INSIGHTS

Cyber made simple.

one brightly cyber

MFA MAY NOT BE ENOUGH

BY JAY BORDEN

MFA, Multi-Factor Authentication, has been recommended for years as providing security beyond usernames and passwords. For many years it worked and helped keep everyone safer.

One of the earlier methods of MFA sent a code either by email or by SMS to a user's mobile phone. That code was then entered into a logon confirmation screen. The use of SMS circumvented compromised computing devices.

Over time cybercriminals have become smarter and found ways to defeat older MFA techniques which are no longer secure and have contributed to a 500% increase in ransomware payments according to recent research.

We have been recommending the use of newer phishing resistant types of MFA for a while. Now their use has become imperative.

Snowflake, the cloud data storage platform and about 165 of their clients were breached using stolen credentials sold on the Dark Web. None of these companies required MFA. A username and password was all that was required to gain full access to their systems and all the information including what is stored on the Snowflake, a cloud storage system.

To make matters worse, research showed that those username and password combinations had been for sale on the Dark Web for years. Even without MFA, had the passwords been changed, the credentials wouldn't have worked. Of course, MFA is still recommended.

Many devices have been infected with malware and info stealers. In those cases, a simple password change would not protect anything. The info stealer would have gotten the new password and put it into the hands of the cybercriminals. From there it would have wound up for sale on the Dark Web again.

onebrightlycyber.com
(888) 773-1920

MFA MAY NOT BE ENOUGH

CONTINUED

Sadly, many forms of MFA are not much better than a username and password combination. So, simply using MFA is not going to make you safer. Phishing resistant MFA is necessary.

What is phishing resistant MFA?
Phishing resistant MFA is characterized as methods that prevents someone from clicking a fraudulent url that asks the user to enter their MFA credentials or prevents the attacker from seeing or getting the access control token from the MFA.

If neither one of those are true, then the MFA is not considered phishing resistant.

An easy way to identify phishing resistant MFA solutions are ones that comply with at least one of the following standards.

NIST 800-63-B AAL3-Level Solutions
NIST is the National Institute of Standards and Technology. Their standard states that at least one cryptographic authenticator used at AAL3 SHALL be verifier impersonation resistant.

FIDO2
FIDO stands for Fast Identity Online and is an alliance that created a standard for phishing resistant MFA.

There are a number of MFA solutions available. Before selecting one confirm that it conforms to one of those standards.

Anything else is not as secure and may not be any better than a username and password. In fact, it will be worse because you believe it is making you safer.

One Brightly Cyber helps keep you safer by providing alerts when your credentials are found on the Dark Web and providing them 12-24 months before other vendors. This gives you time to change compromised information, hopefully before something worse happens.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.