Multi-Factor Authentication: Two is One. One is None.

Sun, 10/09/2022 - 11:11

|

Rob Tompkins, CISSP, Lead Cybersecurity Engineer, Tulane IT Information Security Team

View PDF

Perhaps you have watched one of the dozen or so survival shows where the contestants are left in the middle of a barren godforsaken landscape with nothing but a few items and their wits to survive.

Or you may have seen one of the many global competitions where contestants engage in a larger-than-life race around the world.

These shows are increasingly popular because we often wonder what we would do in impossible situations. Would we survive? Would we know what to do when everything is on the line?

A phrase that I have heard in these shows is: **“Two is one. One is none.”** This is a regular phrase in military and survival planning. It means if you have two of something and one breaks that is like having only one; if you have one of something and it breaks: Game Over.

This holds true in cybersecurity as well. **If you have only one thing protecting your account, like a password, and “that gets broken,” then it is like having nothing at all: Game Over.**

If you can add a second thing into the mix to protect your online accounts, then if your password gets stolen you are still protected. Fundamentally, this is the concept of multi-factor authentication (MFA).

A common misconception about MFA is that it protects the machine (or you) from an attack. In reality, it is protecting your account from being accessed by someone other than you, from a computer other than yours.

Computers don’t care where you are logging in from, everything is just 1’s and 0’s to them. Something must be added to the mix that will allow us to prevent malicious actors from logging into our devices, sites, and services. The most common tool for this is your cell phone. Inserting your phone into the authentication process forces an attacker to overcome a second obstacle to gain access. Best practices and tips for using multi-factor authentication to secure your online accounts.

Don't catch MFA fatigue

In the cat-and-mouse cybersecurity world, this has led to a new attack called “MFA Fatigue Attacks.”

Since you now must either “approve a voice call” or “click accept on your phone,” **attackers have started generating high volumes of these approval prompts**. They are hoping that you will get sick of them or think that something is wrong and click “Allow” to make them stop. This is a very successful attack. If you ever have this happen to you, you can report the prompt as fraudulent and someone on the Information Security team will investigate.

Another way attackers will attempt to bypass MFA is simply by asking you for your MFA code over the phone. An attacker will call you, usually pretending to be from an IT department, tell you they need to confirm something and ask for your MFA code. While unbelievable, **this attack is surprisingly effective. You should never share a passcode over the phone.** This is the easiest way for someone to bypass the protections on your account. What they are really doing is logging into your account using the code you just gave them!

Attackers can't bypass MFA if it isn't there

The worst data breach in national security history was an attack against the Office of Personnel Management (OPM), the Human Resources department of the Federal Government. In 2015, OPM discovered someone accessing one of their servers late at night when everyone should have been offline. A quick analysis revealed they had been hacked. The attack was most likely state-sponsored, and the hackers had been in their system for a long time. It affected service members, politicians, and government workers of all kinds. According to Wikipedia:

"*Approximately 22.1 million records were affected, including records related to government employees, other people who had undergone background checks, and their friends and family. One of the largest breaches of government data in U.S. history, information that was obtained and exfiltrated in the breach included personally identifiable information such as Social Security numbers, as well as names, dates, and places of birth, and addresses.*"

Ironically, the OPM used MFA throughout the organization, but none of the agency's 47 major applications required it… leaving them vulnerable to attack.

The Cybersecurity battle is won or lost with good practices. On this battleground, multi-factor authentication is not just a good idea: it is essential for survival. Don't let yourself be an OPM with MFA available, but not in use.

Cover yourself with MFA wherever and whenever you can.

Two is one, one is none.

Additional Resources

- MFA Fatigue: Hackers' new favorite tactic in high-profile breaches
- Multi-Factor Authentication at Tulane
- Knowledge check: Take the Tulane MFA quiz