Cybersecurity Self Assessment

St. Charles
Chamber of Commerce

You can use this assessment in two ways:

OPTION 1 - Check boxes for YES answers, and calculate your points. The best score is 380. A score below 360, or several missing check marks, indicates the need for improved security.

OPTION 2 - Use this assessment as a general guide for your staff and your IT team/provider. Don't worry about the points!

Best Practices

□ Do you have a well-documented policy for all of the following? Acceptable Use, Internet Access, Remote Access & BYOD (Bring Your Own Device), Email & Communications, Disaster Recovery, Encryption & Privacy (10 points per item)

□ Do you use modern, valid, and up-to-date software for all purposes and regularly apply security patches? (70 points)

□ Do you hold regular employee training that covers the latest in data security? (70 points)

User Security (10 Points Per Item)

□ Do you require regularly updated, complex employee passwords?

□ Do you regularly audit and disable outdated accounts?

□ Do you avoid shared accounts and passwords?

□ Do employees check that all websites are secure when sharing company information or passwords?

Email Security (10 Points Per Item)

□ Do you have an email security filtering solution? Filtering solutions protect against malicious emails you can't recognize

□ Does your email policy state that sensitive information won't be sent over email? e.g., passwords, banking info, and anything else most safely communicated over the phone

Website Security (10 Points Per Item)

□ Is your SSL certificate up to date?

□ Do you use a secure web hosting company? They should isolate hosting accounts, maintain server logs, and back up your site regularly.

Network Security (10 Points Per Item)

□ Do you use a commercial-grade firewall?

□ Do you password-protect your router and make internal Wi-Fi accessible to employees only? (Configure guest networks separately.)

□ Do you use VPN (virtual private network) technology for remote access to the office?

□ Do work computers automatically lock the screen and require logging back in after a period of inactivity?

□ Do you limit and log access to the physical locations or rooms containing network devices (such as switches) and any in-house servers?

□ Do you store data securely in cloud software, using password best practices for accessing this data?

Ask an IT Expert (10 Points Per Item)

□ Are your firewalls running the most current firmware, considered next generation hardware, and covered by manufacturer warranty or manufacturer-contracted support?

□ Do you regularly scan your network for vulnerabilities? e.g., viruses, malware, and unauthorized devices

□ Do you store passwords as encrypted values?

□ Do you perform regular backups of data and configurations, as well as test restore?

Your Total: