# Lab 2.2: Applying Marketing Models

Now that you understand the importance of explaining the WHY to effectively change behavior, you are going to apply the AIDA model to help communicate that. Your end goal is to create a marketing campaign where your workforce comes banging on your door wanting to use MFA (or a different initiative, if you wish). Let’s leverage the AIDA Marketing Model to figure out how you can do just that.

## STEP #1: ATTENTION

You must first get people’s attention and have them take notice of you. Often, this starts by describing the problem you want to solve. What message will you use to get their attention? What is the problem you are attempting to solve?

## STEP #2: INTEREST

Once you have their attention, you then need to generate their interest. What does your solution do? How does it solve the problem you described in the first step?

## STEP #3: DESIRE

Persuade people. You are changing their mindset from “I Like It” to “I Want It.” What value or benefit does your solution provide them or the organization? One approach is to focus on the “WIIFM,” or how they will personally benefit from your initiative.

## STEP #4: ACTION

Enable them to take action. In sales, this is called “conversion” or “call to action.” Good marketing creates a sense of urgency. How do you get them to start enabling or using your new solution?

*Phishing-Resistant MFA is an advanced form of MFA that vendors and organizations are beginning to roll out. In fact, we are* [*seeing recent government requirements*](https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf) *for phishing-resistant MFA to be implemented. What exactly is it, what are the benefits, and what does it mean to you and your organization?*

**What Is Phishing-Resistant MFA?**

Authentication is the process of confirming someone’s identity. In other words, are they really the person they claim to be? Every time you log in to a website with your username and password, you are authenticating. Traditionally authentication has been a username and password combination. Your username states who you are, and knowledge of your password confirms your identity. The problem with passwords is they are painful and confusing for people to use and relatively easy for cyber attackers to compromise. There are multiple ways a password can be compromised. While they may have been “good enough” 10 to 20 years ago, passwords are no longer good enough today.

As a result, a far stronger form of the authentication was developed, something called *two-factor authentication*.  As the name implies, for this stronger form of authentication, two factors are required—usually something you know (your password) and something you have (your mobile device) or something you are (biometrics). This way, if your password is compromised, your identity is still safe, as a cyber attacker does not have access to the second method (such as your mobile device). This concept is similar to your ATM card when you withdraw money. To successfully withdraw money, you need both your ATM card and your personal identification number (PIN). This is why you never want to write your PIN on your ATM card.

This layered method is a far stronger approach, and one many organizations and websites are adopting. In fact, two-factor authentication is quickly becoming a standard because it is so effective at stopping authentication-based attacks. However, there are several problems.

First, we have to agree on what we want to call it. Originally the most common term was two-factor authentication, as two factors were involved, but other names are often used, including two-step verification, strong authentication, and one-time password (OTP). However, most of the industry seems to be standardizing on the term multifactor authentication (MFA). Quite often, people are confused, thinking there are differences in these terms (and there can be), but in general these terms refer to the same thing. We will use the term MFA moving forward.

Unfortunately, not only do we use different names for the solution, but they are implemented in many different ways. Three of the most common ways at SANS we see MFA implemented are as follows. You first log in to your account with your username and password, then either …

1. A unique code is texted to your mobile device.
2. A unique code is generated in a mobile app on your mobile device.
3. A unique code or request is pushed to your mobile device.

There are other variations of MFA, but almost all of them share a weakness—human interaction is required. You have to do something with the code—and where human interaction is required, people can be phished. In other words, a cyber attacker can insert themselves in the authentication process. After a victim logs in to a website, and after a victim gets their unique MFA code, that code can then be tricked out of the victim and used by the cyber attacker to gain access to the website. In other words, these approaches to MFA are “phishable.”

Now, before you panic, any one of these MFA methods is exponentially better than just using a password alone. Should we stop using MFA because it is “phishable”? Absolutely not. The MFA methods have huge value. However, cyber attackers are only going to get better at exploiting the human side of MFA. So, what’s next? Phishing-resistant MFA.

Phishing-resistant MFA is nothing more than the same authentication process we just described, but people are removed from the equation. There are several different ways to implement this, but we’ll walk you through the most common approach, called FIDO. [FIDO](https://fidoalliance.org/what-is-fido/) is a standard created years ago by the [FIDO Alliance](https://fidoalliance.org/overview/), a nonprofit team of multiple organizations from around the world. This vendor-neutral standard is being adopted by most of the big players, including Google, Amazon, Microsoft, and Apple. So how does it work?

When you create an account online (or update an existing account to use FIDO), you register your device with the website. This device can be a special token (like a [YubiKey](https://www.yubico.com/products/)), or you can use your mobile device (e.g., your smartphone) as the token. When you register your device, it and the website create a cryptographic key pair unique for your account (known as asymmetric encryption or public-key cryptography). Although you don’t need to know the technical details, what happens is that, based on this key pair, the website now “knows” and trusts your device. In the future, to log in to the website, you simply log in with your device—quite often, no password is required.

From a user perspective (which will vary from website to website and device to device), all that happens is that when you visit a website you have created an account for, it will ask you to verify yourself with the device. To ensure that it’s really you with your device (as opposed to someone stealing your device and trying to log in as you), you will be asked to prove it is really you via biometrics (fingerprint, face scan, etc.). From the user perspective, the entire authentication process is nothing more than biometrics.

What makes this so effective is that there is no unique code to phish or trick people out of. Almost everything happens between your device and the website. The only human interaction is the biometrics—something people already do every day. So, we have a solution that is not only far more secure, as it far more resistant to phishing attacks, but also far easier for people to use. Does this technology eliminate all risk? No. As it becomes widely deployed, new attacks will be developed, but it will be MUCH harder for the cyber attacker.

“Passkey” is the name members of the FIDO Alliance have given this new form of authentication. In fact, [Apple released passkeys as part of iOS16 and MacOS Ventura](https://www.wired.co.uk/article/apple-passkeys-password-ios16-ventura), so expect other big companies to be announcing these features soon (if they already haven’t). Hopefully this gives you an idea of what “phishing-resistant” MFA is.

## *Note: FIDO is extremely resistant to phishing attacks, but adopting FIDO does not mean your organization is secure against phishing. A huge number of phishing attacks have nothing to do with passwords (infected email attachments, BEC, call-this-phone-number attacks, etc.). We’re bringing this up because we’re seeing organizations implying that because they’ve adopted FIDO MFA, they can't be phished. Not true! Some of the most effective phishing emails out there have just one or two sentences and a phone number for the victim to call. So remember, “phishing-resistant MFA” and standards like FIDO are incredibly strong authentication mechanisms that are highly resistant to phishing attacks, but there is a HUGE number of phishing attacks that have absolutely nothing to do with authentication.*