DTS DanTech Services
Computers under control!™
Technology Times April 2025 Issue

Dan Foote
Owner/President

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Amazon disables privacy option, will send your Echo voice recordings to the cloud

by Pieter Arntz

Amazon has announced its Echo devices will no longer have the option to store and process requests on the device itself, meaning your voice recordings will now be sent to the cloud for processing.

In an email sent to customers, Amazon explained that the feature "Do Not Send Voice Recordings" will no longer be available beginning March 28, 2025.

The reason for this change? AI.

"As we continue to expand Alexa's capabilities with generative AI features that rely on the processing power of Amazon's secure cloud, we have decided to no longer support this feature." Basically, the processing requests that rely on AI features can't be done within the limited processing power of the Echo device itself. This means that voice recordings will be sent to and processed in the cloud.

Amazon promises the recordings will be deleted after Alexa processes your requests if you enable the "Don't Save Recordings" setting (we recommend you do this). But is that promise enough? And what happens to the data before it's deleted? After all, it wasn't that long ago that Amazon's Ring camera feeds were available for all staff and contractors to view.

This change confirms existing fears about user privacy with the implementation of the generative AI version of Alexa.

- Continued on page 2

Best Monitor by PC Gamer and Ratings.com

MSI MPG 321URX QD-OLED

The MSI MPG 321URX is remarkable for PC gaming. It has a high 240Hz refresh rate with very low input lag for a responsive feel, and motion also looks extremely crisp thanks to its near-instantaneous response time.

Its near-infinite contrast ratio and perfect black uniformity are ideal for dark room gaming, as blacks look deep and inky. It also gets bright enough for highlights to pop, and colors look rich and vivid.

Compared To Other Monitors

The MSI MPG 321URX is a superb gaming monitor for PC and console gamers. Its 4k resolution ensures a detailed image, and its 240Hz display provides a crisp and responsive feel. It displays deep blacks next to bright highlights in a dark room, and small highlights pop.

Like several other 32-inch 240Hz OLEDs, such as the ASUS ROG Swift OLED PG32UCDM and the Gigabyte AORUS FO32U2P, it has several features to help enhance productivity, such as a USB-C port with 90W of power delivery and a KVM switch.

It has considerably less VRR flicker than most OLEDs, so it's a great option if you're sensitive to VRR flicker.

However, it doesn't have Dolby Vision support, so if that's important, you may want to consider another similar monitor like the Dell Alienware AW3225QF.

Click here to check it out

- Continued from page 1

Due to financial losses that came with Alexa's operation, Amazon introduced the AI-powered Alexa+ which has far more capabilities and should generate more cash-flow. Alexa+ is based on several major language models such as the in-house development Nova, and Claude from Anthropic.

In a statement Amazon told TechCrunch:

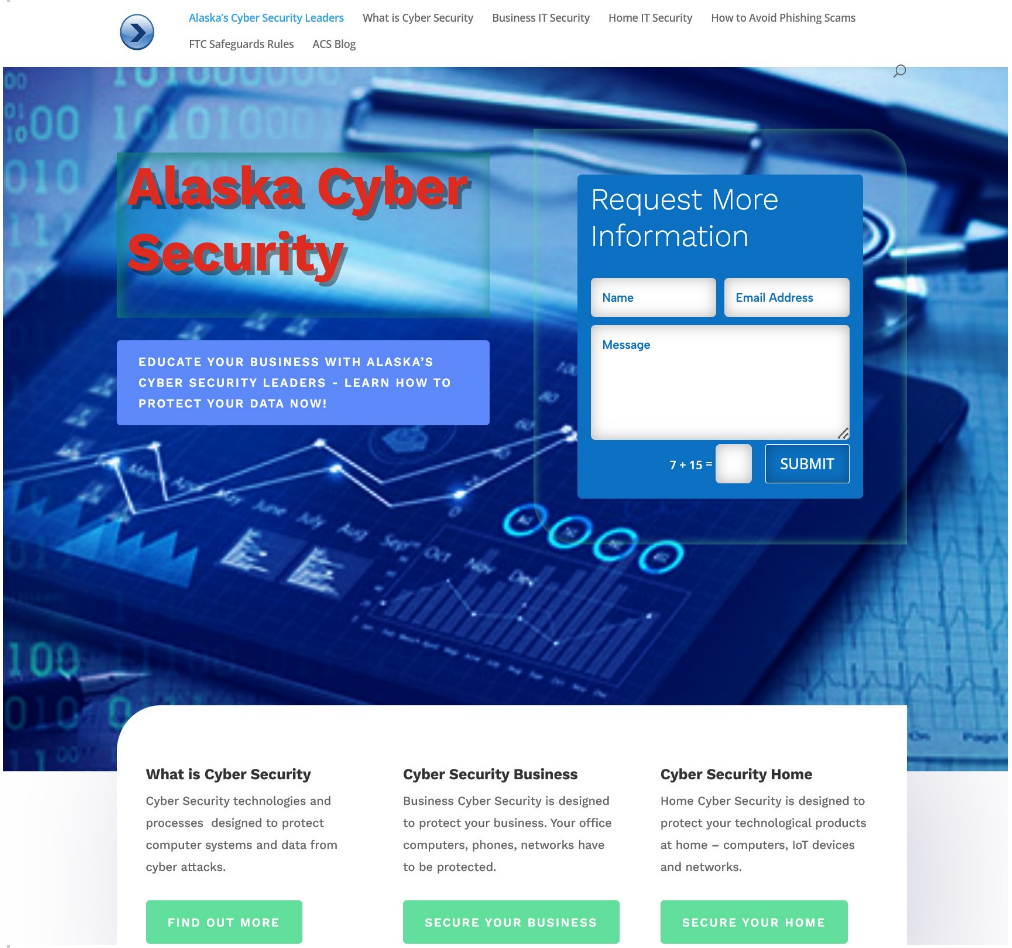
"The Alexa experience is designed to protect our customers' privacy and keep their data secure, and that's not changing. We're focusing on the privacy tools and controls that our customers use most and work well with generative AI experiences that rely on the processing power of Amazon's secure cloud."

This sounds reassuring, but something that doesn't leave the device can't get lost along the way. So, the "Do Not Send Voice Recordings" sounds a lot safer to me.

Reportedly, the change specifically affects the fourth generation Echo Dot (4th Gen), Echo Show 10, and Echo Show 15 devices, for customers in the US with devices set to English.

When devices are too smart

I love gadgets as much as the next person, but with some devices I wonder whether it's really necessary to make them "smart." The only way to protect your privacy and security at home is to avoid using devices that connect to the internet, including your phone. Obviously, in today's world, that's an impossible task for most. Therefore, the second-best option is to consider which devices are absolutely necessary for work, pleasure, and convenience, and slim down the list of smart-enabled devices.



Alaska Cyber Security

EDUCATE YOUR BUSINESS WITH ALASKA'S CYBER SECURITY LEADERS - LEARN HOW TO PROTECT YOUR DATA NOW!

Request More Information

7 + 15 =

What is Cyber Security

Cyber Security technologies and processes designed to protect computer systems and data from cyber attacks.

Cyber Security Business

Business Cyber Security is designed to protect your business. Your office computers, phones, networks have to be protected.

Cyber Security Home

Home Cyber Security is designed to protect your technological products at home – computers, IoT devices and networks.

Warning over free online file converters that actually install malware

The FBI Denver Field Office as warned of an increasing number of scummy websites offering free online file converter services. Instead of converting files, the tools actually load malware onto victims' computers. The FBI warned specifically about that malware leading to ransomware attacks, but we've also seen similar sites that install browser hijackers, adware, and potentially unwanted programs (PUPs).

The cybercriminals offer any kind of popular file conversion to attract victims, **with the most common ones converting .doc to .pdf files and vice versa**. There are also sites that offer to combine multiple images into one .pdf file. And it's not as if these file converters don't work. Usually, they will, and the victim will think nothing more of it. They might even recommend it to a friend or co-worker. But in the background, their system has hidden malware in the file the victim has downloaded, which is capable of gathering information from the affected device such as:

Personal identifying information (PII) including Social Security Numbers (SSN).

- Personal identifying information (PII) including Social Security Numbers (SSN).
- Financial information, like your banking credentials and crypto wallets.
- Other passwords and session tokens that could allow the scammers to bypass multi-factor authentication (MFA).
- Email addresses.

There are a few possible scenarios the cybercriminals might pursue:

- They encourage you to download a tool on your device to do the conversion. This is the actual malware.
- You might be recommended to install a browser extension that you can use going forward.
- In the most sophisticated scenario, the so-called converted file contains malware code that downloads and install an information stealer and everyone who opens it will get their device infected.

Cybersecurity threats in 2025

Cybercrime is one of the most significant rising risks that businesses face in 2025, and cybercriminals do not discriminate when targeting businesses. That said, in many cases, the bigger or more successful your business is, the more at risk of receiving a cyber threat you'll be.

Social engineering

Social engineering remains one of the most dangerous hacking techniques employed by cybercriminals, largely because it relies on human error rather than technical vulnerabilities. This makes these attacks all the more dangerous because it's a lot easier to trick a human than it is to breach a security system. And it's clear that hackers know this: according to Verizon's 2024 Data Breach Investigations report, 68% of all data breaches involve some form of non-intentional human interaction.

In 2023, social engineering tactics were a key method for obtaining employee data and credentials. In recent years, social engineering attacks have become more sophisticated and harmful due to technological advances such as deepfakes and Generative AI. Attacks are becoming more difficult to identify and cybersecurity companies are being forced to quickly improve their systems.

Common types of social engineering

Here are a few of the most frequent types of social engineering attacks:

* Phishing: Criminals send messages through email, text, or social media, pretending to be a reputable source with the goal of getting individuals to reveal sensitive information and data such as bank account info, social security numbers, and passwords.
* Spoofing: Similar to phishing, but the attacker "spoofs" an email address or even an entire website to deceive individuals. For example, they may change a single letter in an email and create a landing page that is nearly identical to the original.
* Whaling: A highly strategized phishing attack that personally targets high-ranking executives and officers within a company with the goal of getting access to incredibly sensitive information or sending large sums of money.
* Baiting: Scammers will lure individuals into clicking on fake advertisements with attractive offers and promotions, such as free products and discounts. The links may either install malware onto the device or ask individuals to input personal information.

Third-party exposure

Cybercriminals can get around security systems by hacking less-protected networks belonging to third parties that have privileged access to the hacker's primary target. One major example of a third-party breach occurred at the beginning of 2024 when AT&T addressed a massive third-party data breach that affected more than 70 million customers, exposing call and text data, passwords, and more.
This type of cyberattack is especially dangerous as many third parties tend to be much less secure than the major companies they work with. Third-party threats have become increasingly more common, and in 2023, 29% of all data breaches occurred due to a third-party attack.

Artificial intelligence cyber threats

Without a doubt, AI has changed the game when it comes to cyber threats. AI-driven attacks use machine learning to quickly analyze security systems, identify and penetrate weak spots. Additionally, cybercriminals are now able to automate attack processes, so not only have the attacks become more sophisticated, but also more frequent. According to a 2023 survey from CFO.com, 85% of cybersecurity professionals believe that the rise in cyberattacks is due to AI tactics.

Continued on the page 4

WiseSky Pet Air Purifier for Home, 3-in-1 HEPA Filter, Remove Odor & Dander, Covers 1644 Ft², W-Cat Model, 10pcs Pre-filter Include

What do volcanos and pets have in common? They produce dirty air particles. **A solution for pet hair and dander and dirty air particles.**

W-Cat air purifier is designed for large rooms up to 1,644 ft². This pet air purifier effectively removes cat hair, dander, odors, and allergies while operating quietly with 360° air intake. PM2.5 and VOCs senor. Easily control it via Smart App.

Pet-friendly Design - comes with a bite-proof power cord, 24v low voltage and automatic power-off function when 45° tipped off. The three-color light could be turn off easily at night, and 7.5mm gap prevent cat's paw from getting stuck.

Quiet Mode for Better Sleep - Fixed speed mode doesn't frighten pets. The quiet mode ensures that both you and your furry friends enjoy peaceful, undisturbed sleep at night

Smart Air Quality Monitoring - PM2.5 and TVOC sensors monitor indoor air quality 24/7. The three-color air quality indicator shows real-time AQI, helping you keep track of the air quality in your home and ensure a healthy environment for your family, and our smart app can help you monitor at anytime anywhere.

- Continued from page 3

Additionally, in our 2023 cyber risk index report, we found that 90% of startup founders are concerned about the dangerous potential of AI cyberattacks. This has caused a shift towards a more proactive approach to improve systems and increase security. As mentioned above, AI has also really pushed the boundaries of phishing, with 95% of businesses agreeing that phishing attempts have gotten more sophisticated and personalized in the last year.

With all this said, artificial intelligence hasn't been all bad news for cybersecurity; it has actually improved capabilities in recent years. Security systems that utilize AI have improved threat detection, are more automated, and can even point out weak points in your system.

New technology, such as IBM's AI threat detection systems, helps businesses stay ahead of the curve by fighting AI-powered attacks with AI-powered security.

Ransomware

One of the most financially burdensome cyberattacks is ransomware. Ransomware is a type of malware that blocks access to software or files in a computer system until a specific sum of money is paid.
While ransomware attacks are by no means a new threat, they are becoming significantly more expensive and more frequent.

Between 2023 and 2024, the average ransom fee skyrocketed more than 500% with the average recovery from an attack costing $2.73 million in 2024. Similar to legitimate software companies, cyber-criminal groups are continually developing their tool kit for themselves and their customers – for example, to make the process of data exfiltration quicker and easier. Another trick that threat actors sometimes pull off is rebranding their ransomware, changing bits and pieces in the process. This makes ransomware attacks harder to identify before it is too late.

Ransomware attacks also cost companies in the form of income lost while hackers hold system access for ransom. In 2023, the average length of system downtime after a ransomware attack is 136 hours or 17 business days.