Top 5 Reasons to Leapfrog to Phishing-Resistant Authentication

IT and security are accustomed to transition from generation to generation of technology advancements. But, sometimes a leapfrog is not only possible but is the right way to go. Here are the Top 5 reasons to leapfrog to phishing-resistant MFA.

1 Recommended for security today and as a step to Zero Trust

A White House OMB "Zero Trust Cybersecurity" memo requires phishing-resistant MFA as a first step to Zero Trust. For both enterprises and government agencies, phishing-resistant MFA is achievable by selecting strong authenticators and an architecture with known parameters (such as asymmetric cryptography to defeat hackers). These are well-understood requirements that are achievable with the right approach.

2 Phishing-resistant MFA Applies Across the Authentication Board

Phishing-resistant MFA applies across authentication methods including Certificate-Based Authentication, across a wide range of authenticators (some phone authenticators, smartcards, and USB keys), and for needs ranging from enterprise to government. So, it can be readily adapted for the various scenarios needed by your organization.

3 When done right – Phishing-resistant MFA is more efficient for end users

In addition to well-documented vulnerabilities, MFA based on one-time passwords or codes is bothersome to end users in many ways. It takes a lot of time to authenticate, with frequent re-sending of credentials when the "push" email or text goes astray or times out. Phishing-resistant MFA relies on an authenticator code (e.g. PIN) or user-specific characteristic that is fully secure, easy to provide, and saves time for each and every authentication request.

4 Phishing-Resistant MFA enables systematic and programmatic authentication

Since the authentication process is part of an integrated online process, Phishing-Resistant authentication is fully programmable. And, when coordinated by a platform that spans all the various users, machines, interactions, and environments that need authentication, authentication can be systematic as well.

5 Phishing-resistant authentication makes IT and security more productive

Today's authentication lifecycle is onerous for IT – for example, credential resets alone consume 40% of enterprise help desk resources. By standardizing on a programmable phishing-resistant authentication approach, IT and security teams can streamline their work – from initial enrollment of authenticator to the entire lifecycle of the credentials for the end user, machine, or application. And, this makes all teams – end users, IT, and security – more productive.

Learn more about Phishing-Resistant Authentication in our blog.