1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

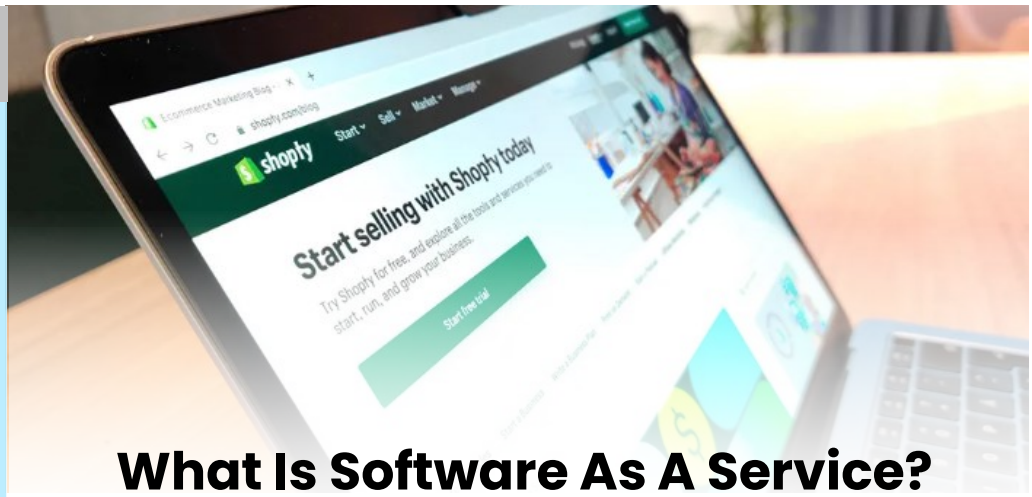
"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

May 2024

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"



What Is Software As A Service?

Introduction

How do you get new software onto your systems?

There are two ways you might get new applications delivered to your system: On-premises and software as a service.

On-premises software is installed and maintained on the customer's own servers, whereas SaaS software is hosted and managed by a third-party vendor.

The SAAS model hosts applications via a cloud provider, and it is made available to customers over the internet. SaaS applications are typically accessed through a web browser or mobile app, and users pay a subscription fee to access the software.

Pros of Software as a Service

One of the immediate benefits to SaaS is that their providers typically have more resources to invest in security than individual organizations. This means that they can deploy the latest security technologies and best practices to protect their customers' data. It also means that they are updated more frequently than on-premises software tends to be, hence security vulnerabilities are patched more quickly, reducing the risk of exploitation.

Think about how this would bring benefits to the modern workplace. In an age where companies have some employees in the office, others at home and some across the world, we need our software up to date and secure regardless of our proximity to the main server.

Continued on pg.2

Continued from pg.1

Since SaaS applications can be accessed from anywhere with an internet connection, employees can work remotely without having to worry about the security of their devices or the network they are connecting to.

Some other benefits of SaaS include:

- Since SaaS software is typically priced on a subscription basis, it can be more affordable than the upfront costs of purchasing and installing on-premises software.
- It does not require anyone to come in to install or tinker with it, simplifying set up, updates and repairs.
- You can easily add or remove users as needed, making SaaS software a great choice for scalability. Providers typically have more resources to invest in security than individual organizations, so SaaS software is often more secure than on-premises software.

Cons of Software as a Service

With any technology, though, there are going to be downsides. For SaaS, the primary concern is that the application is targeted by cyber-attacks—since it's not restricted to a physical locale, threat actors could find a way to exploit it.

You also must remember that you're trusting a third-party service. SaaS providers have access to customer data; it is important to choose a SaaS provider with a strong track record of security and data privacy.

Other disadvantages with SaaS software include:

- Once you choose a SaaS provider, you may be locked into their platform, which can make it difficult to switch providers if you are not happy with the service.
- Since SaaS providers have access to your data, you entrust your security and overall data privacy to a third party.

If you are subject to industry regulations, you may need to ensure that the SaaS provider is compliant with those regulations. Compliance is no joke!

Conclusion

Overall, SaaS can be a valuable tool for improving cybersecurity, but it is important to be aware of the associated challenges and take steps to mitigate them. Look for providers that have been audited by a third-party security organization and that have a clear privacy policy in place, so you know they take your data's privacy seriously. Implement strong authentication and access controls for your SaaS applications so that unauthorized users can't break in.

Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim your FREE copy today at

https://www.cti-mi.com/itbuyersguide-524/

Security Corner

AI Got Your Tongue?

Did you know that cybercriminals can impersonate real people's voices…and then clone them, so you think you're listening to somebody else?

In other words, you may think you're talking to your boss or local politician or even your best friend…but it could really be a bunch of special software **deepfaking** their vocal likeness.

How Does AI Clone Voices?

Hearing a familiar voice, especially from an authority or loved one, lowers defenses and makes you more likely to believe their claims!

Where could someone find *your* voice online? Social media posts, voicemails, leaked recordings and even public speeches are all commonly posted online. Once trained, the AI model can synthesize new speech based on the learned patterns. That is to say, they can make this stolen "voice" to say things that the original audio file never said.

In light of this technology, it's important to **be wary of unsolicited calls or messages, even if they sound familiar.**

Conclusion

How can you stay safe from AI voice cloning scams?

- Be wary of unsolicited calls or messages, even if they sound familiar.
- Never share personal information or send money based on phone calls or texts.
- Verify information directly with the source, not through the caller.

For more information about the dangers of misinformation, call us at 248-362-3800 or visit: https://tinyurl.com/24b5hbjs

Google & Yahoo's New DMARC Policy– Why Businesses Need Email Authentication

Have you been hearing more about email authentication lately? There is a reason for that. It's the prevalence of phishing as a major security threat. Phishing continues as the main cause of data breaches and security incidents.

A major shift in the email landscape is happening. The reason is to combat phishing scams. Email authentication is becoming a requirement for email service providers. It's crucial to your online presence and communication to pay attention to this shift.

Google and Yahoo are two of the world's largest email providers. They have implemented a new DMARC policy that took effect in February 2024. This policy essentially makes email authentication essential. It's targeted at businesses sending emails through Gmail and Yahoo.

But what's DMARC, and why is it suddenly so important?

The Email Spoofing Problem
Imagine receiving an email seemingly from your bank. It requests urgent action. You click a link, enter your details, and boom – your information is compromised.

The common name for this is **email spoofing**. It's where scammers disguise their email addresses. They try to appear as legitimate individuals or organizations. Scammers spoof a business's email address. Then they email customers and vendors pretending to be that business.

These deceptive tactics can have devastating consequences on companies. These include:

- Financial losses
- Reputational damage
- Data breaches
- Loss of future business

Unfortunately, email spoofing is a growing problem. It makes email authentication a critical defense measure.

What is Email Authentication?
Email authentication is a way of verifying that your email is legitimate.

Email authentication uses three key protocols, and each has a specific job:

- **SPF (Sender Policy Framework):** Records the IP addresses authorized to send email for a domain.
- **DKIM (DomainKeys Identified Mail):** Allows domain owners to digitally "sign" emails, verifying legitimacy.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Gives instructions to a receiving email server including, what to do with the results of an SPF and DKIM check. It also alerts domain owners that their domain is potentially being spoofed.

SPF and DKIM are protective steps. DMARC provides information critical to security enforcement. It helps keep scammers from using your domain name in spoofing attempts.

Why Google & Yahoo's New DMARC Policy Matters
Both Google and Yahoo have offered some level of spam filtering but didn't strictly enforce DMARC policies.

- Starting in February 2024, the new rule took place. Businesses sending over 5,000 emails daily must have DMARC implemented.
- Both companies also have policies for those sending fewer emails. These relate to SPF and DKIM authentication.

Look for email authentication requirements to continue. You need to pay attention to ensure the smooth delivery of your business email.

The Benefits of Implementing DMARC:

- Protects your brand reputation
- Improves email deliverability
- Provides valuable insights

5 Data Security Trends To Prepare For In 2024

With cyber threats evolving at an alarming pace, staying ahead of the curve is crucial.

It's a must for safeguarding sensitive information. Data security threats are becoming more sophisticated and prevalent. The landscape must change to keep up.

1. **The Rise of the Machines:** AI and Machine Learning in Security
2. **Battling the Ever-Evolving Threat:** Ransomware
3. **Shifting Strategies:** Earlier Data Governance and Security Action
4. **Building a Fortress:** Zero Trust Security and Multi-Factor Authentication
5. **When Things Get Personal:** Biometric Data Protection

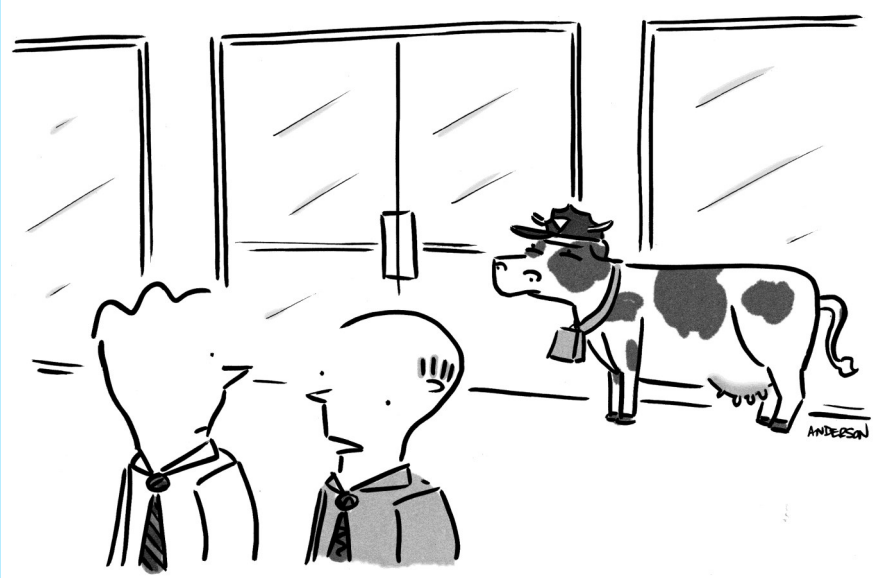
10 Most Common Smart Home Issues

Back when you were a kid, living in a "smart home" probably sounded futuristic. While we don't have flying cars, we do have internet capable telephones and voice-activated lights.

But even the most advanced technology can have analog problems. Hackers can get past weak passwords. Bad connections can turn advanced into basic pretty quickly. Have you run into any issues with your smart home gadgets?

Here are some of the most frequent problems and their related solutions.

1. **Connectivity Woes –** Restart your router and your devices. If that doesn't work, ensure you've positioned your router centrally. Or invest in a Wi-Fi extender for better coverage.
2. **Device Unresponsiveness –** Try turning it off and back on.
3. **Battery Drain –** Adjust settings to reduce power consumption. Disable features you don't use.
4. **Incompatibility Issues –** Check to ensure your devices are compatible with each other. Build your devices around your smart home platform. Review the manufacturer's specifications thoroughly to avoid compatibility headaches.
5. **Security Concerns –** Use strong and unique passwords for all your devices and accounts. Enable two-factor authentication when possible.
6. **App Troubles –** Try logging out and logging back in to refresh the connection. If issues persist, uninstall and reinstall the app.
7. **Automation Gone Wrong –** Review rules and test individually.
8. **Limited Range –** Move your devices closer to the router for better communication.
9. **Ghost Activity –** Investigate causes and change passwords.
10. **Feeling Overwhelmed –** Refer to your device manuals and online resources



"Oh, that. We beefed up security."