SAFEGUARDING DIGITAL DATA

BY NICHOLAS SHOOK, ESQ.

Target, Home Depot, eBay: all big companies that sell a lot of merchandise online. But that's not the only thing they have in common; each company has lost tens of thousands of user account passwords, enabling attackers to log in as another person and act maliciously under the guise of that person.

As lawyers, we are asked to be guardians of our clients' secrets. One mistake could cripple a client's case and leave us vulnerable to malpractice lawsuits. With nearly all data stored on digital drives today, it is paramount to take as many precautions as possible to protect client data.

In this article, I will lay out suggestions about best practices in authentication and encryption, based on my experiences as a professional software developer. Authentication, to developers, means ensuring that the user of an application is, in fact, that person. Understanding how authentication works will help you understand how to keep your digital data safe. But first, some background on cryptography.

Sharing and keeping secrets is nothing new. Since writing was invented, people have been sending hidden messages to each other. With secrets came people who wanted to be privy to the secrets, and therefore intercepted these messages. The secret-keepers, knowing that there was a chance their messages could be stolen, developed cryptography, the art of concealing text from any reader unfamiliar with the key intended to uncover its meaning.

Among the earliest forms of cryptography were single-substitution ciphers. Using this method, each letter was replaced by another letter in the alphabet; a phrase like "Nevada lawyers" could be written as "Pzexox axlbzcg." Unfortunately for the secret-keepers, these codes were not hard to break (and are now featured in children's brain-teaser books). Consequently, the secret-keepers evolved their codes, using multiple substitutions or numbers to encrypt a message. With each evolution in encryption, code-breakers evolved too, which in turn raised the standards of encryption. Simon Singh's excellent "The Code Book" delves into the history of codes and code-breakers, and is a great read if you find this topic interesting.

Relating back to software and digital data, logging into a software application is no different from sending and reading secret messages; it

is simply an example of how cryptography has evolved as of 2014. The most common technique used in protecting digital secrets is asymmetric cryptography.

Asymmetric cryptography involves the use of two keys. One key, the public key, is shared with abandon among any programs wishing to use the key; the other key, the private key, remains a secret, as it is the only thing that can decipher the public key. A private key can be thought of as a password used to log on, and oftentimes it is. Fortunately for secret-keepers, it is nearly impossible to decrypt asymmetric cryptography without knowledge of the private key. With encryption algorithms like RSA, Blowfish and SHA-2, it would take every computer on earth thousands of years to run all the calculations necessary to break the code.

As such, the biggest current risk to digital security is known as a side-channel attack, which occurs when an attacker obtains one's private key. Side-channel attacks most commonly occur through phishing, where an attacker feigns agency from a trusted entity like a bank and an individual acts upon that representation. To prevent side-channel attacks and ensure proper authentication, I recommend encrypting your data, using strong passwords and two-factor authentication, only connecting to secure wireless networks and websites with SSL, and checking for duplicate uses of your name.

Encryption is not set up by default on Windows or Macintosh computers, however it is built into both operating systems. Please refer to instructions on BitLocker if you are running Windows, or FileVault if you are running a Mac, to encrypt all the data on your machine. Both solutions offer full-disk encryption, meaning that if someone were to get ahold of your computer, they would need a private key to decrypt any file on your machine. When using a cloud service such as Dropbox or Clio, make sure the service offers full encryption of all data uploaded (both of these companies do).

It is surprising how many people, including lawyers, use awful passwords for important Internet accounts. Please never use a plain-language word, especially "password," for Internet accounts. The best practice is to use an array of random passwords, such as "ao)@@3eugqkrch4134," that are unique to each application. I highly recommend a password manager like 1Password, or the default Keychain Access that is built into Macintosh and enables users to randomly generate and save unique passwords for every application they use.

Two-factor authentication simply refers to using more than one way to authenticate yourself to a program. It is most common to have two-factor authentication with a cellphone, so both a password and a randomly generated code only seen on a person's cellphone are necessary to

continued on page 24

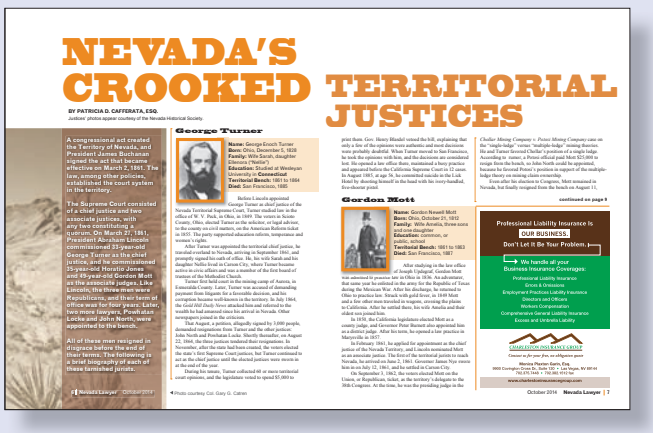
LETTERS TO THE EDITOR

continued from page 5

the oral histories we have published, available at the UNR Oral History Program website. We added eight more oral histories to the collection last year, for a total of 17, and we have funding dedicated to the production of more to come.

The October issue's editor, Ms. Cafferata, and your contributor, Ms. Timko, are members of our society. We invite your readers to explore our website and to join us in these efforts.

Thank you,
Peter J. Smith
Nevada Judicial Historical Society ■



NEVADA'S CROOKED TERRITORIAL JUSTICES

BY PATRICIA D. CAFFERATA, ESQ.

Justices' photos appear courtesy of the Nevada Historical Society.

George Turner

Gordon Mott

I really enjoyed Patricia Cafferata's article on the Crooked Territorial Judges. I realize there were space limitations in article, but I have to point out that John W. North was very busy before and after he lived in Nevada and probably the only Nevada attorney who founded not one, but two cities (Northfield, Minnesota and Riverside, California)! He also was nominated, but was not elected, to the California Supreme Court after he left Nevada. Among other honors, there is a high school and a park named after him in Riverside.

Again, wonderful job on this article in particular and this entire issue of *Nevada Lawyer*.

Matthew Wm. Nelson, Esq.
Gresham Savage Nolan & Tilden, PC ■

SAFEGUARDING DIGITAL DATA

continued from page 23

authenticate that user. If you use software with the option of two-factor authentication, such as gmail, Facebook or Dropbox, you should enable such authentication immediately. If you use a website or application that does not have it, it might be worthwhile to submit a ticket to that company requesting such a feature, especially if you have critical information on that service.

When connecting to a network, always be wary of networks not requiring a password. Oftentimes, devices save wi-fi information. Therefore, if you are connecting to an unfamiliar wi-fi network, set your device to forget that network. In regards to using websites, only trust websites with SSL, which creates a secure tunnel between your computer and the servers hosting the website. Otherwise, anyone can read your traffic with a packet sniffer program such as Firesheep.

Finally, in regard to authentication, don't let anyone pretend they're you. While this is fairly obvious, it is easier said than done. It is easy to spoof or imitate one's identity over the Internet. To safeguard from digital impersonators, I recommend checking to see who is using your name or moniker on http://namechk.com (built in Nevada).

These suggestions provide a baseline of what a lawyer needs to do to protect his or her data from malicious attackers. However, this list is by no means exhaustive, and like anything else in tech, will be outdated in the near future. Keeping abreast on safeguarding digital data is important, but not necessarily time-consuming. There are a plethora of great websites that aggregate what is necessary to keep your data secure. I recommend Mashable (http://mashable.com/category/online-security/), or if your prefer something more technical, Hacker News (http://news.ycombinator.com). ■

NICHOLAS SHOOK is a lawyer and developer for Q-Centrix, where he builds tools for hospital compliance and analytics. He can be reached at nicholas.shook@gmail.com for any questions pertaining to software.