The Cybersecurity Readiness Podcast Series

Episode Title	Implementing Phishing Resistant Multifactor Authentication
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.dchatte.com/podcast/ https://the-cybersecurity-readi.captivate.fm/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	George Gerchow, Chief Security Officer and Senior Vice President of IT, Sumo Logic
Summary Pitch	The Cybersecurity and Infrastructure Security Agency (CISA) recently (Oct 31, 2022) released fact sheets urging all organizations to implement phishing-resistant multi-factor authentication (MFA). In this episode, George Gerchow, Chief Security Officer and Senior Vice President of IT, Sumo Logic, and I have an in-depth discussion on this very important security subject matter. The scope of coverage ranges from providing an overview of MFA and its benefits to discussing the challenges and hurdles of implementing phishing-resistant MFA, recommended implementation approaches, and the future of MFA.
Time Stamps	01:53 -- Please share with listeners some highlights of your professional journey. 02:51 -- Please provide listeners with an overview of what multifactor authentication is. 03:52 -- A recently published article on Dark Reading reports that a massive phishing campaign targeting GitHub users convinced at least one developer at Dropbox to enter in their credentials and the two-factor authentication code, leading to the theft of at least 130 software code

	repositories. Essentially, the perpetrators exploited the multi-factor authentication fatigue. George, your reactions. 06:51 -- You said that many organizations don't even have multifactor authentication. That begs the question, why is that the case? Is there a technology aspect to it, a technological complexity of having multifactor authentication integrated into existing legacy systems? Is there a cost aspect to it, is it very expensive? What does your experience tell you? 08:30 -- From personal experience, I haven't felt the fatigue. Even if I had to review several times or take that extra step to authenticate, I would because I am paranoid about ensuring that access is very secure. So I have brought about a change in my own mindset. I'm just curious to know if organizations are striving to bring about a change in the multifactor authentication mindset. What are your thoughts? 12:23 -- As humans, it is our natural tendency to assume, Oh, it's not going to happen to me. And if it does, we'll deal with it then. And I know that organizations also often have that mindset, some organizations know they will get bailed out. George, what are your thoughts? 22:21 -- Would you like to expand on how organizations go about implementing phishing-resistant MFA? What solutions are available out there? 25:09 -- George, I read about this FIDO authentication, the FIDO Alliance, where they have developed this protocol to enable phishing-resistant authentication. Can you expand on that? 26:50 -- During our planning meeting, you made a couple of very poignant statements, one of which is, "leaders should create a culture where employees feel they can slow down for the sake of security." Help tie this to our discussion on multifactor authentication.

	30:44 -- Going back to this multi-factor authentication fatigue, is there really a fatigue? Or is it being hyped up? What's the real story? 35:33 -- George, I'd like to give you the opportunity to share some final words, some key messages for the listeners.
Memorable George Gerchow Quotes/Statements	"Absolute laziness is really what it comes down to in the beginning; I don't want to disrupt my organization by having them go through this extra step." "Development organizations that are heavy with startups, the developers do not want to take that extra step. Sometimes executives are also unwilling to follow through with that extra authentication step -- Do I really have to do this? I know it's a policy, but can't I get around this? And the answer should be flat-out No, under any circumstances." "Whenever you can help your employees, the people that work for your company, do something that not only benefits the company but also benefits them personally, the better off the organization is going to be." "The two things that most hackers go after are health and wealth." "Like, how cool would it be if you got into a car and went to start the engine, and the engine wouldn't even start unless you had the seatbelt on?" "One-time code (OTC) is the way to go when implementing phishing-resistant multi-factor authentication. And let's ensure we implement MFA around critical applications, users, and data." "I'm sorry, sometimes you (developers) need to be slowed down. What if we drove on the road with absolutely no speed limits whatsoever? We create all kinds of damage. So I just think that there's this perception, this emotional transition Dr. Dave that people have to make, and we have to help them get there."

	"You need technology to back up the policy because people are people, and people will try to circumvent things a lot of times if they know there's no accountability." "A lot of times, security used to be looked at as a business inhibitor, mow it's a business enabler. People will want to do business with you when you have really good security hygiene in place, especially as we're looking at supply chain attacks that we've seen over and over again over the last few years."