# ESSENTIAL CYBERSECURITY CHECKLIST FOR BUSINESSES

## SPAM EMAIL

Most attacks happen via email. Make sure you are utilizing a security service designed to reduce spam.

## PASSWORDS

Apply security policies to the network, such as enhanced password policies and limited user access.

## SECURITY AWARENESS

Users are the biggest threat to security. Train them on data security best practices, spotting email attacks and company policy.

## ADVANCED ENDPOINT SECURITY

Security is built in layers. Utilize software like OpenDNS, Webroot and Malwarebytes to protect yourself from cyber attacks.

## MULTI-FACTOR AUTHENTICATION

MFA adds an extra layer of protection to ensure even if your primary password is compromised, your data stays safe.

## COMPUTER UPDATES

Make sure you have an automatic service for critical updates and patches.

## DARK WEB RESEARCH

Know if any of your passwords or accounts are for sale on the dark web so you can be proactive in preventing a data breach.

## FIREWALL

Ensure your network parameters are safe to prevent unauthorized Internet traffic from reaching your computer.

## ENCRYPTION

Encrypt all your sensitive data so that if your hardware falls into the wrong hands, your data remains protected.

## BACKUP

Backup locally, backup to the cloud and make sure you are testing those backups often. That way your business stays functioning in the event of a disaster or downtime.

## CYBER INSURANCE

Cyber damage and recovery insurance policies are available as a final piece of protection for your business.

## SECURITY ASSESSMENT

Establish a baseline and discover where your vulnerabilities are.

Call us at 512.472.6000