COLORADO

Governor's Office of Information Technology

Serving people serving Colorado

# Google 2-Step Verification

| | |
|---|---|
| **Nomination Category** | Cybersecurity |
| **Nomination Contact** | Brandi Simmons<br>brandi.simmons@state.co.us<br>303.818.5982 |
| **Project Initiation Date** | May 2016 |
| **Project Completion Date** | November 2016 |

## I. Executive Summary

“Hello. I’ve sent you a confidential document. Enter your username and password to open it.”

That’s how it often begins. A simple email, coming from what may appear to be a known and trusted source. It ends with credentials being harvested across hundreds or even thousands of accounts. IT staff scramble, trying to track and stop the phish from spreading and IT executives are forced to explain that this cyber attack was successful because an end user unknowingly gave his or her credentials up in a phishing attack. In the IT world, it’s like a wildfire, both in terms of mobilization to stop it and the way the threat is ever-changing. These scenarios play out every day in offices across the country. It happened within executive branch agencies at the State of Colorado but it was not going to be tolerated by the Governor’s Office of Information Technology (OIT). Early in 2016, OIT’s Google Team along with the state’s Chief Information Security Officer began planning the project that would prevent successful phishing of state Gmail users. By the end of 2016, we achieved 100 percent compliance with Google 2-Step Verification (2-Step) and reduced successful phishing attempts across Gmail users to zero.

## II. Project Narrative
## Concept

State of Colorado executive branch agencies have been using what was called Google Apps for Government, now G Suite, since 2012. OIT chose this as an enterprise solution to eliminate 15 aging and disparate email systems and to streamline cost and work time through the use of collaborative tools. To date, Google has resulted in $14.7 million in cost avoidance for the state.

There are 32,000 Google accounts across the state enterprise. Along with Gmail, 16.4 million documents are stored in Google Drive, and it is widely used for collaboration internally within each agency, between agencies, and with community partners and local governments. Despite efforts to educate end users on best cybersecurity practices, phishing and spear phishing attempts were occurring with increasing frequency and complexity, making it difficult for even some of the most savvy users to recognize and avoid the phish.

What we did:

To combat the growing number of phishing attempts, OIT sought a solution that could be implemented relatively quickly and offer a two-factor authentication process with multiple options to accommodate both user preference and the fluctuating security environment. The Google, or G Suite, off-the-shelf 2-Step Verification functionality met those basic requirements.

Google 2-Step adds an extra layer of security that requires users to provide more than just a password and username to access their account. Users receive a code generated from Google and must enter that code as a second step of authentication. The code is provided to them by phone, text, or a set of one-time use codes that can be downloaded.

How it worked:

On July 12, 2016, the Office of Information Technology became the first state office to implement 2-Step. In the first week there was a 70 percent adoption rate. It was opened to the remaining state agencies for enrollment on Sept. 13, 2016 with an implementation window of 60 days leading to enforcement by Nov. 15, 2016.

Key reasons for the successful rollout were effective communication, a focus on change management, and ensuring there was strong support for such a change at the executive leadership level. Our communication and change management plan involved gaining buy in from leadership - both at OIT and within the executive branch agencies we serve. It also encompassed a high level of user accountability. Communication elements were created for both digital and print platforms with elements that included direct email, newsletters and posters. Our efforts at the top level helped us understand the specific needs of each agency and allowed us to create solutions to address them. IT Directors and agency leadership were kept informed of enrollment at their agency. Throughout the enrollment period we created targeted communication to those end users who had not yet enrolled reminding them of their responsibility in this initiative.

## Significance

By implementing 2-Step Verification, OIT has taken a powerful step in securing state systems and data that could be accessed by unauthorized individuals as a result of the credentials obtained through a phishing attack. On a broader level, the implementation and enforcement of 2-Step for State of Colorado employees has illustrated that the task of implementing two-factor authentication is achievable within the public sector.

While there were certain hurdles to the full implementation, the flexibility to develop solutions allowed OIT to overcome those challenges and facilitate enforcement. One of those solutions was something we called the Code-inator.

A problem that we encountered among some of our state employee population was the resistance to using a personal cell phone to receive the second factor code. There was also the most challenging and unique use case - state employees who work in correctional facilities or state hospitals where mobile devices or hard tokens cannot be in their possession during the work day.

The most straightforward solution for these employees was the use of backup codes. G Suite allows the user to generate a set of ten backup codes that can be downloaded or printed. But, as the name denotes, these backup codes were to be used when the user could not access the code sent via text or voice. It

was not designed to be a primary method of authentication. The challenge to our state Google Team was to design a solution that allowed for the generated backup codes to be the primary method for second factor authentication.

While several different solutions were presented, the most sustainable and beneficial was one we developed as an on-premise web app. Hosted behind our firewalls and only accessible through specific state IP addresses, this web app allows users to enter a separate username and password to retrieve backup codes without needing a printout or any other physical device. We call it the Code-inator. It is successfully being used at three of the state agencies OIT serves. The ability to develop this solution to meet our customer's needs was the key to achieving 100 percent compliance with 2-Step among our user base.

## Impact

The State of Colorado's security teams fight vulnerabilities every day. Currently, the state receives more than 8.4 million security events every day. Many of these are phishing attempts. The most common and costly type of successful phishing attack against the state has been an attempt to gather Google login credentials. The implementation of Google 2-Step Verification has eliminated these types of successful phishing attacks. It is expected to save the State of Colorado more than 150 hours each year that had previously been spent on fighting phishing.

Google 2-Step was needed to protect the information of Colorado's state employees, residents and businesses. Common actions like using the same password for multiple accounts, downloading unapproved software, and clicking on email links put employees at risk for having their passwords stolen. Google 2-Step prevents hackers from getting private, confidential or sensitive information from Gmail or Google Docs belonging to state employees. With 2-Step, attackers are stopped when they try to send out emails not actually generated by the owner of the email address or when they try to control the account.

The State of Colorado's 2-Step Verification implementation puts the state at the forefront of cybersecurity innovation, and is one of the first to make two-factor authentication mandatory for all state employees.