can download and use to help protect your computer from hacking, viruses and malware while accessing the internet. You can install McAfee® LiveSafe™ using the download link and access key provided by your EPB representative.
- 6. Educate all employees on internet security practices, policies and best practices for your business.**
- 7. Create a cyber security plan for your business.**

(If you need assistance, check out the Federal Communications Commission Small Business Cyber Planning tool at [fcc.gov/cyberplanner](https://www.fcc.gov/cyberplanner).)