ANTIFRAGILITY PROCESSING GAME DIGITAL FOOTPRINT
SEPTEMBER 2015 ISSUE 23
TACTICSANDPREPAREDNESS.COM

TACTICS AND PREPAREDNESS

SKILLS AND SURVIVAL FOR ALL SITUATIONS

COMBAT RELOAD OR TACTICAL RELOAD

YOUR M4, M16 AND AR

BY: ERIC LEID | *PHOTOS COURTESY ERIC LEID*

When I evaluate the capabilities of shooters on the firing line, I look at their confidence and mechanical competence as well as marksmanship in determining their overall firearms proficiency.

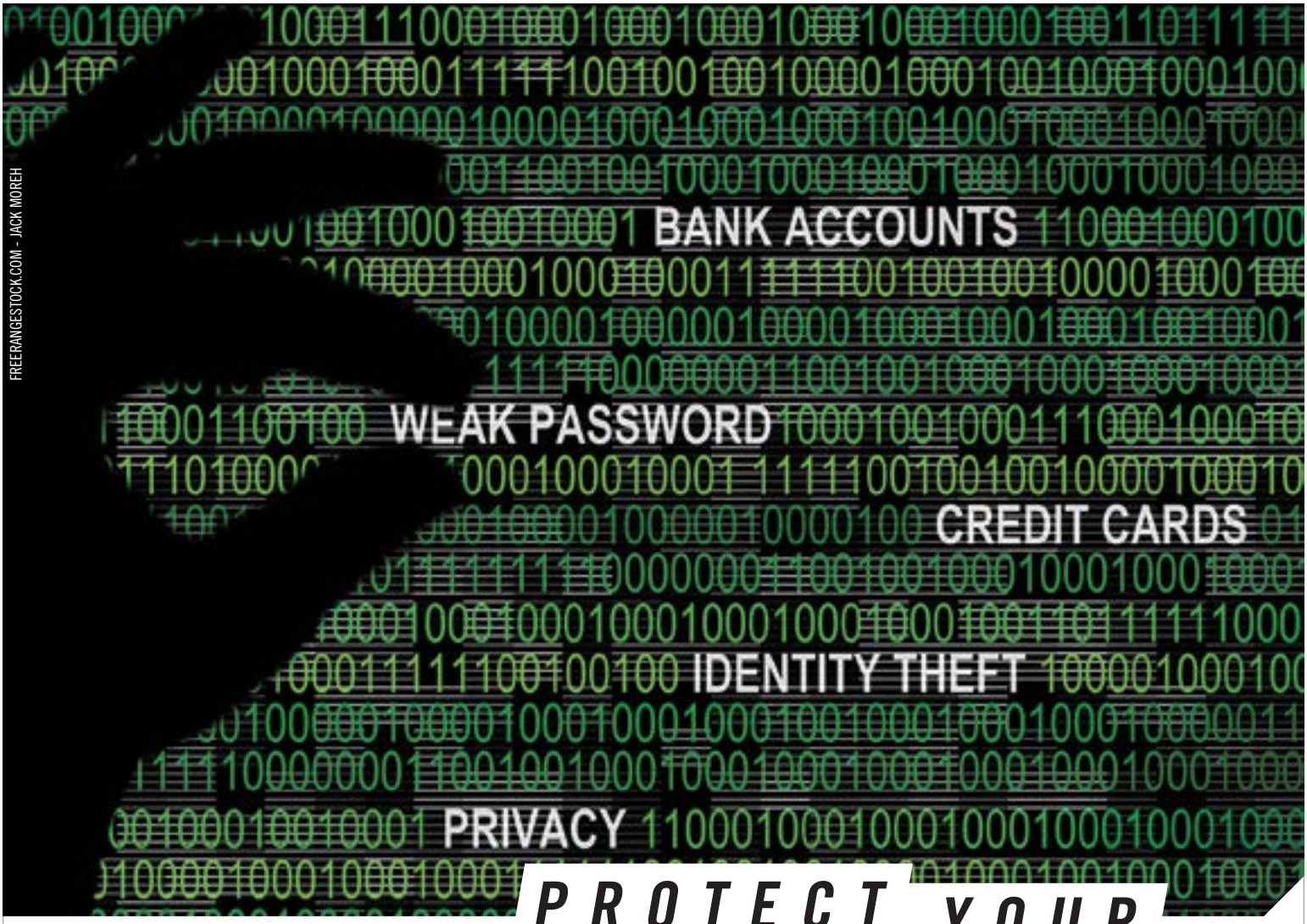
COMBAT RELOAD: EJECTING AND LETTING DROP THE EMPTY MAGAZINE FOR FAST RELOAD.

TACTICAL RELOAD: REMOVING AND RETAINING A PARTIALLY LOADED MAGAZINE IN EXCHANGE FOR A FULLY LOADED ONE.

Safe gun handling skills are crucial. You have no business carrying a gun without them, but that is only the tip of the iceberg for a skilled gunfighter. Can those shooters efficiently execute a reload? How about clearing a malfunction? Add bulky gear to get in the way, the distractions of extreme weather and incoming rounds impacting around your position and you'll see that ordinary tasks become extraordinary very quickly.

A competent shooter knows when something is wrong with the tool in their hands. As I'm shooting, even if I'm not counting my rounds, I know from weight and intuition when I'm nearly to the bottom of a magazine. When I've fired that last round, the recoil feels distinctly different to me regardless if I'm shooting rifle or pistol. I know the slide or bolt has locked to the rear and I begin my reload drill. If I have a malfunction, the recoil also feels different or there will be no recoil at all. Assuming we're in a gun fight and I run my rifle dry, my first option will be to transition to my secondary weapon if I have one. My firing hand comes off the pistol grip of my rifle and establishes a firing grip on my holstered pistol as my sup-

continued on next page



FREERANGESTOCK.COM - JACK MOREH

PROTECT YOUR DIGITAL FOOTPRINT

BY: DR. BRANDEN R. WILLIAMS

If you are reading this, I'm willing to bet you don't take personal security lightly.

From a physical perspective, I suspect you might carry defensive tools on your person at times, and some of you use tradecraft to blend in and avoid the appearance of being a ripe target. But what about your digital footprint? How is your digital tradecraft?

I'm a digital guy by heart. I grew up using computers, from the early Apple II through some high-tech mid-tier systems, down to the Raspberry Pi (a credit-card sized PC that can run on a battery). If you want to find information on me, it's pretty easy. Sometimes I get confused for an athlete or that former actor who dated Amy Smart (who now is the guy that Hollywood goes to when they need to buy or sell their house). I have a pretty big digital footprint, but it pales in comparison to many—especially the generation of kids just now preparing to graduate from high school and college.

Let's take a look at *your* digital footprint and how you can protect yourself. The concept of a digital footprint is essentially your life online. It includes things like your email account(s), your browsing and searching behavior, your shopping accounts like Amazon, your social media accounts like Facebook, your cellular telephone activity, emails sent to searchable email lists, and any government documents subject to the Freedom of Information Act that could be digitized, such as arrest records, court proceedings or property tax filings. If there is some kind of a record about you that is digitized (say, a marathon race result), that's included too.

One of the biggest risks to your digital footprint are your passwords or, in many cases, your password. Many people use one or two common passwords across all of their digital accounts. If I compromise one, I now own many (if not all) of your accounts. You


FREERANGESTOCK.COM - JACK MOREH

NEVER USE THE SAME PASSWORD ACROSS DIFFERENT WEBSITES. SHOULD IT GET COMPROMISED ON ONE SITE...

should be using a different password (if not username/password) combination for every online service such that one service's compromise doesn't put your entire digital footprint at risk.

Let's walk through a scenario. Let's say that you have a LinkedIn page and you use the same email address and password for it that you do for your online banking page. If LinkedIn has a compromise, your username and password combination could be tested at banks until someone got lucky to log into your bank account. This is why you want different passwords everywhere.

"But Branden," I can hear you exclaiming, "I can barely remember the password I have right now!" Not to worry, we have tools for this called password managers. Thanks to my password manager, I can report to you that I really do not remember any of the passwords for the sites that I use. It's brilliantly freeing from a memory perspective and allows me to guard against someone using a password from one of my logins to access another site. For those of you who are in the Apple ecosystem, the latest version of their operating system will automatically suggest and save passwords for you on many sites. It's not universal, but it works pretty well. For everyone else, there are a number of options that you can choose and will even synchronize across multiple devices and platforms. Lifehacker has a whole section of their website dedicated to password managers that make this one-password-per-site concept an easy one to implement. You can see it at http://brando.ws/pwmgr2015. Of course, you must decide if you want to expand your "circle of trust" to include any specific password manager and the infrastructure and people behind it.

Even with unique passwords on every site, there are more steps you can take to protect your accounts. Many sites offer additional authentication options on top of a password to help ensure that you are actually you. If you are wondering if one of the services you use allows for a two-step or two-factor authentication process, you can use your DuckDuckGo-Fu to find out (DuckDuckGo is a search engine that does not track your searches). It's as easy as searching for "enable 2-factor auth in *X*", where *X* is the service for which you are enabling two factor authentication. If it is available, you are most likely going to find it that way. You should be able to find Facebook, LinkedIn, Twitter, Google, Paypal, GoDaddy, and Dropbox at a minimum. Read my post at http://brando.ws/twostep2015 to learn more.

Once you add additional security features to the accounts that create your "footprint," it's time to think about your browsing behavior and how you can mask that. Have you ever noticed that when you search for something on Google, such as a getaway vacation, you start seeing travel ads on other sites you might visit, such as USA Today? That's because your browsing activity is sold to marketers to increase the chances you may purchase a product from them. This happens in many more places you patronize than you probably realize. Even though marketers can track you, there are ways to opt out.

Many browsers have the ability to opt out of ad tracking built in, but websites do not always pay attention to your wishes. You can test how your browser acts by visiting http://brando.ws/optout2015 and following the prompts. You can even submit requests to opt out of various tracking programs right there. You can also choose to use browsers in a way that attempts to keep your activity private, which is sometimes called a "private window" or as Chrome calls it, Incognito mode. In this case, your browser will not keep your history or cache, and tries to limit what is either stored on your local machine or is transmitted about yourself to the web. Ideally, cookies and other tracking mechanisms should not be stored or transmitted either.

The challenge with these modes is that your computer may not remember where you have been, but websites absolutely do. They can see your source IP address (the Internet routable address associated with your home or computer) and track or geolocate you that way. It isn't a perfect science, however, as your IP address will periodically change and not all geo-location services on IP addresses work flawlessly. Regardless, the tracking still happens and there are ways to address this.

One way is to use the Tor network (www.torproject.org) to increase your privacy. Tor works by connecting a group of computers together, such that you enter the Tor network on one node and exit on another. When you use Tor, the sites that try to locate you and

convert to the local language, such as Google, might show you Russian or Simplified Chinese characters. That is a byproduct of using the network.

Tor is not your end-all safety net, however. The network is targeted just like anything else by bad guys (and good guys) for the purpose of stealing personal information or compromising hosts. Anyone can sign up to run a Tor node, so consider that it may mask your origin, but the network may see your content. I like to use Tor as a quick way to anonymize my traffic from local prying eyes, but I would never log into any account in my digital footprint over a Tor connection.

There are other options for keeping your traffic secure that may be more trustworthy. Several companies offer Virtual Private Network (VPN) services that work similarly to the Tor network, but claim additional assurances of security and privacy because they control the VPN nodes directly. In this case, you could potentially access accounts in your digital footprint with more assurance that your credentials will be kept secure the entire way through. Be sure to research your VPN provider. There was a recent incident with one provider where a security professional discovered that they actively hacked machines on the Internet to illegally use their resources for their VPN nodes.

What about email? Aside from text messaging, email may be your go-to method to communicate with a third party. If you want to maximize your chances of keeping the information private, you need to think about using something other than Gmail. I found an email service called ProtonMail.com that provides just this. Your mailbox is encrypted and you can send emails somewhat anonymously (unless you identify your account somehow). The email account can be disposable just like a Gmail account, but in this case the servers are housed outside of the US. That doesn't guarantee an unscrupulous NSA employee who may be willing to violate the Fourth Amendment can't see it, but it helps.

Some researchers have discovered how to identify you based on your keystrokes. There is a proof of concept Chrome plug-in called KeyboardPrivacy that attempts to help solve this issue for you. If you want even more privacy tips, backgroundchecks.org has a list of 172 things you can do to enhance your online privacy (http://brando.ws/bgchk2015).

Your digital footprint doesn't go away when you die. Be sure you make arrangements to pass on your password vault to a loved one with specific instructions on what you want them to do with your online accounts. Without the proper credentials, your family may not be able to delete your old online accounts.

A TOR NETWORK CAN HELP PROTECT YOUR PRIVACY FROM SITES THAT TRY TO LOCATE YOU.

There are many ways that your online activity is tracked and used. Some are for legitimate purposes, some are not, but your digital footprint is growing every day. My goal is to give you a couple of specific tools that you can use to protect it and share some of the ways that the information can be misused.

WHAT CAN YOU DO?

Your digital footprint expands every day you are on the planet, sometimes regardless of your online activities. That said, there are a number of things you can do to protect your digital footprint and help develop your digital tradecraft:

Using the same username and password over and over is a recipe for identity theft. Even though your bank may not be the company that was compromised by hackers, if you use that same username and password somewhere else that was compromised, there is a good chance you will suffer. Be sure to let the password manager suggest long, random passwords to increase the security on those accounts. Use a (trustworthy) password manager to keep your online credentials safe.

Double check your often-used web services for two-factor or two-step authentication options and turn them all on. This way, when a new computer tries to log in, there is another step that must be taken beyond a username and password. Check your search engine for ways to do this on your popular services.

Mask your online traffic when appropriate. Choose a VPN provider or fire up the Tor network browser to mask your origin when doing certain things online. Be sure you understand the structure model of your provider so you understand how much you can trust that the contents of your traffic (and identity) will be safe.

Go through the list of 172 things you can do to mask your online activity (http://brando.ws/bgchk2015) and try a few out.

Make sure your browser does not send advertising information about you to third parties. In addition, check the links above to opt out of popular advertisement tracking programs. ✓

BIO

Branden R. Williams (www.brandenwilliams.com) DBA, CISSP, CISM is a seasoned security executive, ISSA Distinguished Fellow, and technology consultant.