PHILLIPS FINANCIAL
AN INDEPENDENT FIRM

BEST IN BRIEF
Insight and Inspiration from Phillips Financial

February 2017 Edition
Online Security: Avoiding Account Vulnerability

How many times did you login to a digital account today? It probably was more than once. Some people access digital sites via computer or tablet, but many others rely on their phones. *Deloitte* recently reported the essentials of life have expanded and now encompass air, water, food, and smartphones:[1]

> "The time it takes for us to pick up our phones in the morning continues to shrink: More than 40 percent of consumers check their phones within five minutes of waking up. As a first thing, we check our IM or text messages (35 percent), followed by emails (22 percent). During the day, we look at our phones approximately 47 times and that number rises to 82 for 18- to 24-year-olds. Once the day is over, over 30 percent of consumers check their devices five minutes before going to sleep and about 50 percent in the middle of the night."

No matter what device they choose, in order to access an account, users must prove their identity. Typically, proving who you are requires one or more pieces of information. These may include:[2]

- **Something you know**, like a PIN, password, or pattern;
- **Something you have**, like a code-generating phone or hardware token; or
- **Something you are**, as proved by fingerprints, voice recognition, or eye scans.

Before data breaches became an all-too-common occurrence, a lot of people relied on single factor authentication (SFA) to protect digital accounts. For example, a username plus a password. The single factor in this instance is your password.[3]

The rise of two-factor authentication

Today, more and more people are relying on two-factor authentication (2FA) to protect their accounts. With 2FA, you enter a username, a password, and a second factor. Often, the second factor is a temporary code that is sent to your mobile phone via text message (a.k.a. Short Message Service or SMS) or voice mail. This form of 2FA is remarkably convenient, but it may not provide the level of security you may want to have.[2, 4]

In July 2016, the *U.S. Department of Commerce, National Institute of Standards and Technology* recommended account providers – banks, retailers, financial companies, lenders, social media sites, messaging app providers, and so on – offer alternative ways to authenticate accounts, "Due to the risk that SMS messages or voice calls may be intercepted or redirected..."[5]

Duo Security cautioned that account holders should not rely on codes sent by text message or voice mail because:[2]

> "…on many devices, the default configuration allows an SMS to be visible on the lock screen. This can lead to accidental exposure of the passcode through shoulder surfing or if someone has physical access to a device that is locked but still active on the cellular network."

That's not the only way 2FA users may be vulnerable. Codes sent by text message and voice mail are not something we know, have, or are, rather they are something we receive. This means there is no way for the account provider to confirm an authorized user receives the code.[2]

Hackers have targeted the 2FA vulnerability

Forbes recently reported hackers have found ways to hijack SMS codes and steal millions. One victim,[6]

> "…was notified the passwords had been reset on two of his email addresses. He tried to set up new passwords himself by prompting the email service to send him text messages containing a code – but they never arrived. 'So I called the company to make sure I hadn't forgotten to pay my phone bill, and they said, you don't have a phone with us. You transferred your phone away to another company,' [the victim] says. A hacker had faked his identity and transferred his phone number from [one phone provider] to a carrier…that was linked to a…[voice] account in the hacker's possession."

The hacker received all of the victim's phone calls and messages and subsequently used them to reset passwords for email addresses and accounts by having the SMS codes sent to the victim's (and now the hacker's) phone number. It took just a few minutes for the victim to be locked out and the hacker to gain access to 30 accounts, including bank and payment processing accounts.[6]

There are 2FA options that provide greater security

While it is a good idea to change your security choices for accounts that are currently sending codes via text or voice mail, there is no need to panic. *Wired* pointed out:[7]

> "…attacks aren't exactly easy to pull off, and likely require the attacker to figure out the user's cell phone number in addition to the password that they've stolen, guessed, or reused after being compromised in a data breach from another hacked service. But for anyone who might be a target of sophisticated hackers, all of those techniques mean SMS should be avoided when possible for anything login-related."

Fortunately, there are other 2FA options that provide an improved level of security. *Wired* suggested using authentication applications or tokens that generate one-time codes. Both are more secure than SMS options.[7]

Keeping data secure online is a significant issue and the primary reason people continue to avoid accessing sensitive accounts electronically, according to the *Federal Reserve*. Staying up-to-date about security vulnerabilities and protections is critical if digital communication is an integral part of your life.[8]

Sources:
[1] https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html
[2] https://duo.com/blog/nist-shouted-who-listened-analyzing-user-response-to-nists-guidance-on-sms-2fa-security
[3] https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/
[4] http://www.abbreviations.com/SMS
[5] https://pages.nist.gov/800-63-3/sp800-63b.html
[6] http://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#7fc9cefb22db
[7] https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/
[8] https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf (Page 2 of report)