FEBRUARY 2022 | THE OFFICIAL NEWSLETTER OF JUST SOLUTIONS INC.

MAKE IT EASY

NETWORKS, PRINTERS, PHONES AND SECURITY

1997-2022 25 YEARS GREAT BUSINESS RESULTS.

WEBINAR

Ramp Up Your Cybersecurity

Thursday, 24th February

1:00 PM - 2:00 PM

REGISTER NOW

Differences between various MFA tools and why they matter

What makes MFA software weak or strong and what that means to you

Tips on choosing the best MFA software for your company

Why a strong human firewall is your best last line of defense

What Is MFA?

With David Wolf, Vice President of Just Solutions Inc.

If technology wasn't confusing enough for most people, ransomware and cybersecurity are compounding the problem. Employees are required to know how to identify "fake" emails and "scams." When an email shows up marked urgent from your boss to handle something, you must stop and make sure it really is your boss sending you the request.

Oops, you clicked on the link or opened an attachment by accident. Your browser opened, but you quickly closed it. Phew, oh good, nothing happened. Maybe it was a resume you opened since you work in HR. Or a vendor invoice if you work in AP. The scenarios are endless, the results are the same. **Your account has been compromised.**

Why Should You Care?

Continued On Pg. 2

Join us Thursday, February 24th at 1:00 PM to learn more about Multi-Factor Authentication.

Security is not perfect but that doesn't mean we shouldn't add additional layers of protection.

You don't know it yet and it may be weeks or months before the "bad people" (threat actors, a fancier name) make their move. In the meantime, they've been collecting your usernames and passwords for all your accounts including banks, credit cards and who knows what else. How can you stay protected when these threat actors have your passwords or pin codes you use every day on so many sites?

The answer is additional layers of security beyond just a password. Multi-Factor Authentication (MFA) is an example of this layer of security. Geo-fencing is another example. Let's stay with MFA for now since that's today's topic. You may hear people talk about "Two Factor Authentication (2FA)" as well. Multi means two or more! So, let's count the "factors". The first one is the password you thought was secure. That's one factor. Let's add something you know – the security question. Where were you born? That's a second factor. But wait, is that secure? Not with social media these days! What's another factor? How about a 6 digit code sent to your cell phone via text message? What about a mobile app on your phone that provides you with a security code?

The optional code is an additional factor since a password is something you know and the code on the phone is something you have. A CAC card (smart card with a chip) is something the military uses. So, let's try that out. You use the CAC card at your computer AND enter a password. This includes both something you know and something you have. Add in a PIN being sent to a fob or smartphone, and you have an additional factor. Biometrics – reading your fingerprint, retinal scanner, facial recognition, voice recognition are all examples of "multi-factor" options.

A hacker who might have your password won't have access to your cell phone, CAC card, your eye, or your fingerprints. MFA should make losing your password to a hacker a non-event. All you must do is change your password after a known breach event.

Can MFA be hacked? Well, unfortunately, yes. If your phone has been hacked, they can intercept the code coming to your phone. Are your fingerprints in a database somewhere? Security is not perfect but that doesn't mean we shouldn't add additional layers of protection. That's why we must always stay vigilant!