

Understanding What's Important in Today's Digital Economy

This document serves as further education to important topics related to your business. Simply understanding the basics and how each relates to your company can help improve your operations run more efficiently in today's digital economy.

Cyber Security & Network Administration

Cyber security is the technologies, processes and procedures designed to protect networks, devices, programs and data from unauthorized access and cyber attacks. You may also hear it referred to as 'information technology security'.

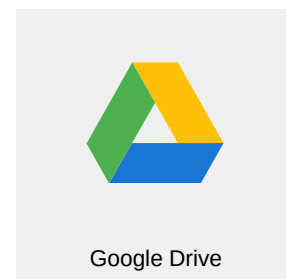
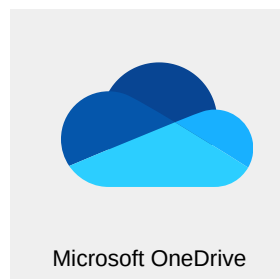
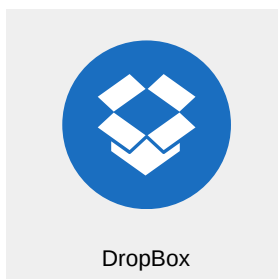
Why is cyber security important? With an increasing number of users, devices, and programs in the modern enterprise, combined with the increasing deluge of data - *much of which is sensitive or confidential* - the importance of cyber security continues to grow.

Network Administration is the operational tasks that help a network run more smoothly and efficiently. Tasks such as evaluating network infrastructure, daily backups and intrusion detection are vital to a company's security and performance.

What is the Cloud?

Sometimes perceived as a mystery, "the cloud" refers to servers that are accessed over the internet. The cloud allows users to access and share files and applications from any device. Typically in a cloud environment, files are more secure and users are able to collaborate more efficiently.

EXAMPLES OF CLOUD STORAGE COMPANIES



Why vulnerability scanning and patch management?

Vulnerability scanning detects and identifies weaknesses in the IT infrastructure. It is a way to see whether the network has any loopholes that can make it easy for attackers to penetrate.

Patch management is the process of managing a company's network of devices by installing all missing patches to ensure these devices are up-to-date.

Vulnerability scanning coupled with patch management enables a company's IT system to proactively mitigate the risk of cyberattacks from occurring.

What are phishing scams and how to detect & stop them?

A phishing scam is a fraudulent email or text message that appears to come from reputable organizations such as internet service providers, universities, banks, social networking sites, email providers, software vendors, etc. Then a scammer uses the collected information to open new accounts or invade the consumer's existing accounts.

HOW TO DETECT PHISHING SCAMS

- Check for misspelled email addresses
- Story telling with a call-to-action
- Message creates a false sense of urgency
- Poorly written email or text

HOW TO STOP PHISHING SCAMS

- Don't click on any attachments or links
- Ensure your computer's software is up-to-date
- Update all apps on all devices
- Use multi-factor authentication

The impact backups have on your business

Backing up your company's data on a regular cycle is important in order to have a secure archive of important information just in case something happens. Loss of data and other important information happens to companies everyday. It doesn't discriminate against large or small businesses either.

Backing up your data also improves productivity, customer relationships, various audits and more! This should be standard practice for every business in every industry.

CYBER TECH CONNECTION

Cyber Tech Connection is a Managed IT Service Provider that helps deliver complete technology services to small to enterprise businesses. With over a decade of experience, our comprehensive suite of IT solutions enable companies to run more efficiently and profitably.

CONTACT US

(800) 218-9471

cybertechconnection.com

team@cybertechconnection.com



Veteran Owned