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

November 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!"

Is Your Smart Phone Spying On You?

Introduction

How often has a friend, coworker or family member introduced you to something for the first time… only for it to show up on your Instagram and Facebook feeds next time you log in?

It's a popular theory that smart phones are covertly constantly listening in on our conversations to target ads and personalize online experiences.

More than half of Americans, and 60% of Millennials in general, believe that their devices are eavesdropping on them at least *some* of the time.

In a quickly deleted blog post, Cox Media Group just confirmed your worst fears.

Is This Thing On?

The deleted Cox Media Group blog post titled "It's True. Your Devices Are Listening to You" sparked a significant uproar concerning online privacy and ad targeting practices.

The post allegedly boasted about CMG's "Active Listening" technology, which claimed to analyze anonymized audio data from smartphones and smart speakers to understand users' needs and preferences. This was then used to target them with highly personalized ads based on conversations around specific products or services.

What exactly is Active Listening? The technology is allegedly meant to target "pre-purchase

Continued on pg.2

Continued from pg.1

conversations," by illicitly activating the microphone on phones and other devices. Then artificial intelligence determines what key phrases advertisers want to hear. Like all artificial intelligence, this technology will become more accurate and even smarter as it acquires more data.

The post was framed as a breakthrough marketing guide for potential companies who wanted to buy and track that user data, helping to reach new and local business.

The Public Reacts

The blog post immediately ignited concerns about privacy invasion and lack of transparency regarding data collection practices. Aside from the clear potential for unintended (and unwanted) eavesdropping, critics also questioned how anonymous Active Listening keeps the user, as well as everyone's consent in the process. Just because you might want your phone to listen in on your conversations, doesn't mean that your friend wants to be recorded!

Ethical implications aside, therein also lies concerns about how these recordings could potentially be misused.

In response, Cox Media Group quickly removed the blog post and issued a statement denying that they listen to or process any individual's conversations. They clarified that their advertising solutions rely solely on aggregated and anonymized data sets sourced from third parties, not direct audio monitoring.

However, the deleted post's content and the lack of clear prior communication about data collection methods, have left the public unsure and very concerned. Indeed, the very idea of Active Listening technology raises questions about the future of user privacy when it comes up against the private sector.

Conclusion

So, is your phone really listening to your conversations? It's extremely possible! From the looks of technology like Cox Media Group denies having, the capability already exists. It's a matter of navigating the legal and ethical landscapes, as this will determine what data privacy legislation and consent options come about in the future.

Nothing is set in stone! We still have data privacy laws in place which guarantee our right to anonymity and security online. As long as that's true, you can rest easier about your data privacy.

Free Executive Guide: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This guide will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
https://www.cti-mi.com/protectdata1124
or call our office at (248) 362-3800

Security Corner

All MFA Is NOT Created Equal

We've all heard the hype around multi-factor authentication. Also known as MFA, this function protects your accounts by requiring an extra measure of verification on top of your username and password.

The Best MFA to Use

While multi-factor authentication remains the best option for protecting your work and personal accounts, it's not infallible. That's why we strongly recommend incorporating *biometric identification or authentication apps* into your MFA strategy, rather than relying solely on traditional one-time passwords (OTPs).

So, what makes biometric ID and authentication apps the superior choice for preventing a breach on your accounts? One of the most significant benefits is that biometric authentication methods, such as fingerprint or facial recognition, are inherently more secure than OTPs.

Conclusion

It's not just about the security of these methods. Biometric and authentication app both provide a much more *efficient* MFA sign-in experience.

- Biometric methods are often more convenient for users. You don't need to remember a password or carry a separate device. Just a quick scan of your fingerprint or face, and you're in.
- Authentication apps can generate codes quickly and securely, often without the need for an internet connection.

By leveraging these advanced methods, you can protect your accounts more effectively and enjoy a more convenient and efficient authentication process.

For more information about typosquatting, call us at 248-362-3800 or visit: https://tinyurl.com/y7aeufxs

Navigating The Challenges Of Data Lifecycle Management

Data is one of the most valuable assets a business can have. Managing this data throughout its lifecycle can be challenging. Data lifecycle management (DLM) refers to several processes and policies that govern the handling, storage, and eventual disposal of data.

Businesses generate and store vast amounts of data. As this happens, effective DLM becomes more critical. Navigating the challenges of DLM requires a comprehensive approach that balances security, compliance, and operational efficiency.

Understanding Data Lifecycle Management

DLM involves the governance of data. It starts from its creation and continues to its eventual disposal. The lifecycle includes several stages:

- Data creation
- Storage
- Use
- Sharing
- Archiving
- Deletion

Each stage presents its own set of challenges. Mismanagement at any stage can lead to security risks, regulatory non-compliance and increased operational costs. Implementing a robust DLM strategy ensures proper data handling at every stage.

The Importance of Data Lifecycle Management

Effective DLM is crucial for several reasons. First, it helps ensure data security. A well implemented DLM strategy includes security measures that protect data at every stage.

Second, DLM helps businesses follow regulatory requirements. Failure to comply can result in significant fines and reputational damage.

Finally, DLM helps improve operational efficiency. By managing data effectively, businesses can reduce storage costs, streamline operations and ensure that data is available when needed.

Challenges of Data Lifecycle Management

- **Data Volume and Variety**. There has been a proliferation of digital devices and platforms. The result is that companies are collecting more and more data.
- **Data Security and Privacy**. Protecting data is a critical aspect of DLM. As data moves through its lifecycle, it is vulnerable to various security threats.
- **Data Retention and Deletion**. Deciding how long to keep data and when to delete it is a critical aspect of DLM. Holding onto data for too long can increase storage costs and expose businesses to security risks. But deleting data prematurely can lead to compliance issues. It can also mean the loss of valuable information.
- **Data Accessibility and Availability**. Ensuring that data is accessible when needed is another challenge of DLM. As data moves through its lifecycle, users may have archived it. It can also be moved to different storage locations or deleted. Businesses should balance data accessibility and security by enforcing access controls, such as role-based access and MFA. Businesses must also plan for data availability during disruptions such as hardware failures, cyberattacks, or natural disasters through data backup and disaster recovery plans.

How AI Is Helping Small Businesses

• **Streamlining Customer Support with AI Chatbots** reduces response times and enhances experience.
• **Improving Marketing with AI-Powered Analytics** for targeted advertising and predicting trends.
• **Automating Routine Tasks with AI Tools** such as scheduling and expense management.
• **Enhancing Inventory Management with AI Forecasting** and automatic reordering.
• **Personalizing Customer Interactions with AI** through customized marketing.
• **Enhancing Recruitment and HR Processes with AI** by screening resumes and predicting performance.
• **Securing Data with AI Powered Cybersecurity** to detect anomalies and automate threat responses.

6 Simple Steps To Enhance Email Security

1. **Use Strong, Unique Passwords.** Use a password manager and avoid reusing passwords.
2. **Enable Two-Factor Authentication (2FA).** Choose a 2FA and set it up for all accounts.
3. **Be Cautious with Email Attachments and Links.** Verify the sender, scan attachments, and don't click on suspicious links.
4. **Keep Your Email Software Updated.** Enable automatic updates.
5. **Use Encryption for Sensitive Emails.** Encrypt emails containing sensitive information and educate recipients.
6. **Watch Your Email Activity.** Set up activity alerts, regularly review account activity, and respond quickly to suspicious activity.

Data Breach Damage Control: Avoid These Pitfalls

Data breaches are an unfortunate reality for all types of businesses. When a breach occurs, the immediate response is critical. How you manage the aftermath can significantly impact your reputation and financial stability.

Effective damage control requires a well-planned approach. But there are common pitfalls that can exacerbate the situation:

• **Delayed Response.** The longer it takes to respond, the more damage can happen.
• **Inadequate Communication**. It leads to misunderstandings, frustration, and further reputational damage.
• **Failing to Contain the Breach**. Once your business detects a breach, take immediate action to prevent further damage.
• **Neglecting Legal and Regulatory Requirements**. Failing to comply can result in significant fines and result in legal action.

"Take the groundhog - now *that's* a sweet gig."