# Shared Workspace – Is Your Data Safe?

*The documented security weaknesses of coworking behemoth WeWork don't have to happen simply because a workplace is shared.*

SEATTLE, WASHINGTON, USA, September 11, 2019 /EINPresswire.com/ -- What are you worried about right now? A looming deadline, a difficult client, that noise your water heater (or possibly your cat) was making this morning? Whatever it is, it's probably enough, and you'd prefer if your workplace itself didn't pile on.

According to technology journalist Sean Captain, writing recently in Fast Company, WeWork has significant issues surrounding the security of their customers' identities and data. The company's network security structure is based on aging Wi-Fi security systems originally designed for home Wi-Fi. That generally inadequate system is accessed via a shared password known to huge numbers of current and former customers across multiple sites in the United States and abroad. And if that's not alarming enough, the password in question is one that regularly appears in top-20 lists of ridiculously easy-to-guess passwords no one should ever use.

Essentially, the technological equivalent of putting their customers' data in a pile on the street with a tarp draped over it and a sign reading don't steal this.

They could do better than that. And we know because at ATLAS Workbase, we do better than that. We asked Ken DeMaria, our Vice President of Technology and the architect of our network, how our data stays secure.

"For a start, everyone has their own username and password, which they control," says Ken. This means network access is limited to current ATLAS members, and every individual on the network is known—no shadowy figures skulking through the network with a guessed password. "That way," Ken adds, "if there was a problem, we'd be able trace back where the problem came from."

Individual names and hard-to-guess passwords are key to preventing the network from being spoofed, or used by criminals as a false front for a different network. "Since there are no shared passwords on our member network, it makes it much more difficult for an attacker to create a spoofed Wi-Fi network."

Spoofing is perhaps the most significant danger faced by users of an insecure network. A criminal can drop a $99 piece of hardware in an office that will produce a copy of the real network, with a slightly stronger Wi-Fi signal for users in the device's immediate vicinity. If proper Wi-Fi security isn't in place, those unfortunate users will automatically connect to this faux network. Compromised networks are used for a disturbing variety of activities, ranging from simply accessing the personal information of an individual user, to spreading dangerous malware, to conducting any number of man-in-the-middle attacks. In such attacks, criminals insert themselves into interactions between two parties—perhaps you and your clients—to intercept anything from financial information to intellectual property.

So, clearly, these threats are significant enough that we must not rely on passwords alone. Beyond individual, user-controlled passwords, the ATLAS Workbase network uses enterprise standard authentication and encryption, designed to be suitable for use in major enterprises such as Fortune 1000 companies.

By contrast, as Captain noted in Fast Company, if a WeWork customer is concerned about the company's nearly nonexistent network security, they'll be happy to upsell them a private network—for an additional $195 per month and a $250 setup fee. Which is great, if you're itching to spend extra money and think you can trust the unknown people who set up the wildly insecure security in the first place.

At ATLAS Workbase, if you ever have network security or other technological questions, or you simply need a bit of technical assistance, Ken or any of our help desk staff are here for you. And that means here, on site. WeWork customers will find their technical questions routed to a remote call center. But, we regard flawlessly functional technology—technology so smooth you hardly notice it—to be one of our basic services. So, use it! Our technology team members are selected because they want to help, and are good at it. Anytime it's needed (or even might be needed) any ATLAS member will have an in-person conversation with someone who wants their technology experience to be seamless, whether that takes a quick tweak, or some extensive hand-holding.

Figurative hand-holding, that is. For literal hand-holding we might have to upcharge you.

Kim Burmester
ATLAS Workbase
+1 415-378-2492
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.