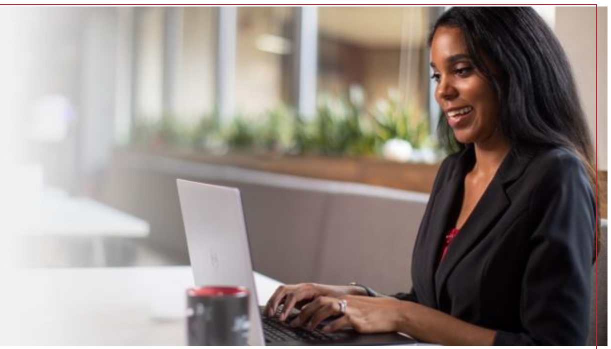
okta + BAYADA®



How to Create Strong Passwords

When you setup your new Okta Single Sign On login account with Multifactor Authentication, picking a strong, unique, hard-to-guess password will make it difficult for malicious hackers to break in and steal your identity. Here are four simple tricks to help you create passwords that are easy for you to remember, but virtually impossible for others to guess.

Tip # 1

DO NOT reuse the same password for multiple accounts.

This may be the biggest and most common mistake out there. It may not be a big deal if someone hacks your coupon account, but if they can use that same password to get into BAYADA and your bank account, that is a big security problem.

If you find it hard to remember a different password for every website, you can save them all in one password manager. A ‘password manager’ or ‘password vault’ is a software program that securely stores passwords and automatically fills them into login pages. It also helps you generate and save strong, unique passwords when you sign up with new websites. Just make sure that password vault has a strong password!

Tip # 2

The strongest passwords have 8 to 16 characters, a combination of upper and lowercase letters, at least one number, and at least one symbol.

The length and complexity of a password provides more security because it is harder—and more time consuming with every character—to guess. Hackers use automated software to submit hundreds of thousands of guesses per minute trying to access your online account. Some of these software programs, called 'dictionary' or 'brute force repetition' tools, use English dictionaries to sequentially guess your password.

How to remember a unique, strong password

Memory Trick # 1

Use an easy-to-remember sentence.
Pick a phrase you like, then use the first letter of each word to create a fun, easy-to-remember passphrase. For example, “The best time of year is spring”—use the first letter of each word to create a passphrase: Tbtoyis (notice the upper and lowercase letters). That is your base.
Then, add memorable numbers and symbols (avoid personal information that can be found online, such as birthdays, anniversaries, birth years, street address, or zip code). Examples: Tbtoyis25% T8b8t8o8y8i8s!! @Tbt0y1s

Memory Trick # 2

Use keywords related to one topic.

Choose something meaningful to you such as a trip, a life event, a movie, a song, a hobby, or anything that catches your interest. That is your topic.

Each time you create a unique login password, start with a hard-to-guess word associated with that topic (avoid personal names or places that can be found online). For example, if your topic is your honeymoon, you can start with something you ate there—pineapple (a nice long word). Pineapple is your base. Then, add upper and lowercase, number(s), and symbol(s). For example, pineapple could become P1ne@pp13 as a password.

These tips and tricks should be applied to both your work and personal accounts to protect your identity.
If you have any questions, please contact our IT Service Desk office at 215-757-9000.