LawPracticeTODAY
THE MONTHLY WEBZINE OF THE ABA LAW PRACTICE MANAGEMENT SECTION

Set Up Two-Factor Authentication: What Are You Waiting For?

By Catherine Sanders Reach

February 2013

> “In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.”

Thus starts the story of Mat Honan, a writer for Wired Magazine. Mat’s story should be a cautionary tale for all, especially lawyers whose duties to maintain the confidentiality of client data extend the need for added security beyond just personal inconvenience. Mat admits that much of what happened could have been avoided by using two-factor authentication on his Google account and other security measures. So, why didn’t he do it? Because adding layers of security means adding a layer of complication, and sometimes inconvenience. However, to unravel from a firm security breach or hack would be even more inconvenient.

Google’s Gmail, Google Chrome, LastPass, Dropbox, WordPress and many other popular services have added an extra layer of security that a user must enable called “two-factor authentication”.   Gmail, Google’s widely used and free online email platform, was one of the first of the consumer cloud products to offer two-factor authentication. Since most online accounts require an email address, which often act as a user name, locking down your Gmail account with a really strong, unique-to-that-account password and turning on two-factor authentication will go a long way in reducing risk. Why? Because as Mat Honan explains, he had his online accounts “daisy chained” together with shared usernames, passwords and associated email.

What is Two-Factor Authentication?

The concept of two-factor authentication is that a person cannot access another user’s account without something she *knows* and something she *has*. In the case of these popular services, the solution is a strong password plus a secondary code that is sent via text to a smartphone or mobile device. Both are required to access the account. For two-factor access to laptops, devices like USB tokens and smart cards must be plugged in for the machine to boot up. Likewise, you can buy external biometric security devices, such as a fingerprint reader, which is a substitution for what the user *has* to what the user *is*. Let’s look at how to enable two-factor authentication for some of the most widely used cloud services.

Setting Up Two-Factor Authentication in Google

To enable two-factor authentication for Gmail you will actually be applying what they call "2-step verification" across your Google account, which means this will also help protect your Google Drive, Picasa, Google+, and any other Google online products you use. From Gmail, look in the upper right corner and click on the gear icon or the arrow next to your profile picture and go to your account. Then click on "security" from the left column. Click "settings" next to 2-step verification to get started. You will be asked to input a phone number and a backup phone number. Make sure these numbers are for phones that can receive text messages. Alternatively, you can get an app for iPhone, BlackBerry or Android instead of receiving a text message. Once you have done this, then every time you log into your Google account (Gmail, Drive, etc.) you will need to have your phone handy because you will need to enter your password and a one-time use code sent to your phone.

"But, wait…" you will start to say. Don't worry, some handy options make this foolproof and not at all onerous! As a tertiary precaution, Google supplies you with a one-time list of printable backup codes so that if your phone is unavailable you can still sign into your account. They suggest keeping the codes somewhere accessible, like your wallet. Also, you can create a list of trusted computers, like your home and work computers, which will not require the SMS code to access Google. In this way your usual workflow is not disrupted. Just check "trust this computer" the first time you enter the verification code and you will not have to enter the code again. However, for your portable devices, it would probably be wise to keep 2-step verification enabled. The primary goal here is to keep outsiders from hacking your Google account, not to make it difficult to use your own technology!

Other Google products that are not compatible with 2-step verification work outside of the browser, such as Google Voice mobile app for iPhone, some chat clients and Chrome Sync. For these, you will need to create an application-specific password. From the 2-step verification setup screen, click on "Manage application-specific passwords". Enter the name of the application, such as "Chrome at Home" or "GVoice on Phone," then click "generate password". Enter the newly generated password in place of your regular password, and voilà. From that same page, you can see which applications have these auto-generated passwords, and can revoke access at any time. This page also shows you sites, apps and services that you have granted access to your Google account, what they have permission to access, and you can revoke access with a click.

Setting Up Two-Factor Authentication in Dropbox

To turn on two-factor authentication in Dropbox, login to the web interface and go to settings – security – and click "change" next to 2-step verification disabled. The process is much the same as with Google, giving you a choice to receive security codes via text or a mobile app. It also provides an emergency backup code in case you lose your phone. Dropbox suggests you write it down on a piece of paper and keep it safe. Like Google, you can see which phones, computers and tables you have given access to your Dropbox, and can revoke access if necessary.

Setting Up Two-Factor Authentication in LastPass

The process is slightly different for LastPass, which uses a grid-based multifactor authentication for free accounts. In choosing to enable this, you can allow mobile and bookmarklet access to bypass the grid and allow offline access. Then, you must print a spreadsheet-like grid of random characters. Once activated, in addition to username and password, you will need to provide four random values off your grid based on coordinates given to you by LastPass. LastPass describes it as being like playing Battleship. Once you've entered the coordinates, you can choose to trust a particular computer. This may seem overly difficult, but remember that LastPass is used to guard all of your other passwords so it makes sense that the degree of difficulty is higher.

Conclusion

In my experience, using two-factor authentication has been transparent in my day-to-day usage after I set it up and trusted my few devices. Setup is quick and knowing that that a hacker cannot remotely access your email, documents, or stored passwords is worth the very small amount of time it takes to enable this extra security layer.

Catherine Sanders Reach *is the director of law practice management and technology for the Chicago Bar Association.*