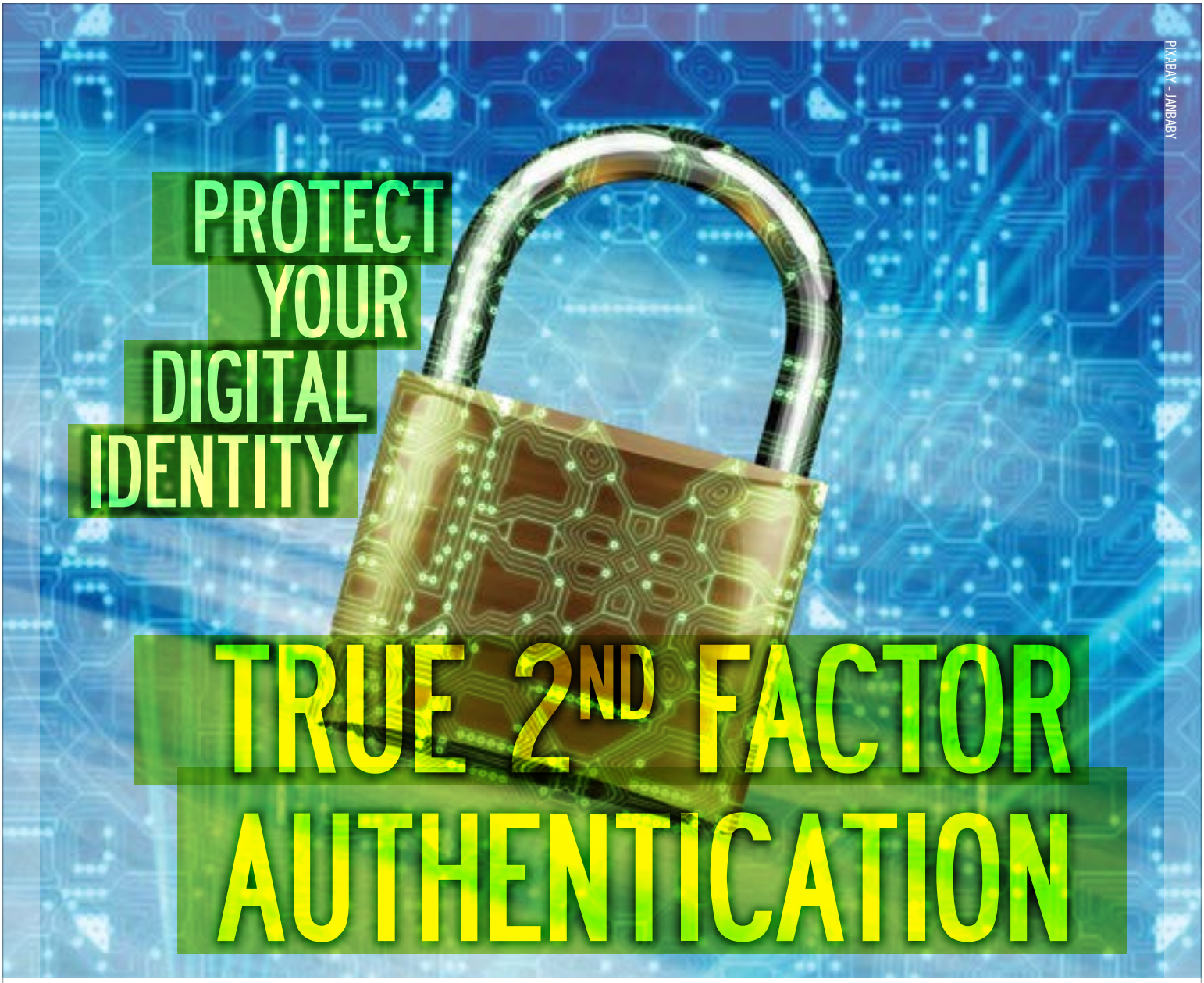

PIXABAY - JANBABY

PROTECT YOUR DIGITAL IDENTITY

TRUE 2ND FACTOR AUTHENTICATION

Imagine this. You have been waiting for years to find a parcel of land that you can call your own—not a small postage stamp lot in the middle of a city, but acreage that is at least thirty minutes from the general store.

BY **DR. BRANDEN R. WILLIAMS**

It's 3:00 p.m. on a Thursday and the phone rings. You don't recognize the number, but the caller announces herself as Sally from your title company. Her voice sounds familiar, and she is calling to let you know that she is emailing your wiring instructions to your Gmail account.

Sally mentioned that in order to close on time on Monday, you need to get the wiring instructions to your bank Friday morning, so they can schedule the wire transfer to go on Monday, first thing. She mentioned that it would be even better if you could get the wire transfer completed today, so the funds will be ready ahead of your closing on Monday. You remember your bank's cutoff time was 4:30 p.m., so you decided to get it done. After all, who wants to show up to close on their dream only to be turned away because of a bank error?

You thank Sally and disconnect the call. As expected, there is an email from Sally in your inbox with wire instructions and the correct amount to send. You call your banker, read off the info, and away the money goes.

The next morning you receive a call from someone claiming to be Sally from the title company. Sally tells you she is ready to verbally give you the wiring instructions for your closing and will send a copy via email as well. Confused, you ask her why she is calling again when the funds were wired yesterday. She sounds surprised, checks the escrow account and notices no funds were sent. As she reads you the account and beneficiary information, you realize in horror that you've been duped and your money was wired to a fraudster, not to the title company.

BUSINESS EMAIL COMPROMISE

The story above is fictional, but it is inspired by real events that happen every day.

The attack above is called Business Email Compromise (BEC) and exploits poor email account security of small companies and individuals. In the above case, it could be that your email account, your real estate agent's account or your title company representative's account was compromised. Everything about the transaction including the schedule for when you will close on your land are likely present in the email or calendar functions of one of those three parties.

Recent stats from the FBI from institutional filings and complaint data between June 2016 and May 2018 suggest that this problem is still a major issue and a growing concern. There were nearly 20,000 cases totaling over $1.6 trillion dollars in losses during that time.

To give you a comparison in scale, that is nearly three times the entire annual budget for the U.S. Department of Defense for 2018. Year after year, we are losing more money to BEC than we spend on keeping our country safe.

The underlying problem that allows this to happen is the fact that so many of our online accounts are protected with only a username and password. Some now add in SMS-based authentication, but this is inherently flawed as it relies on the security and process of cell network operators to maintain integrity during that process. SMS can be intercepted in more sophisticated attacks through malware and SS7 signaling attacks, or more likely, someone in a mall kiosk swaps your SIM for the attacker's and all of your calls and texts get routed to the attacker instead.

Other contributing factors are the victim's propensity to fall for covert elicitation attempts, social engineering attacks and our generally poor operational security around our online accounts. Common or repeated usernames and passwords without a second factor of authentication are trivial to compromise.

TRUE 2ND FACTOR AUTHENTICATION

To explain why SMS is not really a good factor for authentication, we need to understand more about how these networks work.As our reliance on telecommunications grew in the 1950s - 1970s, telecom carriers quickly realized they needed help with automation and signaling as they connected calls from carrier to carrier and land to air. SS7 was introduced with one key feature to combat abuse—the signaling is out of band.

For the more technical readers out here, older protocols used in-band signaling in which call setup information was sent on the same channel as their voice using various tones that users could manipulate.

Once we moved to out of band signaling, we solved one problem, but created another. The SS7 signaling protocol does everything from setting up and tearing down phone calls globally, sending an SMS, local number portability and number translations. It was not designed with security in mind.

BETWEEN JUNE 2016 AND MAY 2018, THERE WERE NEARLY 20,000 CASES TOTALING OVER $1.6 TRILLION DOLLARS IN LOSSES. WE LOSE MORE MONEY TO BUSINESS EMAIL COMPROMISE THAN WE SPEND ON KEEPING OUR COUNTRY SAFE.

It's not something we should trust for authentication, especially since a financially motivated employee at a mall kiosk could move your number to a new SIM he controls and start moving calls and texts to his new device instead of yours.

True second factor authentication takes many forms, but it normally takes the form of something you have. It could be a small device on your keychain with a rotating six-digit number or an app on your phone that gives you a code. Google, Facebook and Yahoo (ironically) have been working on alternatives that work pretty well. In fact, Google credits their use of the Yubikey (more below on these devices) to completely eliminate the effectiveness of phishing attacks, thus all but removing the threat entirely from their employees.

CONFIGURING TWO-FACTOR AUTHENTICATION

There are two base requirements you need in order to start configuring your true second factor of authentication. First, you need an authenticator. For consumers, those will come in two forms: either a FIDO/U2F compliant authentication device such as a Yubikey (www.yubico.com) or an authenticator app such as Google Authenticator or Authy on your smartphone.The second thing you need is a way to add it to your online account. Companies like Google (for Gmail), Facebook, Protonmail and Dropbox as well as Windows, Linux and macOS have all integrated authenticator apps or FIDO/U2F authenticators to add security.

EXAMPLES OF 2ND FACTOR AUTHENTICATORS

In the aftermath of the Snowden disclosures, he revealed both a number of tools and techniques used by the NSA to collect intelligence as well as showed how technologies such as TOR can be used to get around this monitoring. In a practical sense there are, of course, completely legitimate reasons to want to securely exchange information between parties—a digital dead drop. Here is a list of additional tools that you might find useful:

Google Authenticator (Check Google Play or Apple App Store) is a free authentication app that generates codes for a true second factor authentication option. It's extremely popular due to its ease of use. You scan a QR code from the website you want to enable the 2nd factor, verify it scanned correctly by entering the code displayed. That's it. You are done. Keep in mind, if you upgrade your phone you must move the tokens to your new phone before wiping your old one. This is where backups are critical in case you do something silly like forget to migrate your keys.

Authy (https://authy.com) is another freely available app that has more features than Google Authenticator, but it also has some quirks you need to be aware of. It is built for more flexibility, so they support the concept of transferring and managing your keys centrally among multiple devices, but that can be problematic if you are not paying attention to those devices or your Authy account. Consider this one perhaps more of a power user play.

Yubikeys (https://yubico.com/) are physical devices that plug in to the USB ports (or newer ones leverage Near-Field Communication for use with smartphones) that provide highly secure authentication using known standards and strong crypto. Keep in mind, there are many Yubikey copycats coming into play, including Chinese entrant Feitian. Some are better than others, but keep in mind the influence that nation states could have on authenticators for key personnel.

Krypton (https://krypt.co) is one of my new favorite FIDO/U2F authenticators that leverages the same open standards that Yubikeys do, but seamlessly integrates into your phone and browser. When you log in, instead of having to type additional codes, you can simply tap the prompt on your phone to provide the final step for authentication.

Some services offer specific authenticators that are unique to them. For example, Google offers a tap to authenticate option if you have one of their apps on your phone. Facebook may push a one-time password through their app for you to use. You should also expect banks in 2019 to roll out this functionality for mobile banking over SMS.

BACK IT UP

No matter which authentication technology you choose, you need to make sure you have a backup. If you are using an app on your phone, it's free and easy, but what happens if you lose or break your phone? If you buy a Yubikey, be sure you buy at least two. One should go in your safe in case you lose the primary.

Every company that implements a true second factor also allows for the use of backup codes. These are a series of one-time passcodes that can be used in the "Break Glass" scenario of losing other authenticators. Since you will ultimately remove your cell phone for SMS-based fallback authentication, downloading, printing and securely storing these codes is critical in case you end up losing your phone or losing your authenticator. You should consider making a copy of your codes and storing them offsite as well in case of a fire or natural disaster.

Remember, your goal is to remove the vulnerability of SMS-based authentication, but do it in a way that doesn't permanently lock you out of your online accounts.

ADDITIONAL READING

Did you know that Google wants you to stop using SMS in favor of their authenticator app? Check out this article from last year: https://brando.ws/googsms. SIM Swaps are a massive problem, but there are things you can do to help. Check this Wired writeup for details: https://brando.ws/wiredsimswap. For more details on the FIDO Alliance and the standards they publish, check this link: https://fidoalliance.org/. ✓

BIO

Branden R. Williams, DBA, CISSP, CISM is a seasoned security executive, ISSA Distinguished Fellow and technology executive sought after by global companies to consult on their digital business initiatives. Read his blog, buy his books or reach him directly at ***www.brandenwilliams.com.*** *His latest book on PCI DSS v3.2 Compliance is available on Amazon.*

GEAR REVIEW

GRAVITY WORKS

Whether you are hiking in the wilderness or filtering your own drinking water in a hotel room abroad, simply open the top, scoop water and close. Hang it and let gravity do the work. It filters up to 1.75 liters per minute with a microfilter lifetime up to 1,500 liters of water. They are individually tested to ensure it meets EPA & NSF guidelines for the removal of 99.9999% of bacteria and 99.9% of protozoa including: Giardia, Cryptosporidium, E. coli, Salmonella and Cholera. It weighs 11.5 oz. and stows smaller than most 1 liter bottles. It has an 8 liter (4L filtered + 4L unfiltered) total capacity to supply water for small groups and the microfilter can be back flushed in four seconds to maintain performance. **www.platy.com**