

Date:	Wednesday, May 12, 2021 at 5:45 am PT
To:	Microsoft - All Employees All MS Store Employees FTE All Interns
From:	Bret Arsenault
Subject:	Securing our hybrid workplace

Hi Team,

We are at an inflection point. With **the move to hybrid work** we will embrace a more flexible work model both in terms of where and when we work. We must adapt how we provide a great employee experience that is also secure. Fortunately, with your help we have already achieved so much in our [Zero Trust journey](#), but there is more to do. 'Zero Trust' means we don't assume any identity or device is secure on any network – we verify it. This provides for a consistent and simplified experience from home, the office or anywhere in between.

The world trusts us with their data. It's a great privilege and it comes with great responsibility. We need to continue to earn our customers' trust. We can be a leader in this transition to a hybrid workplace. This past year the shift to remote work has unfortunately created new attack surfaces. Email scams and Ransomware in particular are increasing – phishing is responsible for nearly 70% of industry-wide data breaches. We must continue to raise the bar.

One of the successful ways we have modernized is by embracing a passwordless experience using multifactor authentication (MFA). While only 18% of our customers are using MFA, our workforce is at nearly 100% because of tools like Windows Hello for Business and Microsoft Authenticator. Thanks for helping us get there!

We need your help to make sure your identity, the devices you use and the way we build products and services are aligned with the Zero Trust strategy. Over the next twelve months, employees will see several changes and calls to action which further strengthen our posture *and* improve employee experiences, for us internally and our customers.

- **Keep your devices healthy and managed.** Modern management uses the power of the cloud. All devices that need access to corporate resources must be managed in order to keep your device secure and protected from phishing and malicious websites, as well as to ensure seamless access. Please visit [Modern Management on TechWeb](#) for guidance to transition to modern management as you return to the workplace. The benefit is this can be done from any device on any network (no VPN is required).
- **Secure your home office.** Visit the [Working from Home guidelines on MSProtect](#) and follow the guidelines to ensure you have a secure home network and environment.

- **Build for Zero Trust.** We want engineers and developers to build with a Zero Trust mentality and help us be a showcase of *how* we securely modernize our systems and code. Go to [1ES](#) to learn more about best practices including modern authentication using the [Microsoft Authentication Library \(MSAL\)](#) and modern device management using the [Microsoft Intune App SDK](#) in your applications and services.
- **Be a security hero.** Security is everyone's job and Zero Trust is how we will do it together. If you have feedback on something that is not working, for example, you find a site prompting for passwords, please let our [Zero Trust team](#) know.
- **Attend the Security Summit.** Join us on Oct. 6-7, 2021 for a virtual security summit where you will hear from Microsoft Security leadership, practitioners and customers on our security strategy, leading trends and tools and resources to help you be more secure.

Team, we have a unique understanding of today's security challenges because we live this fight every single day. This is a journey; the company and its customers are in your care. The above calls to action will enable all of us to help Microsoft, our customers and you to be even more secure. We will host a live [Yammer Chat](#) next week with experts from the respective product teams to answer any questions you may have.

Thank you for doing your part.

--Bret Arsenault
Chief Information Security Officer (CISO)