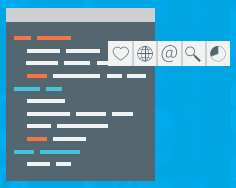
Top 7 Tips
for Cyber Protection

1 Know Your Data

Know where and how your data is stored. Is it kept in-house, at an offsite data storage facility, or outsourced to a third party? Many transaction components require businesses to send customers' personally identifiable information, such as credit card information for payment processing, to a third party. Consider all the elements of your data when evaluating your cyber coverage needs.

2 Know Your Software

Businesses often utilize third-party software programs to pass or retain data. Those businesses may maintain liability should a breach occur. Know how the programs work, who has access to the program, and what security measures are in place.



3 Secure Your Technology

Security measures aren't just for your desktops and servers. Consider all devices that retain or have access to data such as smart phones, home computers, tablets, and other portable devices. Such devices should be password protected and data transmitted to and from them should be encrypted.

4 Practice Security Measures

Put into place routine security measures such as updating passwords, requiring the installation of software security patches in a set period of time, using firewalls, and making backups of important business data.

5 Control Administrator Access

Limit the number of individuals who have privileges to run, change or control critical business applications.

6 Train Employees

Educate employees on the risks of providing personal information on social media, the risks of catching computer viruses from suspicious email links or websites, and the risks of using company resources such as laptops on public networks.

7 Monitor, Monitor, Monitor

Ensure that internal security measures are being followed, anything unusual is investigated, and the business is routinely updating protocols for cyber breaches.

The Partnership

For more information:

PIA® PROFESSIONAL INSURANCE AGENTS