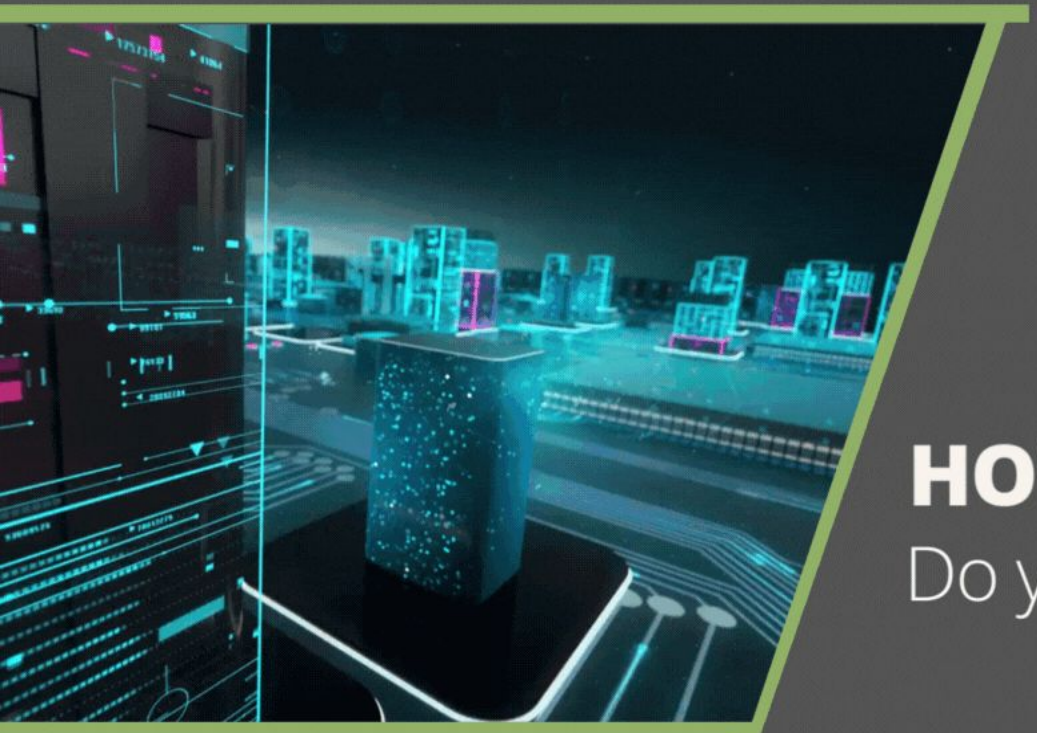


HOW GOOD IS YOUR IT?

Do you really want to know?

Key Takeaways

1. Learn a little more about technology in your business. By the end of the session you should understand some key things about technology in the business.

2. Learn about some new services that you could leverage in your business

3. How vulnerable are you?
   With what you have learned, let's assess how vulnerable you are.

Big Idea

Technology is not magic and a little knowledge can go a long way to demystifying and understanding it.

How Good is your IT?

ABOUT THE SPEAKER

SCAN ME

VITTORIO “VICTOR” CALABRESE

President | Author |Speaker | Consultant

Why is **TECHNOLOGY** important to your business?

Security

Automation

Efficiency

IT SERVICES

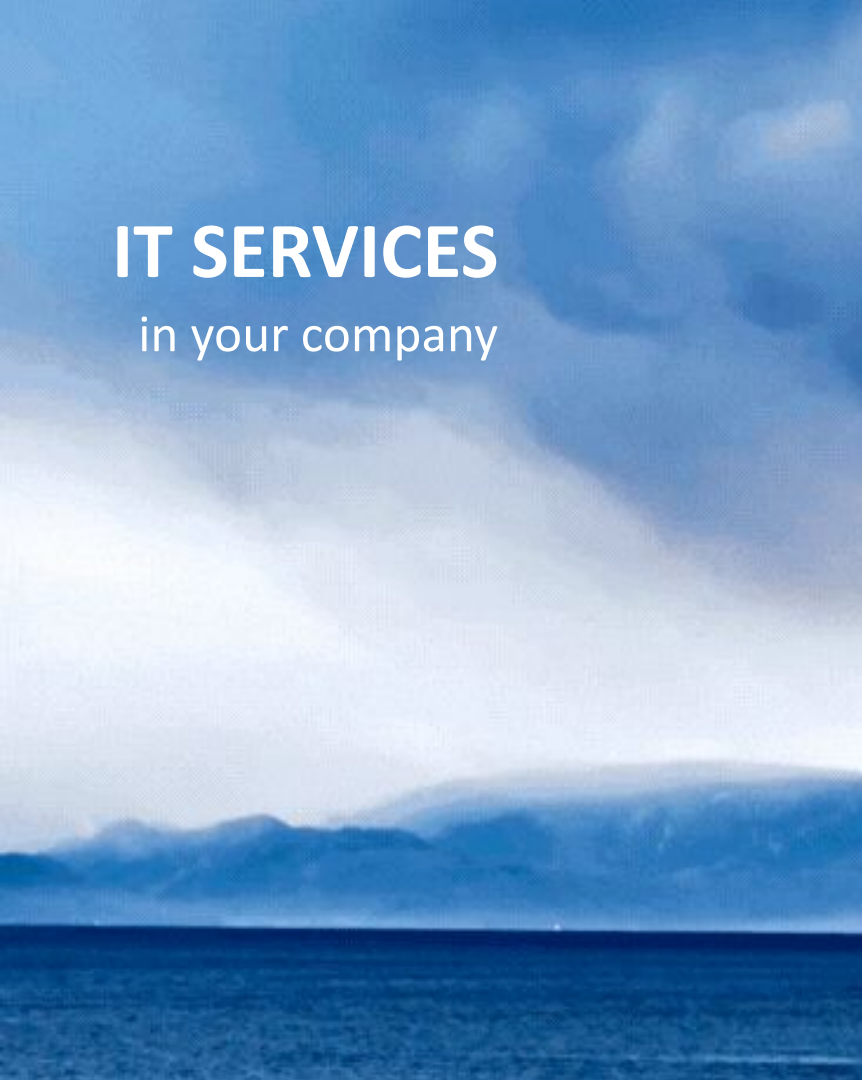
in your company

ISP

(INTERNET SERVICE PROVIDER)

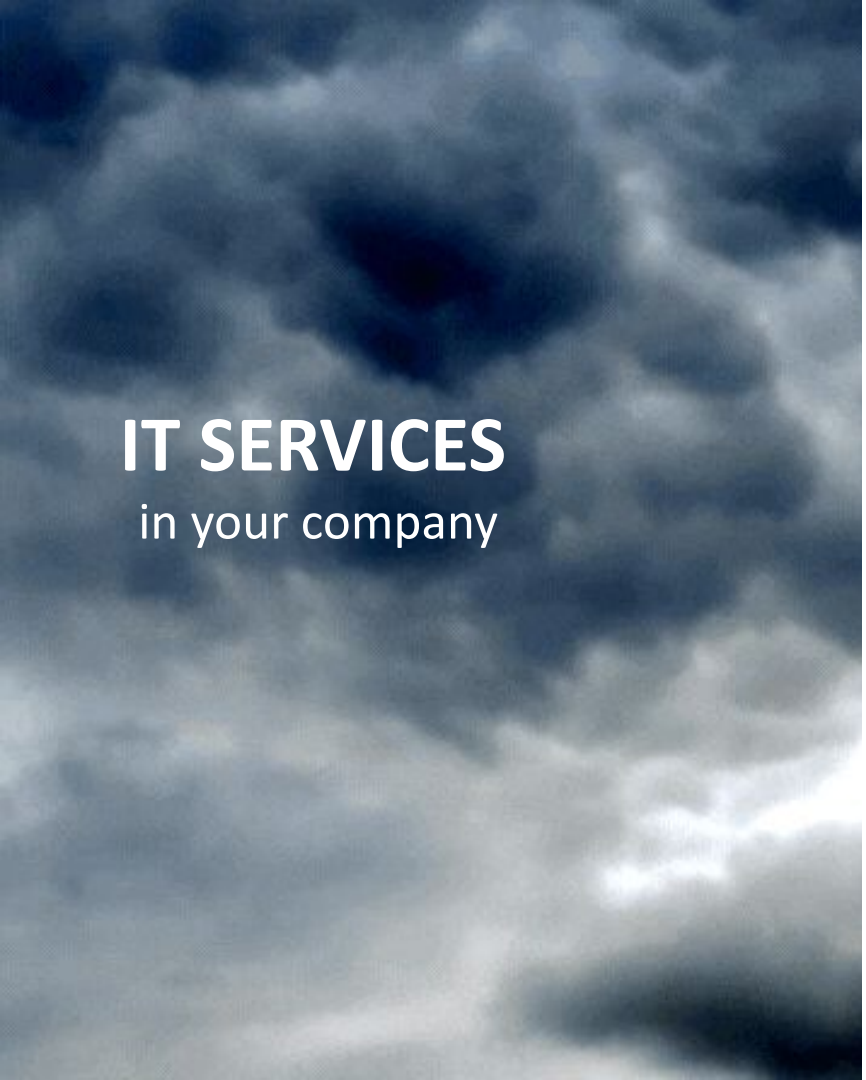
TELEPHONE

OFFICE SUITE



INTERNET SERVICE PROVIDER (ISP)

An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. ISPs can be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.



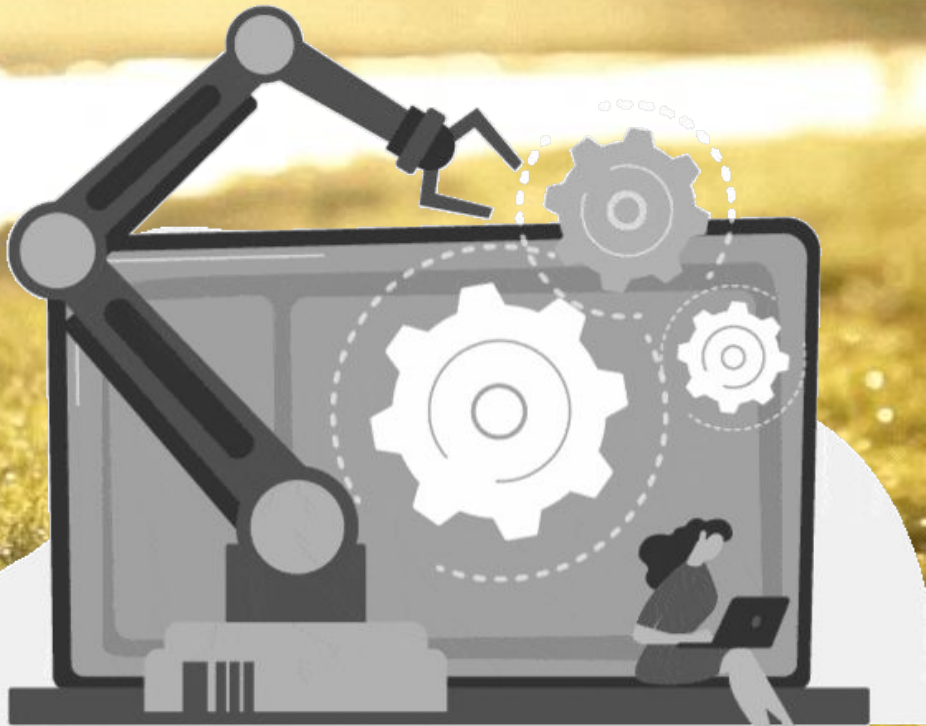
TELEPHONE

A telephone is a telecommunications device that permits two or more users to conduct a conversation when they are too far apart to be heard directly.

OFFICE SUITE

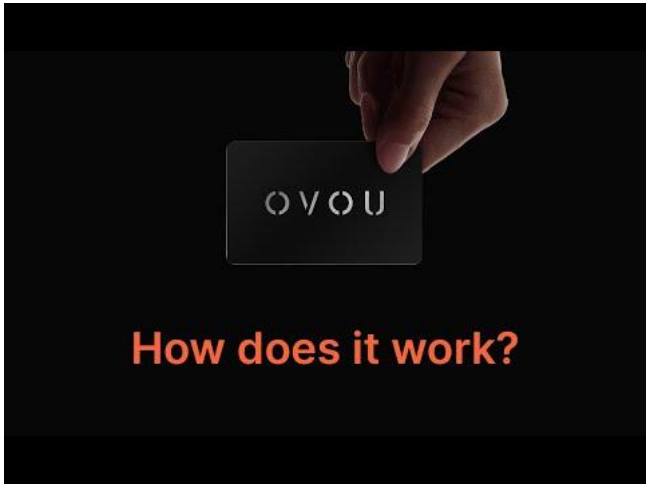
An office suite is a collection of productivity software usually containing at least a word processor, spreadsheet and a presentation program. There are many different brands and types of office suites. Popular office suites include Microsoft Office, Google Workspace and LibreOffice.

Efficiency & Automation



Efficiency/Automation

OVOU



OVOU smart business card helps you build and nurture new connections.

It uses NFC (Near Field Communication) and QR technology to share OVOU Profile with people you meet.

Efficiency/Automation

EMAIL SIGNATURE

An email signature is an important way of strengthening your personal image or brand identity in everyday communication. A professional email signature creates a good first impression and lets you share much more than just your contact info.

exclaimer

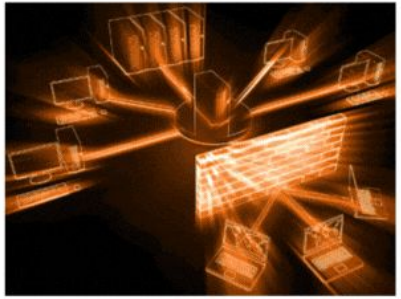
What is a **NETWORK**?

A **computer network** is a set of computers sharing resources located on or provided by network nodes. The computers use common communication protocols over digital interconnections to communicate with each other. These interconnections are made up of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies.

NETWORK

Router

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet.



Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Wireless Access Point (WAP)

In computer networking, a wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.

Switches

A network switch (also called switching hub, bridging hub, and, by the IEEE, MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

What is a **SERVER**?

In computing, **a server** is a piece of computer hardware or software (computer program) that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model.

Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers.

TYPES OF SERVER

ACTIVE DIRECTORY

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

A network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

FILE SERVER

Shares files and folders, storage space to hold files and folders, or both, over a net

APPLICATION SERVER

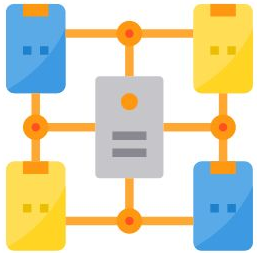
Hosts applications allowing users on the network to run and use them, many times without having to install a copy on their own computers.

SaaS

TYPES OF SERVER

Web Server

Hosts web pages. A web server is what makes the World Wide Web possible.



Phone server

Software designed for modern-day smartphones to host personal web servers, through the use of open source software.

Access Control Server

In the fields of physical security and information security, access control (AC) is the selective restriction of access to a place or other resource, while access management describes the process.

What are **End-User-Devices?**

An **end user device** is a personal computer (desktop or laptop), consumer device (e.g., personal digital assistant (PDA), smart phone), or VR Devices. Today we are also starting to see more IoT devices that can be considered end-user-devices.

END-USER DEVICES

PERSONAL COMPUTER (PC)

PHONE

TABLET

Internet of things (IoT)

The Internet of things (IoT) describes physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

What's the difference?

DISASTER RECOVERY

VS

BACKUPS

BACKUPS

In information technology, a **backup**, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

DISASTER RECOVERY

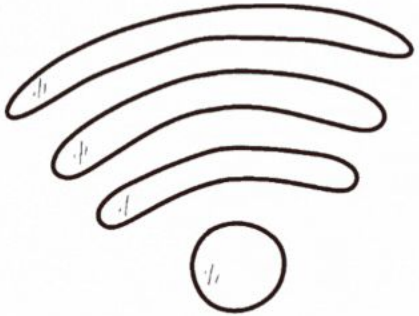
Disaster recovery involves a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Disaster recovery focuses on the information technology (IT) or technology systems supporting critical business functions.

Efficiency & Security

Efficiency/Security

Who has issues with **Wi-Fi** in their office or home?



Efficiency/Security

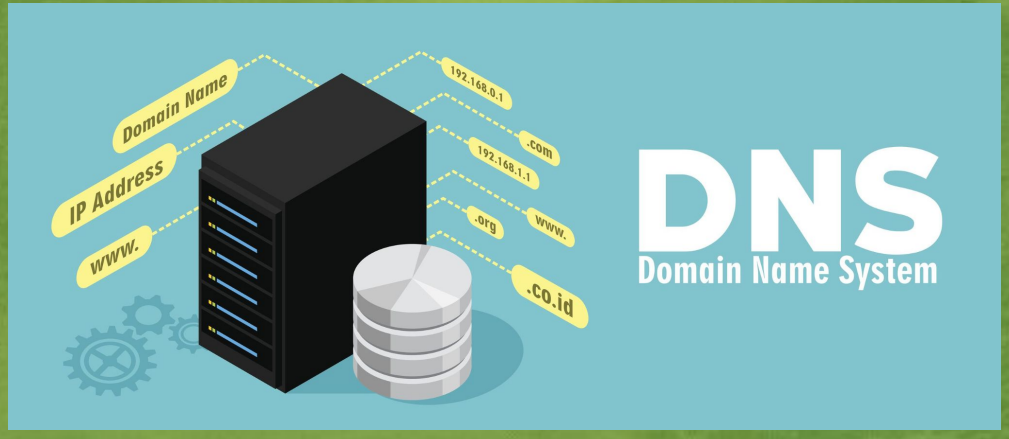
eero works seamlessly with your existing internet service provider, so you can set up your wifi in minutes. Simply download the app, plug your eero router into your modem, and find out where to best place your eero devices for the ideal connection.

eero's patented TrueMesh technology intelligently routes wifi traffic. So you can say goodbye to drop-offs and dead spots with a reliable network optimized for your usage and needs.


15:00

What is **DNS**?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com.



How does email **Work**?

Email are messages distributed by electronic means from one computer user to one or more recipients via a network.

Phishing Attack Red Flags?

Attackers will use any lies necessary to trick you:

- Requests for personal information from seemingly trusted sources, like your bank or IT department
- Unexpected QR Codes via email or text message
- Urgent requests for things like wire transfers or large gift card sums, seemingly from company executives
- Tricks to get you to share your two-factor authentication token or code
- Lookalike social media notifications, like LinkedIn connection requests
- Fake package delivery notices from companies like Amazon
- Great offers from merchants or prizes for filling out surveys or clicking certain links
- Scare tactics like IRS fines or account suspension

Making It Look Real

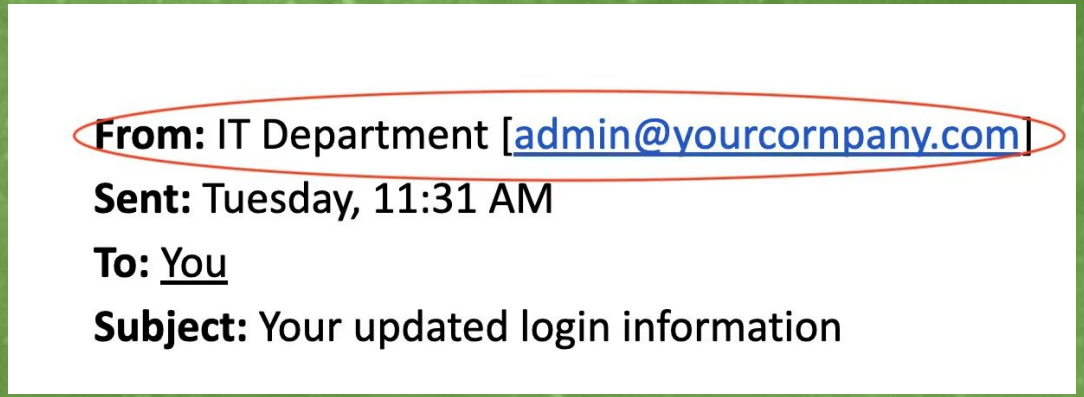
The Following Email Contents are Easily faked:

- Sender Address (spoofing)
- Stolen Graphics (download and rehost)
- Email Signatures (copied from a legitimate email)
- Disguised Links (made to appear legitimate, but link to malware)

Spoofed Email Addresses

Criminals will go to great lengths to make it look like the sender of the email is a valid and trusted source. Very often, they will spoof the addresses of your company executives or client and vendor relationships. Targeted attacks like these are called Spear Phishing.

It's always prudent to look at the sender's actual email address and ensure it's the person you're expecting it to be.



Stolen Graphics

It's very simple for email scammers to swipe real emails from trusted senders. This means that graphics and logos can look exactly like the valid artwork.

In fact, it’s EASIER to just copy the real logos. They’re criminals, after all!

Copied Signatures

While it adds a lot of credibility, email signatures are remarkably easy to copy. They can look exactly like the real thing from your CEO or any other colleague or contact.

Don't be fooled by this simple tactic!

Disguised Links

The text for a link can be completely unrelated to the actual website URL.

Always be sure to check the real domain by hovering your mouse over the link. On most browsers, this shows you the underlying link address, known as the URL (Uniform Resource Locator).

For an added layer of safety, you can often go directly to the website to get the same information, rather than clicking on the link. For example, rather than clicking the link in an emailed connection request from LinkedIn, simply go to the app on your phone or to linkedin.com on your browser. If it's a real request, it'll be waiting for you there!

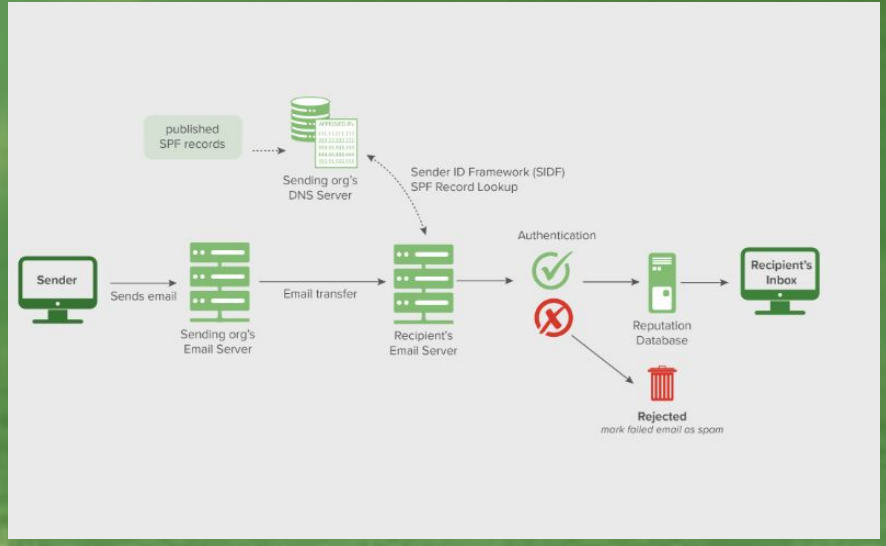
What is **Email Security**?

Email security involves various layers including:

1. SPF - Sender Policy Framework
2. DKIM - DomainKeys Identified Mail
3. DMARC - Domain-based Authentication, Reporting and Conformance
4. Filtering
5. Installed applications

Sender Policy Framework (SPF)

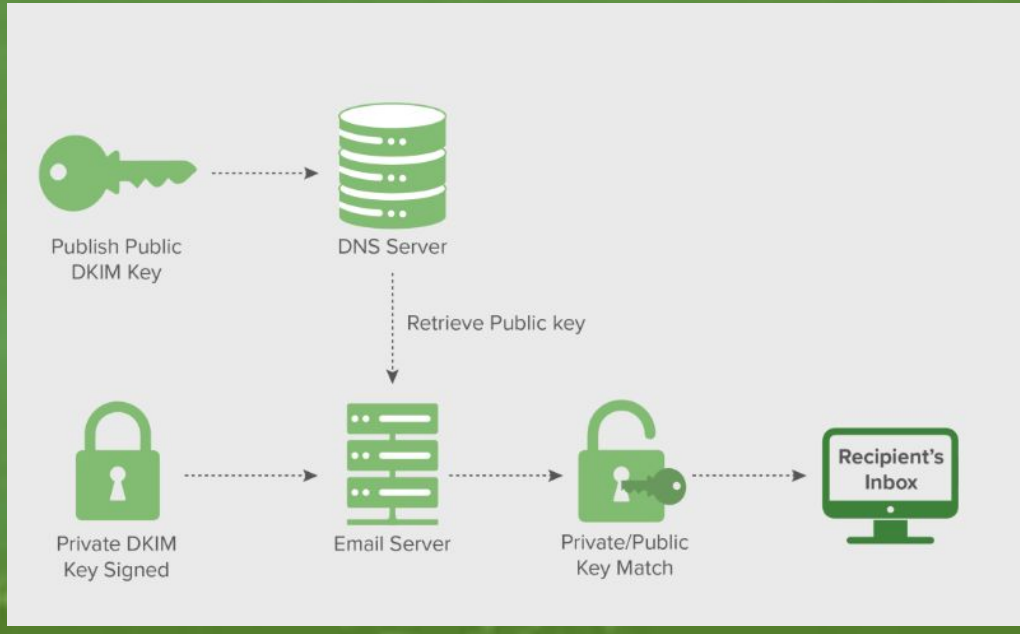
SPF (Sender Policy Framework) is an email authentication protocol that domain owners use to specify the email servers they send email from, making it harder for fraudsters to spoof sender information



@ IN TXT “v=spf1 a include: spf.google.com ~all”

DomainKeys Identified Mail (DKIM)

DKIM (DomainKeys Identified Mail) is a protocol that allows an organization to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. DKIM record verification is made possible through cryptographic authentication.

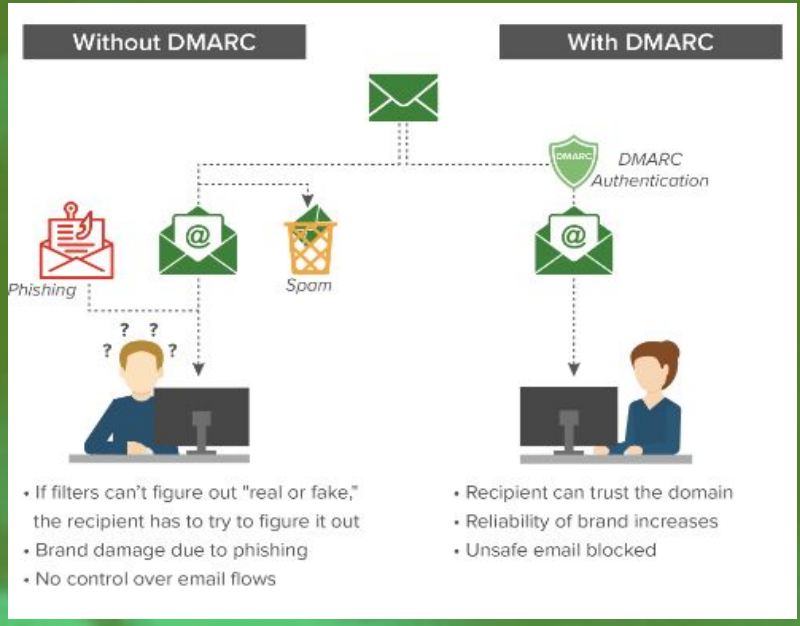


big-email._domainkey.example.com. IN TXT “v=DKIM1; p=76E629F05F709EF665853333EEC3F5ADE69A2362BECE4065 8267AB2FC3CB6CBE”

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a technical standard that helps protect email senders and recipients from spam, spoofing, and phishing.

_dmarc.mydomain.com. IN TXT “v=DMARC1\; p=none\; rua=mailto:dmarc-aggregate@mydomain.com\; ruf=mailto:dmarc-afrf@mydomain.com\; pct=100”



Security

Security

91%

of cyberattacks start with an email.

85%

of organizations were hit by a phishing attack in 2020.

1 in 7

organizations experienced an account takeover in 2022.

$200,000

average ransom fee paid in 2020.

Barracuda
Your journey, secured.

Email attacks are getting more complex and dangerous.
Many email threats today use social engineering tactics to target users and bypass email security gateways. You need to stay ahead of cybercriminals to protect your business and data.

Security

With DMARC you can tell the world how to handle the unauthorized use of your email domains by instituting a policy in your DMARC record.

The three DMARC policies are:

p=none

Monitors your email traffic. No further actions are taken.

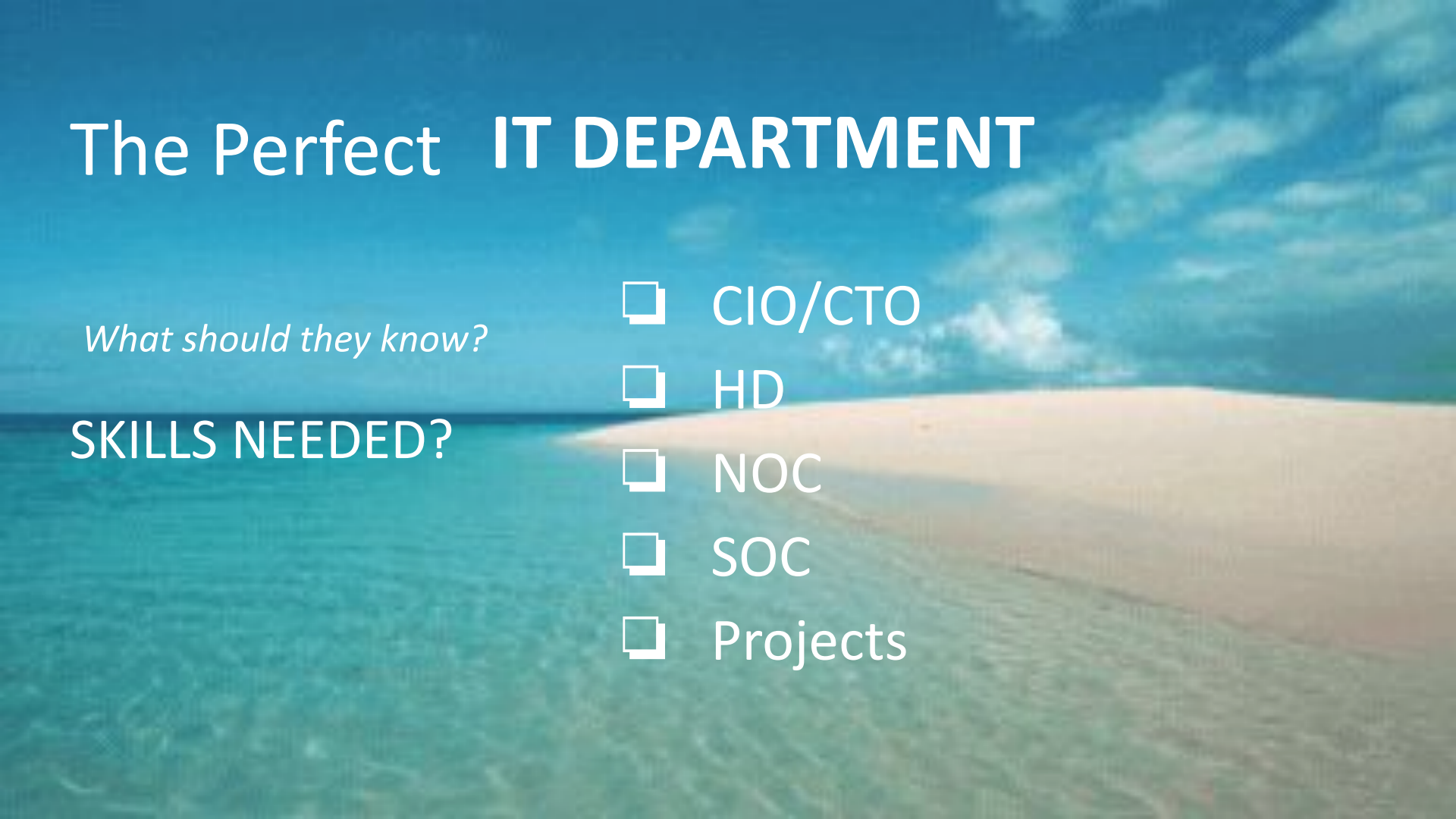
p=quarantine

Sends unauthorized emails to the spam folder.

p=reject

The final policy and the ultimate goal of implementing DMARC. This policy ensures that unauthorized email doesn't get delivered at all.

Domain-based Message Authentication Reporting and Conformance (DMARC) is a free and open technical specification that is used to authenticate an email by aligning **SPF** and **DKIM** mechanisms. By having DMARC in place, domain owners large and small can fight business email compromise, phishing and spoofing. Co-authored by dmarcian's founder, DMARC was first published in 2012.


The Perfect IT DEPARTMENT
What should they know?
SKILLS NEEDED?
CIO/CTO
HD
NOC
SOC
Projects

The Perfect IT DEPARTMENT

What should they know?

Chief Information Officer (CIO)/Chief Technology Officer (CTO)

- **Strategy**
  Cloud vs on prem
  Internal systems vs Product

- **Architecting**
  Stay abreast of the latest technology
  Understand current technology being used
  Understand how various technologies connect with each other
  Finding the right solution based on business needs
  Designing the configuration for the solution
  Ensuring the new system works well with foundational and supplementary applications

- **Budgeting**

- **Internal systems vs Product**

The Perfect IT DEPARTMENT

What should they know?

Help Desk (HD)

- Troubleshooting
- How to
- Documenting/knowledge base
- Training & Testing
- Vendor management

The Perfect IT DEPARTMENT

What should they know?

Network Operations Center (NOC)

- 24x7x365 Infrastructure Monitoring
- Infrastructure Management
- Vulnerability Management

The Perfect IT DEPARTMENT

What should they know?

Security Operations Center (SOC)

A security operations center (SOC) is a centralized unit that deals with security issues on an organizational and technical level.

It comprises the three building blocks for managing and enhancing an organization's security posture: **people, processes, and technology.**

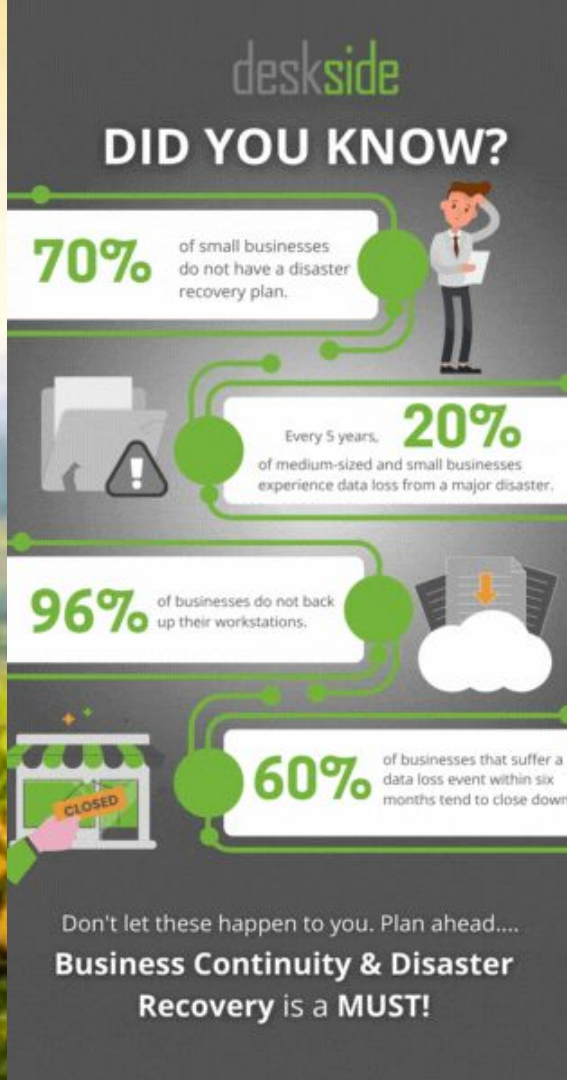
The Perfect IT DEPARTMENT

What should they know?

Project Management

- What to buy?
- Where to buy it?
- How to buy it (CAPEX vs OPEX)?
- Project planning and management?
- Application configuration?
- Infrastructure configuration?
- Bug troubleshooting and resolution?

Security


deskside
DID YOU KNOW?
70%
of small businesses do not have a disaster recovery plan.
Every 5 years,
20%
of medium-sized and small businesses experience data loss from a major disaster.
96%
of businesses do not back up their workstations.
CLOSED
60%
of businesses that suffer a data loss event within six months tend to close down
Don't let these happen to you. Plan ahead....
Business Continuity & Disaster Recovery is a MUST!

Security

Remote monitoring and management (RMM) is the process of supervising and controlling IT systems (such as network devices, desktops, servers and mobile devices) by means of locally installed agents that can be accessed by a management service provider.

Functions include the ability to:

- install new or updated software remotely (including patches, updates and configuration changes)
- detect new devices and automatically install the RMM agent and configure the device
- observe the behavior of the managed device and software for performance and diagnostic tasks perform alerting and provide reports and dashboards

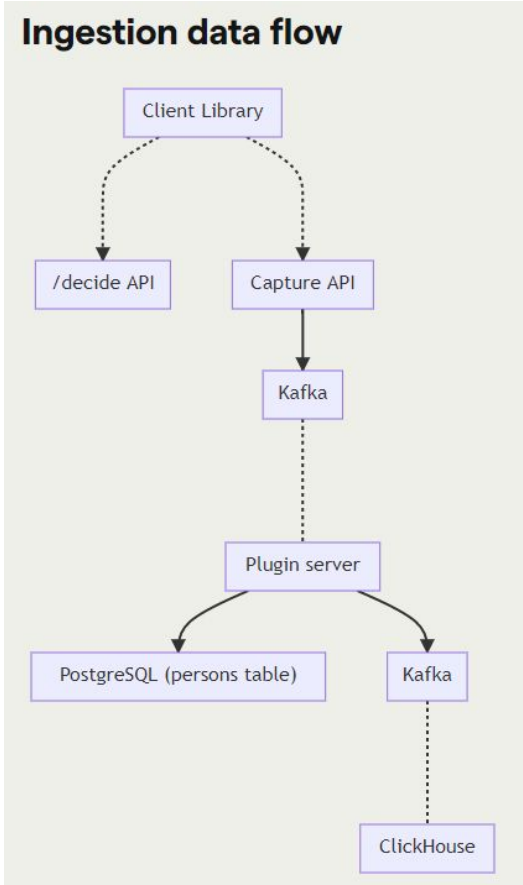
Traditionally, this function has been done on site at a company but many MSPs are performing this function remotely using integrated SaaS platforms.

solarwinds
The Power to Manage IT

Security

Event Ingestion Platform

A fully managed, real-time data **ingestion** service that is simple, trusted and scalable.



Security

Sumo Logic, Inc. is a cloud-based machine data ana
company focusing on security, operations and BI use
It provides log management and analytics services t
leverage machine-generated big data to deliver real
insights.

sumologic

15:00

SECURITY

What comes into mind when you hear the word “**SECURITY**”?

SECURITY

Security for information technology (IT) refers to the methods, tools and personnel used to defend an organization's digital assets. The goal of IT security is to protect these assets, devices and services from being disrupted, stolen or exploited by unauthorized users, otherwise known as threat actors.

The landscape is continuously changing
Violence-as-a-Service (VaaS)
AI Phishing

How Do These Attacks Start?

Most cyber attacks require you to open the door for criminals to enter.

These tend to come in the form of:

- **Malicious Email Attachments**
- **Malicious Links**
- **Phony Phone Numbers**
- **Lookalike Login Pages**
- **Malicious QR Codes**
- **Malicious Texts**

COOL TECHNOLOGY
SECURITY

MSP
(Managed Services Provider)

vs

MSSP
(Managed Security Service Provider)

vs

TSP
(Tech Success Partner)

Which do you currently have?

Technology Success Partner (TSP) provides all the services of an MSP & MSSP:

MSP

- IT Helpdesk
- Infrastructure management
- Application Support
- Network Operations (NOC)
- Vendor Management
- Remote desktops
- Collaboration suites
- Backup & Replication
- Business Continuity & Disaster Recovery

MSSP

- Domain & Email Security
- Network & Cloud Security
- Remote Access Services
- Identity Management
- Security Operations (SOC)
- Security Awareness

Professional Services

- Cloud Transformation
- Cloud Migration
- Strategic IT Planning
- Acquisition Integration
- IT Project Management
- Compliance Management
- Business Process Automation

THINGS TO LOOK OUT FOR

One Person IT

Companies that don't give you choices

Repeat issues

Money fixes all

False sense of security

What is Multi-Factor Authentication (MFA)?

Multi-factor authentication (MFA; encompassing authentication, or 2FA, along with similar terms) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:

- *knowledge (something only the user knows)*
- *possession (something only the user has)*
- *inherence (something only the user is)*

MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorised third party that may have been able to discover, for example, a single password.


yubico
KEEPER
Cybersecurity Starts Here
Security/Efficiency/Automation

What are the different types of MFA?

Phone callbacks

SMS-based OTP

One Time Passcode (OTP) Tokens

Authenticator Apps

Universal Second-Factor (U2F) devices

AUTHY

yubico

Microsoft Authenticator

Google

What is **PASSWORD MANAGER?**

A **password manager** is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.

KEEPER
Cybersecurity Starts Here

LastPass

CURRENT TECHNOLOGY CHECKLIST

SCAN ME

Think about your current Tech situation. What is working? What is not? Can you find any vulnerabilities in your environment?

Actionable Takeaways

1. What vulnerabilities can you identify?
2. What new technologies can you incorporate in your business?
3. Do you have the right people in your IT department?

GROUP DISCUSSION

Let's get into groups of 3, work together to discuss your findings, possible solutions, and highlight a few items to share with the entire group.


THANK YOU!
QUESTION?