E-BOOK

Your Essential **IT Glossary**

Interlaced.io

You're not alone if you're tired of pretending to understand when everyone is tossing around IT terms. IT-speak can seem confusing, but as a people-focused team of experts, we're here to help.

Navigating the IT landscape is difficult if you don't know the language

IT can seem like another language, and in many ways, it is. IT discussions are often laden with confusing lingo and uncommon terms and definitions. It's difficult for newcomers beginning their initial conversations around IT security to understand the issues and options they face.

That's why Interlaced.io created this handy IT guide. Use our comprehensive glossary of IT terms and definitions to build knowledge and jumpstart your search for better network security.

Keep it as a reference guide to refer to as you review your options.

And of course, if you still need someone to walk you through IT language, you can also get in touch with us with more questions throughout your IT search.

Your “Essential IT” glossary of terms and definitions

Below is a glossary of some of the most common words you’ll encounter when considering an IT-managed service provider. We’ve broken it down into four topic categories or sections to make it easier to find the info you need: General, Data, Security, and Cloud.

General

BYOD: Bring Your Own Device (BYOD) is an organizational technology model that allows employees to bring and use personal devices for work-related activities.

Domain: the address of your website that people visit (like interlaced.io). It is also the identifier for internal network administration, including applications, emails, and more.

Hardware: the physical components and equipment of a computer, including CPU, keyboard, monitor, graphics card, and more.

Infrastructure: components of IT enterprises. These can include hardware, software, operating systems, and more.

MSP: Managed Service Provider (MSP): a third-party company that remotely manages and provides enterprise-level IT services.

Software: a set of instructions that tell a computer how to work.

Data

Bandwidth: a measurement of the volume of data that can be transmitted over a network at any given time.

Data center: a facility that centralizes and maintains equipment for businesses to store data and applications.

Database: an organized collection of structured data typically stored and retrieved by users electronically.

Server: a computer that is responsible for responding to requests made by a client program, as well as data delivery. There are different types of servers, including those for the web; also local servers that support intranet systems.

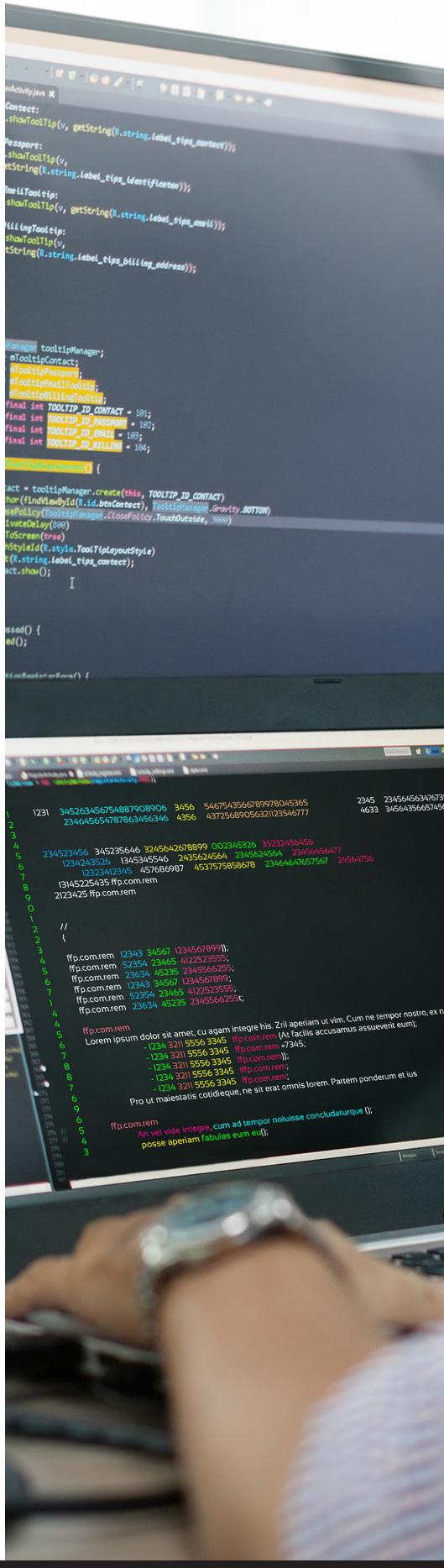
Security

Antivirus software: a type of software program designed to protect computers against cyber criminals by detecting and removing viruses and malware. Antivirus programs protect by looking through web pages, software, files, and applications.

Disaster recovery: An organizational method delineating how a business will regain use and access to their IT system after various unfortunate events. These may include natural disasters, cyber-attacks like ransomware, or other system disruptions.

Encryption: the process of encoding information. Encrypting data will convert it into a seemingly random and unreadable format that can only be translated or read with a decryption key.

Firewall: a security device that monitors incoming and outgoing traffic to block and filter traffic to prevent unauthorized agents from gaining access to a network.



Malware: short for malicious software, it's a category of intrusive applications that interfere with a network's standard actions to damage or destroy computers and networks. Examples include viruses, spyware, adware, worms, and ransomware.

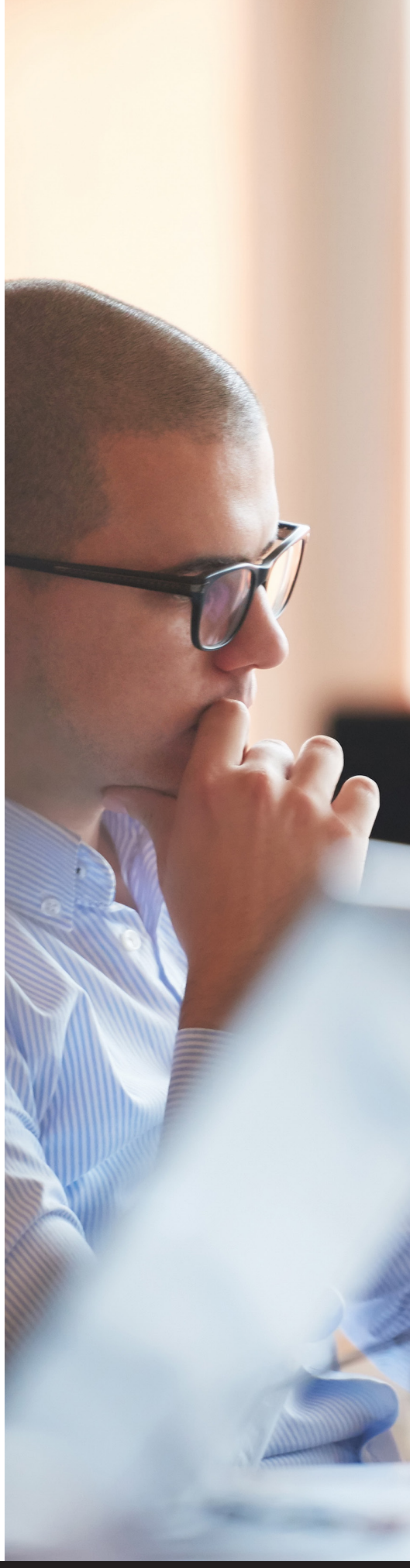
On-premises: a term used to describe software installed and run on computers housed within an organization's physical location instead of an offsite location.

Phishing: a scam, often using spoofing, to trick users into giving out personal info. This is often accomplished with emails that look like they've been sent from legitimate businesses. These emails ask potential victims to perform seemingly harmless acts: go to a website, hit reply, etc. When users click the link, they're sent to a fake website asking for sensitive info.

Ransomware: a type of malware used as a cyber-attack. Once it enters a device, it locks or encrypts the data and blocks it until the victim pays a ransom.

SOC: security operations centers are an onsite or outsourced IT security team providing 24/7 monitoring of an organization's IT infrastructure to catch cyber threats in real-time so they can be addressed before harm is done. They may also select/operate/maintain cybersecurity tech for the business. Also known as an information security operations center (ISOC).

If your organization relies on outsourced technology, customers want to confirm that your internal system is transparent and secure. Standard practice is to give your clients a SOC 1 or SOC 2 report as part of this due diligence package.



That brings us to the two kinds of SOC reports. A SOC 1 audit can help your business survey and report on its internal features, such as your customers' financial records. You should consider a SOC 1 if you offer an outsourced payroll service. If a client asks for the "right to audit" the system's data security, you can give them a SOC 1 report.

A SOC 2 audit, on the other hand, surveys and tracks your company's security, availability, processing transparency, confidentiality, and customer data privacy. SOC 2 audits cover any or all of the above five components. So, if you run a data center, instead of having your clients conduct an onsite audit, you can give them a SOC 2 report.

SIEM: security information and event management (SIEM) is an IT field involving real-time monitoring and analysis of cyber events. It also provides tracking and logging of security data for compliance or auditing purposes. The name is a combination of the terms "security information management" (SIM) and "security event management" (SEM).

Spyware: malicious software application designed to gather sensitive information about an individual or organization, often to harm the user financially. Often found in online advertising, it can also affect hardware.

Trojan Attack: (aka Trojan horse): disguised as a legitimate file or application but contains hidden, malicious code or software that can take control of networks.

Virtual Private Network (VPN): a service that allows you to create a private network while using a public internet connection, providing greater security and privacy.

Cloud

Cloud backup: a service that allows organizations to store data using the internet on an offsite server, often maintained by a cloud provider.

Cloud migration: the process of moving databases, applications, and other systems from on-premises hardware to the cloud or from one cloud to another.

Cloud service provider: third-party companies that offer organizations cloud-based services and platforms, like IaaS, PaaS, SaaS, cloud backup, and other computer solutions.

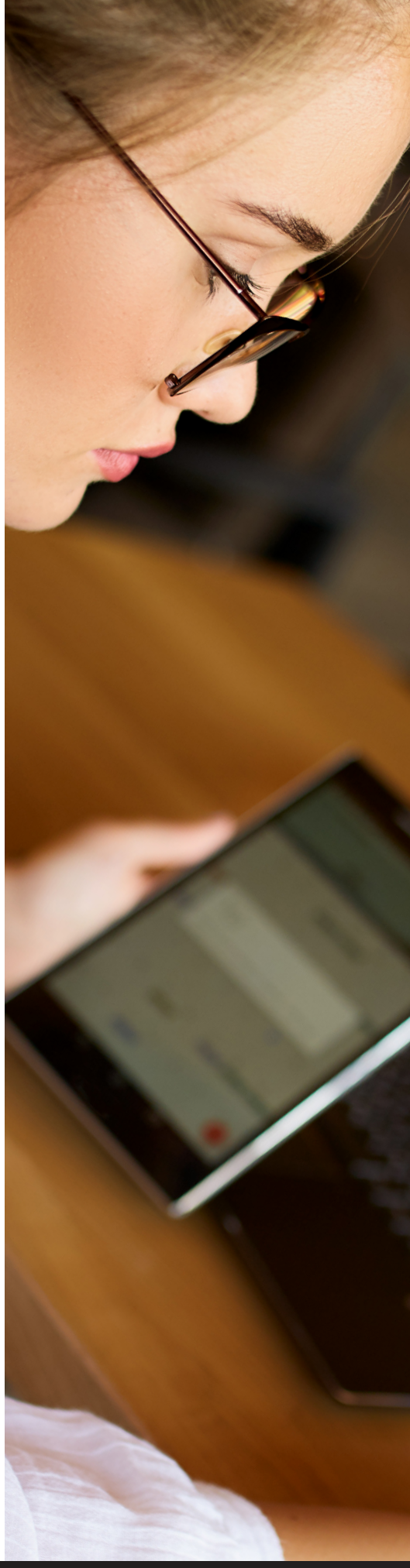
Cloud storage: files stored on the internet with a cloud storage provider or a dedicated private cloud.

Hybrid cloud: a cloud environment comprised of different models, such as a private cloud, public cloud, or on-premises infrastructure.

Infrastructure as a service (IaSS): a type of cloud computing where a cloud provider manages the infrastructure, and a business manages the operating system, middleware, software, and applications.

Multi-cloud: the use of more than one cloud provider to provide various services.

Platform as a service (PaaS): a type of cloud computing where an organization is provided with a platform over the Internet, often for developing and running apps.



Private cloud: cloud computing resources dedicated exclusively to one business or organization. This could be through privately-owned equipment or a third-party cloud provider.

Public cloud: cloud computing resources accessed over the internet that are shared between users.

Software as a service (SaaS): a cloud-based service that delivers software to users over the internet.

Interlaced doesn't just break down computer jargon, as much as we enjoy doing that. Chances are, as you scale your business, you may encounter IT terms and issues you need assistance with. We're committed to helping you out.

As part of our premium IT support service, our team of experts builds scalable IT programs for organizations looking for cost-effective solutions. We offer robust services to help you with software, network issues, and cybersecurity measures. Best of all, as a people-focused organization, we offer affordable, fast, and tailored support, especially for growing and scaling businesses.

If you give us an hour a week, we'll give you a customized, full-featured IT roadmap, a fractional team, and a solid IT program. Learn more about all the services we offer at **interlaced.io/how-we-help.**