CYBERSECURITY IN THE AGE OF CORONAVIRUS

PRESENTED BY

BEN GLASS – PRESIDENT BESPOKE TECHNOLOGY GROUP

JOHN PIRKOPF – IT CONSULTANT BESPOKE TECHNOLOGY GROUP

OUR EXPERIENCE

- Client's relationship with IT and security before the virus had a big impact on outcome
- Working with your IT provider is a partnership – Trust is key
- Clients who viewed IT as an investment (vs a cost/liability) were better prepared
- Clients with a "culture of security" were at an advantage
- There are tons of Coronavirus scams. Be skeptical.

REMOTE ACCESS AND SECURITY

- Firewall and VPN access – Some firms were more ready than others
- Hardware – Office vs Home equipment
    - New life for old hardware
- Bandwidth, passwords, and IT support
- Passwords – Change them, make them longer, turn on dual factor authentication when possible.
- Security Software

THREAT PROTECTION AND PREVENTION

ANTIVIRUS

- Good antivirus software is essential.
- Antivirus software protects your workstations and servers from malicious programs.
- Along with other tools, antivirus can identify and quarantine dangerous programs that find their way onto your network.

ANTIMALWARE

- Monitors your network resources for abnormal behavior and aims to arrest any programs that are behaving abnormally.
- One of the most common types of malware attacks is one where your network will be encrypted, and cyber criminals will demand payment in exchange for a key to decrypt your data.

SPAM FILTERING

- Traditional spam filters compare incoming email messages to a known list of dangerous or "spammy" addresses or attachments and will reject the messages before they get to your computer.
- Newer spam filtering services offer much more. These services test programs and links before allowing messages through.

THE HUMAN FACTOR

- Develop a security-centric culture
- Educate your employees about risks
- Create a culture where people are cautious and feel comfortable reaching out for help if/when problems arise
- Develop clear policies, especially when it comes to money
- It isn't a question of **if**, but **when** something will happen

SOCIAL ENGINEERING IS GETTING SERIOUS

- USB Drops - Loaded with malicious software
- Phone Based Phishing – Targeted to solicit information
- Vishing - Targeted email action to have user call a local number
- Web-based phishing - Targeted email with action to have user visit a website
- Email-based phishing - Targeted email with an action to have user respond with info
- People are taking advantage of Coronavirus

BUSINESS CONTINUITY, BACKUPS AND DISASTER RECOVERY

- Technical security is great, until someone mistakenly clicks on a link, inserts the wrong USB drive, or clicks on the wrong program
- Have a plan
- Have good backups
- Business continuity and disaster recovery – How long can you afford to be down

THANK YOU!!!

TECHNOLOGY GROUP

Ben Glass Ben@BespokeTechGroup.com

John Pirkopf John@BespokeTechGroup.com