BSSi2 Innovations
Review Twice, Implement Once. Doing IT Right the First Time.

Amazon Wants to Share Your WiFi, Without Your Permission

What

Amazon wants you to share your WiFi to create a global wireless mesh internet service, without asking your permission. If you do not want to participate, you have to opt out. They will do this using Alexa, Echo and other Amazon devices like Ring.

When

On June 8th, Amazon will automatically enroll your Amazon devices in Amazon Sidewalk. Sidewalk, per Amazon, is a shared network that's supposed to help its devices (Amazon Alexa, Echo, Ring doorbell, security cameras, tile trackers, etc.) retain connectivity even if a home's internet signal is weak or not working. Sidewalk will take a very small portion of your bandwidth (so they say).

You may opt out of this experiment at any time. But some using Ring have noted that after they opted out of Sidewalk, it opted them back in. So check your opt out setting after June 8th (see below).

Do You Care

You need to ask yourself do you care about being part of this experiment and do you want to accept whatever risks there may be in allowing WiFi access to your devices to your neighbors. We certainly do not think this is a good idea and will not be part of Amazon's experiment. They listen to EVERYTHING and can record everything. Their services also control locks and other security devices in your homes. Remember, devices like Alexa and Echo are ALWAYS listening, waiting for that verbal command. Extending the reach of all this encrypted data to the sidewalk and living rooms of neighbors requires a level of confidence that's not warranted for a technology that has never seen widespread testing.

Amazon's decision to make Sidewalk an opt-out service rather than an opt-in one is also telling. The company knows the only chance of the service gaining critical mass is to turn it on by default, so that's what it's doing.

How to turn off Sidewalk

1. Opening the Alexa app
2. Opening More and selecting Settings
3. Selecting Account Settings
4. Selecting Amazon Sidewalk
5. Turning Amazon Sidewalk Off

Big Brother may not be listening, but Amazon surely is. What a great marketing plan!

Breaking Bad Habits: 4 Ways Your Employees are Putting Your Business At Risk Of Cyber-Attack

Your employees are instrumental when it comes to protecting your business from cyberthreats. But they can also become targets for hackers and cybercriminals, and they might not know it. Here are four ways your employees might be endangering your business and themselves — and what you can do about it.

1. They're Not Practicing Safe And Secure Web Browsing. One of the most basic rules of the Internet is to not click on anything that looks suspicious. These days, however, it can be harder to tell what's safe and what isn't.

A good rule of thumb is to avoid websites that do not have "https" in front of their web address. The "s" tells you it's secure – https stands for Hypertext Transfer Protocol Secure. If all you see is "http" – no "s" – then you should not trust putting your data on that website, as you don't know where your data might end up.

Another way to practice safe web browsing is to avoid clicking on ads or by using an ad blocker, such as uBlock Origin (a popular ad blocker for Google Chrome and Mozilla Firefox). Hackers can use ad networks to install malware on a user's computer and network.

2. They're Not Using Strong Passwords. This is one of the worst IT security habits out there. It's too easy for employees to use simple passwords or to reuse the same password over and over again or to use one password for everything. Or, worse yet, all of the above.

Cybercriminals love it when people get lazy with their passwords. If you use the same password over and over, and that password is stolen in a data breach (unbeknownst to you), it becomes super easy for cybercriminals to access virtually any app or account tied to that password. No hacking needed!

To avoid this, your employees must use strong passwords, change passwords every 60 to 90 days, and not reuse old passwords. It might sound tedious, especially if they rely on multiple passwords, but when it comes to the IT security of your business, it's worth it. One more thing: the "tedious" argument really doesn't hold much water either, thanks to password managers like 1Password and LastPass that make it easy to create new passwords and manage them across all apps and accounts.

3. They're Not Using Secure Connections. This is especially relevant for remote workers, but it's something every employee should be aware of. You can find WiFi virtually everywhere, and it makes connecting to the Internet very easy. A little too easy. When you can connect to an unverified network at the click of a button, it should raise eyebrows.

And unless your employee is using company-issued hardware, you have no idea what their endpoint security situation is. It's one risk after another, and it's all unnecessary. The best policy is to prohibit employees from connecting to unsecured networks (like public WiFi) with company property.

Instead, they should stick to secure networks that then connect via VPN. This is on top of the endpoint security that should be installed on every device that connects to your company's network: malware protection, antivirus, anti-spyware, anti-ransomware, firewalls, you name it! You want to put up as many gates between your business interests and the outside digital world as you can.

4. They're Not Aware Of Current Threats. How educated is your team about today's cyber security threats? If you don't know, or you know the answer isn't a good one, it's time for a change. One of the biggest threats to your business is a workforce that doesn't know what a phishing e-mail looks like or doesn't know who to call when something goes wrong on the IT side of things.

If an employee opens an e-mail they shouldn't or clicks a "bad" link, it can compromise your entire business. You could end up the victim of data breach. Or a hacker might

decide to hold your data hostage until you pay up. This happens every day to businesses around the world – and hackers are relentless. They will use your own employees against you, if given the chance.

> **"Education is a powerful tool and, when used right, it can protect your business and your employees."**

Your best move is to get your team trained up and educated about current threats facing your business. Working with a managed service provider or partnering with an IT services firm is an excellent way to accomplish this and to avoid everything we've talked about in this article. Education is a powerful tool and, when used right, it can protect your business and your employees.

On The Lighter Side

I love dad jokes, but I don't have kids, which makes me a Faux Pa.

Q: Why did an old man fall in a well?
A: Because he couldn't see that well!

I had a dream that I weighed less than a thousandth of a gram. I was like, 0mg.

Mom said I should do lunges to stay in shape. That would be a big step forward.

At first, I thought my chiropractor wasn't any good, but now I stand corrected.

Q: Why are elevator jokes so good?
A: They work on many levels.

I used to hate facial hair, but then it grew on me.

My toddler is refusing to take a nap. He's guilty of resisting a rest.

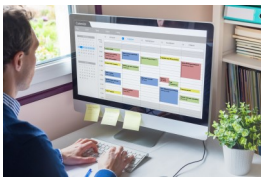
I used to be able to play piano by ear, but now I have to use my hands.

Q: When does a regular joke become a "dad joke?"
A: When it becomes apparent.

Business Tidbit

Eliminate Workplace Distractions To Maximize Your Productivity

While most of us accept that distractions will be a part of our day, if your intention is to get things done and to stay productive and focused, you'll need to minimize those distractions. No, we'll never be able to eliminate them 100%, but we can certainly try. Here's what you can do to cut distractions.



Block Time On Your Calendar (And Stick To It). Use your calendar to its full advantage. Mark time off for e-mails, for all projects, phone calls, Zoom calls, you name it! If it's part of your normal day, put it on your calendar. Even throw on time for miscellaneous stuff. Then share it with all relevant parties and stick to it. If you're working on a project between 1:00 p.m. and 3:00 p.m., that's the word.

Use Sound To Your Advantage. A common source of distraction is sound: it can be office chatter in the background or even neighborhood sounds (for those working from home). Find a sound that complements your workflow. It might be chill music or the sounds of rain or a babbling brook. Find the right sound that helps you zone in and blocks disruptive sounds.

~ Forbes, March 15, 2021

June 2021

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

"Every time I use my name as my password I get hacked. Maybe I should change my name. Or, change my password."

CartoonStock.com

Shiny New Gadget of the Month

Cancel Stress With Cove

Wouldn't it be nice if you could just press a button and your stress would melt away? Well, now it's possible, and it's thanks to Cove. The first of its kind, Cove is a wearable device (like a pair of headphones) designed with "stress cancellation" in mind.

Cove rests on your ears and wraps around the back of your neck. It uses subtle vibrations behind your ears to soothe your stress. Over 90% of those who participated in clinical trials reported a marked decrease in stress, and 91% reported sleeping better.

If you're looking for a new and innovative way to help manage your stress, Cove may be the answer. Due to its compact, lightweight design, it can be used anywhere, anytime. Learn more at FeelCove.com.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

f www.facebook.com/NickAEsp

twitter.com/NickAEsp

in www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

f www.facebook.com/bssi2

twitter.com/BSSi2llc