Securing Your Startup's Infrastructure

Your IT Game Plan/Checklist

Protective Tools

- ☐ Determine your password policy and apply it
  - ☐ Turn on MFA (multi-factor authentication), ensure all passwords are at least 12 characters, and include a number, symbol, and special character.
  - ☐ Enroll in a password manager like 1Password or Keeper and create unique passwords - no duplicates!
- ☐ Encrypt your workstations
  - ☐ Utilize a central management system like Jamf or Intune
  - ☐ Enforce encryption across all workstations and store recovery keys in a secure location
- ☐ Invest in centrally-managed anti-virus software
- ☐ Install firewalls on your network
- ☐ Require employees use an internal VPN (not third-party) when accessing sensitive company data
- ☐ Use Directory as a Service platform like JumpCloud or Okta to manage user access
- ☐ Review anti-spam configuration and configure email authentication methods to prevent phishing attacks

But wait there's more!

tech. superpowers

Call: 617 267 9716
Email: business@tsp.me
500 Harrison Avenue, Boston MA 02118

Process

- ☐ Proper documentation - Write out all the steps in full, so they are always completed consistently and correctly, regardless of who's handling. Start with the following:
  - ☐ Onboarding
  - ☐ Offboarding
- ☐ Easy-to-follow SOPs
  - ☐ Create an SOP for any tasks your organization regularly performs. No matter how simple the task, having a standard procedure on how to perform it will save you time and money in the long run. This will allow smoother transitions between employees and helps to keep your operations running in the event someone is out of the office for an extended period of time.

Training

- ☐ Determine what style training is best for your organization (in-person/synchronous, virtual/asynchronous)
  - ☐ In Person/synchronous -> You can create your own training or work with outside MSP to provide training
  - ☐ Virtual/asynchronous -> KnowBe4
- ☐ Determine if you need to expand securing testing to phone, SMS, or in-person (i.e. physical security)
- ☐ Create a Slack or Teams channel to share phishing emails that you receive
- ☐ In-person reviews of wins and misses on your phishing platform
- ☐ Conduct reviews and audits of active or successful attempts to improve your awareness

People

- ☐ Assign a specific person in your company to be responsible for security posture, policy, and processes
- ☐ Determining internal and external resources for IT
- ☐ From there, it's up to your contacts to help make sure that process is implemented consistently
- ☐ Security discussions should be open and honest - shame free - across your organization.
- ☐ Foster a culture of security, not taking the easy way out.

Overwhelmed? Many organizations partner with an MSP (managed service provider) to help them build out their processes, ensure they're conforming to compliance requirements, and perform onboarding and offboarding services. Tech Superpowers has been working for decades with scaling Boston-based startup ventures.