Multi-factor Authentication Frequently Asked Questions

Brad Christ - 2023-07-14 - Comments (0) - Multi-factor Authentication

Question

Looking for specific information about multi-factor authentication in Okta? See our companion article All About MFA Factors in Okta.

What is multi-factor authentication?

Multi-factor authentication adds an extra layer of security on your account by requiring you to have something you know (username and password) and something you have (e.g. cell phone or hardware token). When applications and services require multi-factor, it will prevent anyone but you from accessing using your account, even if someone else knows your password.

SOU uses Okta for multi-factor authentication.

Why does SOU require multi-factor authentication?

Multi-factor authentication safeguards your account and all the data it contains or can access from being compromised due to a compromised password. Passwords can be compromised through many forms of attack: phishing, password cracking, password leaks from third-party websites and services, reusing passwords, using weak passwords, etc. Passwords alone no longer provide a sufficient degree of safety. Most password breaches can be stopped by multi-factor authentication.

In addition, compliance and regulatory concerns compel us to implement multi-factor authentication. As a university, we have a duty to protect the information entrusted to us by students, and using multi-factor authentication on our accounts is an important safeguard to meet that obligation.

What are the benefits of using multi-factor authentication?

The main benefit of using multi-factor authentication is it protects your account. If you receive a security code or a push notification when you are not trying to log in to your account, you'll immediately know that someone else is attempting to do so and has your password. If this happens, you should change your password and contact infosec@sou.edu immediately! (You can also reach the Information Security Manager at 541-552-6893.)

- Multi-factor authentication adds an extra barrier between your personal information and the bad guys.
- Multi-factor authentication can help keep attackers from accessing your email, documents, payroll, personal information, or research data--and in many cases the sensitive information of others that has been entrusted to you.

- Multi-factor authentication reduces the risk of hackers using your SOU account to perform harmful activities.
- Multi-factor authentication helps protect SOU's systems from harm, reduces our risk, and helps us prove to auditors, insurance providers, and regulatory bodies that we are taking cybersecurity seriously at our university.

I don't have anything confidential in my account, why should I care about multi-factor authentication?
Many attackers are not even interested in your data--although they might be, and you would be surprised what they can glean from your emails and documents. Hackers are more than happy to steal your digital identity through compromising your account so that they can infiltrate our networks and systems or use your identity to socially engineer others in an attempt to compromise even more accounts. In some cases, institutions have suffered devastating ransomware attacks costing millions of dollars in damages all because one person lost control of their account. Don’t be that person. Always protect your SOU account like it has value.

Can I also enable multi-factor authentication for Google?
Yes! To enroll, visit the Google 2-Step Enrollment page. Please note that you can use the Okta Verify app in place of the Google Authenticator app for registration. Okta Verify supports the same kinds of codes and can be used anywhere Google Authenticator is offered.

Why would I want to enable multi-factor authentication for Google in addition to Okta?
Some Google apps and services, such as Drive/Drive File Stream and Chrome, bypass the normal SOU login page. To protect those apps, you must also enable Google 2-Step Verification.

Do I have to use a mobile device?
There are several methods that can be used, including a mobile device app, SMS text message, and voice phone call options. While using a mobile device is most convenient option and the one that most users prefer, faculty and staff may request a hardware token instead. We have a limited supply of standalone hardware tokens available for one-time codes. Contact infosec@sou.edu for more information.

Can I use Okta without downloading the Okta Verify mobile app?
Yes, you can. If you do not want to download and use the Okta Verify mobile app on your smartphone, you can register your phone directly to receive one-time codes via text message or phone call.

Does SOU gain control of my personally-owned mobile device once I install Okta Verify or Google 2-Step Verification?
No!

By installing Okta Verify or Google Authenticator on your mobile device, you do not provide SOU with any additional ability to access your device or monitor your personal activity.

Who is required to use multi-factor authentication?

Anyone who has an SOU account is *strongly encouraged* to configure multi-factor authentication in Okta and on their Google account. Please see our multi-factor authentication policy at https://inside.sou.edu/it/it-policies.html for more information about who is required to use multi-factor authentication.

How do I get started?

See our companion article All About MFA Factors in Okta.