Recent security changes implemented by Google have resulted in some changes to the way information must be accessed, collected and verified from Gmail accounts, and mail accounts hosted through Google Apps. In order to avoid collection delays and frustrations, companies should prepare themselves ahead of time for dealing with these issues during a collection.

**WHAT YOU NEED TO KNOW:**
There are two relatively new security measures and accompanying best practices that are important:

1. **Verification Codes**
   In order to increase security, Google sometimes requests a verification code when a user attempts to access a Gmail account from a browser or machine that has not previously accessed an account. Without the verification code, the account cannot be accessed. Verification codes can only be obtained by the account holder in certain ways (e.g. – a text message sent by Google to a pre-configured cell phone; via an application called “Google Authenticator,” etc.).

2. **Two-Step Verification**
   If a user or organization has chosen to enable two-step verification for their Gmail or Google Apps accounts, collection teams will need to obtain something called an “application-specific password” that can only be generated by the custodian or the account administrator.

**WHAT DOES THIS MEAN FOR YOU?**
Part of the collection process will involve logging into the email account through a browser to verify message counts and other information, which may prompt a Google request for a verification code. To speed collection times, it’s important to:

- Be aware of any users with mobile devices linked to such cloud accounts for the purpose of retrieving or generating verification codes.
- Provide your collections team with access to these users and their mobile devices as necessary.
- Alert these users that a collection will be occurring, and ask them to be ready to provide verification codes during the collection. Note that verification codes change every 30 seconds, so collection teams must work with these users in real time.

To speed collections when two-step verification is enabled, it is important to:

- Allay privacy concerns with custodians before the collection begins: Assure custodians that the application-specific password generated for the collection can be deactivated by them at the conclusion of the collection, thereby preventing future access to emails by the collection team.
- Prepare custodians or account administrators for the process that generating the application specific passwords will take: Ask them to expect a request to generate the password, and set aside time for them to do so.

Collecting from the cloud isn’t as easy as it seems, and enhanced security features like those implemented by Google have the potential to delay collections. With a little preparation, however, legal and IT teams can ease administrative headaches and overcome obstacles to a successful collection.