Two-Factor Authentication: Simple and Powerful Security

By Andrew B. Stockment

You have probably heard horror stories about people whose personal accounts were hacked or companies that suffered data breaches that exposed their customers' information.[1] The personal and business repercussions of an account being hacked range from minor inconvenience to major embarrassment, a damaged reputation, and financial loss. For those of us in the legal profession, beyond merely protecting ourselves, we have an ethical obligation to take reasonable precautions to safeguard our clients' confidential information.

In order to prevent unauthorized access to your account, most online services (such as your e-mail provider and your bank) require you to enter a username and password in order to authenticate your identity and login to the service. Three big weaknesses of the username and password model are: (1) people often select weak passwords; (2) people often use the same password with multiple accounts, which means a data breach of one service provider allows hackers to access all the other accounts that have the same username and password; and (3) usernames and passwords are often compromised, such as by logging in to accounts over an insecure Wi-Fi connection that allows hackers to capture your password or through phishing attacks where hackers use social engineering to trick you into giving them your username and password (e.g., through a phony login page for your bank sent to you in an official-looking e-mail). By using two-factor authentication, you can add an additional layer of protection so that a hacker would not be able to access your account with only your username and password.

WHAT IS TWO-FACTOR AUTHENTICATION AND HOW DOES IT HELP?

Two-factor authentication (also commonly referred to as two-step authentication, 2-step verification, or multi-factor authentication) involves the use of two or more items (or factors) to authenticate your identity and gain access to the service in question. In most cases, the first item is your username and password combination. There are a variety of methods used to provide the second authentication factor, but the most common method of providing the second factor is for the user to enter a short numeric code into the website in addition to the username and password. In most cases, after entering the username and password, the user either generates the second-factor code using a smartphone app or the code is sent to the user either by SMS as a text message to the user's cell phone or by an automated phone call. This second-factor code can generally only be used once and is often time-sensitive, meaning that anyone who intercepted the code would not be able to use it because it would no longer be valid.[2]

Thus, if your account was protected with two-factor authentication, access would only be granted to someone who both (1) **knows** your username and password and (2) **has** access to your phone. The obvious advantage of using two-factor authentication is that a hacker would need to steal your phone in addition to guessing or intercepting your password (and you would probably notice pretty quickly if your cell phone was stolen).[3]

TWO-FACTOR AUTHENTICATION IS EASY TO USE

Although the precise method of two-factor authentication varies from site to site, in most cases configuring two-factor authentication is a straightforward process. For websites that provide two-factor authentication by text message or phone call, the setup process typically requires you to supply your phone number and then type the code that is sent to you by SMS or phone call. And that's it! Your account is setup and protected with two-factor authentication. The next time you login you will be required to supply the security code sent to you by SMS or phone call.

For websites that use a smartphone app to generate security codes, the setup process requires you to install a compatible app. Most implementations support standardized TOTP (time-based one-time password algorithm) apps, such as the free

Andrew B. Stockment
Associate, Lenhart Pettit (Charlottesville)

Practice Areas: Intellectual Property and Technology Law, Business Law, and Securities and Private Equity
Law School: University of Virginia School of Law (2009)
VBA Leadership: YLD Executive Committee (2014 – Present), Intellectual Property and Information Technology Law Section Council (YLD Representative, 2012 – Present), Law Practice Management Division Executive Council (YLD Representative, 2014 – Present), *Opening Statement* (Editor-in-Chief, 2012 – Present), YLD Communications/Publicity Committee (Chair, 2012 – Present),
Awards: Super Lawyers Rising Stars (2013 – 2014), VBA YLD Emerson G. Spies Award (2012)
Bio: Andrew was a software engineer before becoming an attorney, and he has been a lifelong technology and innovation enthusiast (including a particular interest in data security and privacy). When he is not practicing law or working on bar projects, Andrew and his wife Martha enjoy running, hiking, and watching U.Va. sports. Andrew's other articles and projects are available at: www.andrewstockment.com.
Contact Info: abs@lplaw.com or 434.220.9386 **Twitter:** @AndrewStockment

Google Authenticator, Duo Security, and Authy apps[4], meaning you don't need to install a separate app for each website. After installing the app of your choice, you then use the smartphone app to scan a QR code (similar to a barcode) displayed by the website during the setup process, and then you type into the website the short numeric code displayed by the app. You are then protected and ready to go. The next time you login to the website, you will simply open the app on your phone and type the short code it displays.

Most websites that support two-factor authentication will supply you with one or more backup codes that you should print and store in a safe location. The backup code would be used to regain access to your account if your phone was lost or stolen. Of course, if your security codes are received by SMS or phone call, if your phone is stolen, you will still receive the codes on your replacement phone once it is activated with your mobile phone provider.[5]

To make using two-factor authentication less inconvenient, many websites that support two-factor authentication allow you to "trust" the computer that you are currently using so that you will not be required to supply the second factor the next time you login from the same device. Of course, you should only trust your personal computer and you should not trust your device if you are connecting over an insecure Wi-Fi connection.

To determine whether a particular website or service supports two-factor authentication and the methods it supports, you may want to begin by checking: TwoFactorAuth.org. Websites that support two-factor authentication include: Google[6], Microsoft[7], Apple[8], Box[9], Dropbox[10], Facebook[11], Twitter[12], LinkedIn[13], Evernote[14], and Yahoo[15].

BOTTOM LINE: IT'S WORTH THE MINOR INCONVENIENCE

Two-factor authentication is fairly easy to setup. Moreover, it provides a meaningful additional layer of protection for your accounts and the sensitive information stored in those accounts. And for legal professionals who have an ethical duty to safeguard client information, a minor inconvenience for a substantial security gain is definitely worth it. After all, if your account was hacked and a client's information was stolen, your client would probably not be impressed with an explanation that "I decided not to setup two-factor authentication because it was too inconvenient."

Hackers employ many techniques to gain unauthorized account access and to steal sensitive information. There is no panacea that will provide complete protection, and there are many important steps that you should take to mitigate the risk of unauthorized account access, including the password best practices discussed below.[16] But using two-factor authentication is simple to setup, easy to use, and well worth the minor inconvenience of entering a second code when logging in to your online accounts.

PASSWORD BEST PRACTICES

In addition to using two-factor authentication, you should consider implementing the password best practices discussed below.

1. Never use the same password for multiple accounts

You should not reuse the same password for multiple accounts because, if a security breach causes the password to be revealed, the person who obtains it could then use it to login anywhere that you have used the same username/password. It is likely that you have already had one or more of your passwords stolen in one of the many, widely publicized security breaches (e.g., LinkedIn). In particular, you should not reuse the same password for any confidential, sensitive, or important information or accounts, including:

- Any account, device, or service used to store or access confidential client information
- Banks or other financial accounts
- Cloud storage services
- E-mail accounts
- Domain name registrars, DNS providers, or hosting services
- Network access (e.g., to access your law firm's network, VPN, or computer)
- Social networking services (because they are a rich source of personal information that could be used for identity theft or phishing attempts)

2. Use a reputable password manager

Examples of good password managers are: 1Password (www.agilebits.com), KeePass (www.keepass.info), Password Safe (https://www.schneier.com/passsafe.html), and LastPass (www.lastpass.com). (LastPass is widely respected, but unlike the other password managers listed above, it stores your encrypted password database online.) It is also critical to regularly backup your password manager database in a secure location and to make sure you are able to retrieve and decrypt that backup without needing a password or encryption key that is only stored in the password database itself.

3. Use a long, truly random master password for your password manager

The master password for your password manager should be sufficiently complex and random so that it is difficult (but not impossible) to memorize. If you follow the advice to use a password manager to generate and store random passwords for all your accounts, you will probably use the password manager and type your password often enough that it should be feasible to memorize and remember a fairly complex password.

The best practice would be to use a password generator to create a truly random password at least 18 characters long, with mixed case letters, numbers, and symbols. Avoid using "clever" patterns or techniques (e.g., substituting "3" for "E", "0" for "O", or "!" for "l"), all of which are incorporated into the password cracking tools used by hackers—and the speed of such password cracking tools is staggering and increasing all the time. In some cases, cracking tools are able to guess *hundreds of billions* of passwords *per second* or faster. Another alternative would be to generate a password using the "Diceware" method to generate at least eight random words to combine into your password.[17]

If you lose your master password, it could be extremely difficult to regain access to your accounts (particularly if your e-mail password is randomly generated and stored in your password manager). Therefore, you should be absolutely certain you will never forget the master password. It would be a good idea to securely save the master password (or steps to recreate

the master password). Despite some degree of debate on the subject, in most cases, it is reasonably safe to write down your master password on a piece of paper and secure the piece of paper. (Note: Placing a sticky note under your keyboard does not count as securing the paper.)[18] Until you are comfortable that you have memorized the master password, it is probably a good idea to *temporarily* keep the password, or sufficient hints to re-create the password, written on a piece of paper in your wallet.

4. Use your password manager to generate long, random passwords for all of your accounts

The best passwords are too complex for humans to remember (or at least to remember more than a handful), and people are notoriously bad at selecting passwords, even when attempting to select "random" or "complicated" passwords. According to one analysis: 40% of people have a password from the top 100 passwords, 79% have a password from the top 500 passwords, 91% have a password from the top 1,000 passwords, and 98.8% have a password from the top 10,000.[19] When people are required to select passwords using a mix of upper- and lower-case letters, numbers, and symbols, people tend to follow predictable patterns that are easily uncovered by password cracking tools. Instead of attempting to create unique passwords on your own, you should use your selected password manager to *generate* and *store* long, truly random passwords, at least 16 characters in length (longer is better), with mixed case letters, numbers, and symbols for all (or most) of your passwords.

5. Use false, random, and/or nonsensical answers to security questions

Online accounts frequently require or permit you to provide answers to security questions (e.g., "What is your mother's maiden name?") as a way to regain access to the account if you forget your password. However, the security question concept is fundamentally flawed and poses a serious security risk because it encourages users to answer questions for which there is only one true answer (and the answers are often readily discoverable in the age of Google and social media). Having a strong password is of little value if you have insecure answers to security questions. Some well-known public figures, including Mitt Romney and Sarah Palin, have had their e-mail accounts compromised by hackers answering security questions. A security answer is just another password, and anything that would make a bad password also makes a bad answer to a security question. The best practice would be to generate unique, random answers using a password generator and save them in your password manager. For example, website #1: mother's maiden name is: btYxsQb3jh9WgXBYr, website #2: mother's maiden name is: RCQEgVZKyoZRLBHM9. If you can't bring yourself to use different, random answers for each site, at a minimum you should make up false and/or nonsensical answers that you will be able to remember. For example: mother's maiden name: yellow, favorite dessert: spinach.

CONTINUED VIGILANCE

By using two-factor authentication and following the password best practices discussed above, you will substantially increase the security of your online accounts. But no security system is hack-proof, and you should continue to be vigilant, monitor your accounts for unusual activity, and keep current with evolving security best practices. ■

A previous version of this article was first published by the American Bar Association in Law Technology Today*, available at: www.lawtechnologytoday.org/2014/11/multi-factor-authentication-is-effective-and-easy-to-use/.*

Endnotes

1. One of the most famous examples of an individual being hacked was the 2012 hacking of Mat Honan, who was a writer for WIRED. See: www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/. Another horror story about hackers deleting someone's e-mails can be found at: www.theatlantic.com/magazine/archive/2011/11/hacked/308673/. Data security breaches at companies are numerous and widely reported, including the recent hacking of Sony Pictures Entertainment. See: http://bit.ly/2014DataBreaches.
2. Other second-factor methods include: (1) generating a security code using a hardware token or card, (2) entering a one-time use code received by e-mail instead of by SMS or phone call; (3) authenticating through an alternate channel, such as by approving a login request (a) through a smartphone app (Twitter or Duo Security, for example) or (b) by receiving a phone call and entering a PIN using your phone's keypad; (4) hardware tokens or security keys that must be connected to a computer during the login process; or (5) using biometrics such as fingerprints to authenticate. Some online services, particularly financial institutions, use security questions and answers as a supposed additional layer of protection when logging in from a device that does not have a login cookie stored from a previous login session. However, the answers to security questions are nothing more than a second password, and using two unchanging passwords does not provide much, if any, additional security and should not be considered genuine two-factor authentication. Moreover, people frequently pick even weaker answers to security questions than they do for their passwords. See also: www.theatlantic.com/technology/archive/2012/08/security-questions-the-biggest-joke-in-online-identity-verification/260835/.
3. Different implementations of two-factor authentication provide varying degrees of security, and none of them are completely secure. For example, someone could hack into your cell phone account and forward your calls or text messages, or someone could steal your phone or your security key. See: arstechnica.com/security/2014/11/cell-carrier-was-weakest-link-in-hack-of-google-instagram-accounts. But any method of two-factor authentication provides an additional layer of security to protect your account and the information it contains.
4. Google Authenticator: http://goo.gl/mKEWGt; Duo Security: https://www.duosecurity.com; Authy: https://www.authy.com/users/.
5. For some services, such as Apple, it is critically important to save the recovery key (or backup code) that is generated when setting up two-factor authentication. For example, if someone makes too many unsuccessful attempts to login to your Apple account, Apple will place a security lock on your account, and the only method of regaining access to your account is with the recovery key—even if you know your password and have access to your two-factor device. See: http://tnw.to/t3Mmh.
6. https://www.google.com/landing/2step/.
7. http://windows.microsoft.com/en-us/windows/two-step-verification-faq.
8. http://support.apple.com/en-us/HT5570.
9. https://support.box.com/hc/en-us/articles/200526658-Can-I-enable-2-step-verification-for-my-account-.
10. https://www.dropbox.com/help/363.
11. https://www.facebook.com/help/148233965247823.
12. https://support.twitter.com/articles/20170388.
13. https://help.linkedin.com/app/answers/detail/a_id/544/ft/eng.
14. https://blog.evernote.com/blog/2013/10/04/two-step-verification-available-to-all-users/.
15. https://help.yahoo.com/kb/SLN5013.html.
16. It is also important to keep in mind that two-factor authentication is not foolproof and can be circumvented if not implemented correctly. For example, see: shubh.am/how-i-bypassed-2-factor-authentication-on-google-yahoo-linkedin-and-many-others/.
17. See: www.diceware.com. Attempting to think of random words on your own is not sufficiently random.
18. See: www.schneier.com/blog/archives/2005/06/write_down_your.html.
19. See: http://xa.to/1P and http://bit.ly/500WorstPasswords. ■