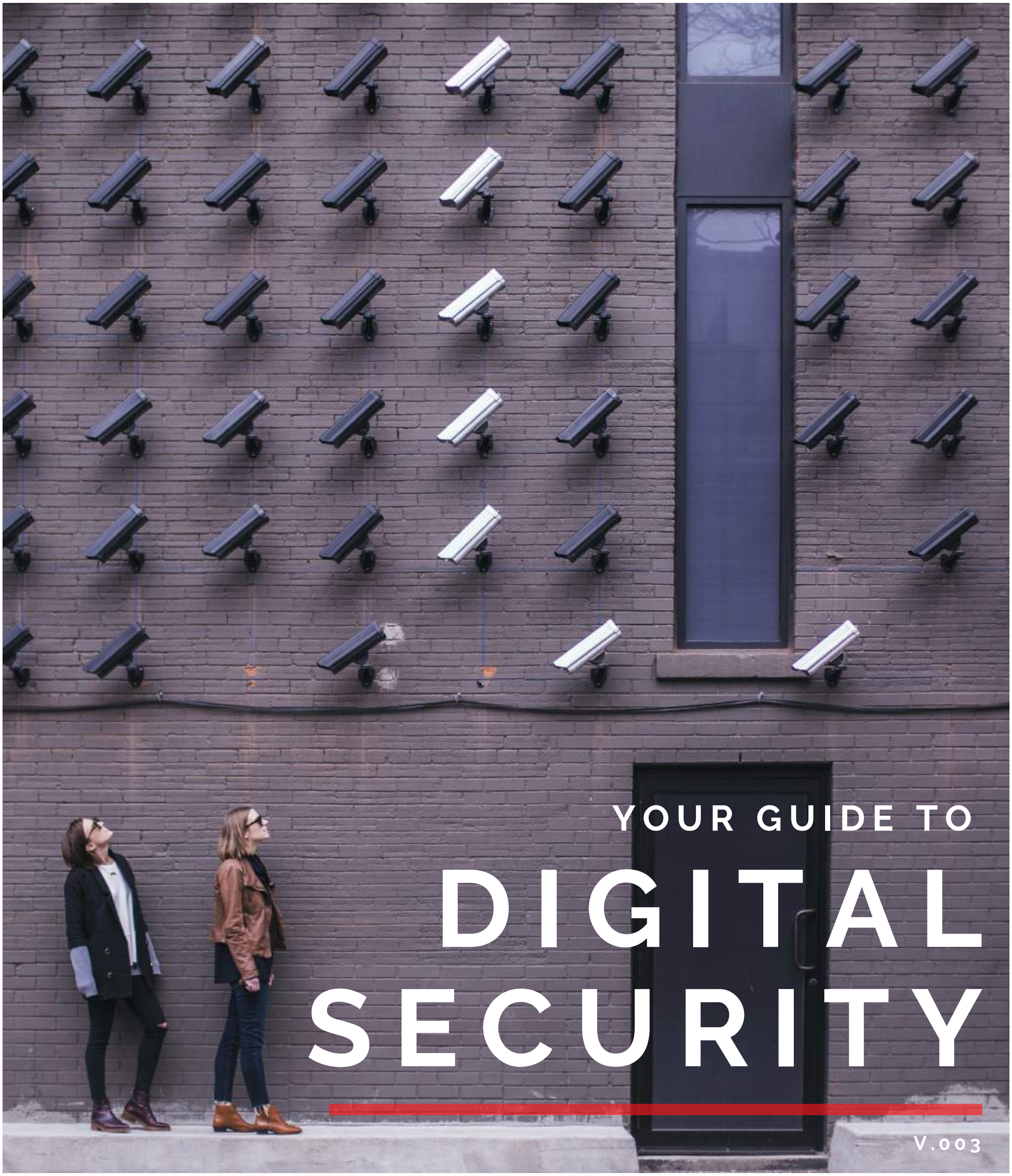
WWW.SIGNATUREMANAGEMENTUNIT.COM



YOUR GUIDE TO

DIGITAL SECURITY

V.003

Signature Management Unit
Great Lakes Region
(202) 952-1511
contact@signaturemanagementunit.com

THIS PAGE INTENTIONALLY LEFT BLANK.

MANIFESTO

DIGITAL SECURITY & PRIVACY | 2021

GREAT LAKES REGION
January 2021

As former intelligence officers, special operations professionals, journalists, and others, we emphasize privacy, discretion, individual responsibility, the criticality of reason and judgment, and living a life of virtue, moderation, and service. We believe forewarned is forearmed, and sometimes avoidance is the best policy. If there are any constants in life, a major one is uncertainty and the fear and apprehension that comes with it. We seek to serve others with trust, precision, and security in the face of uncertainty.

It is said: if you love something, set it free. While true peace and fulfillment cannot come from our intrinsic faculties or actions, we nonetheless desire to contribute our knowledge and experience in a worthy manner that seeks to mitigate the risk of harm caused by uncertainty in life. In today's digital landscape, digital security and privacy are major aspects requiring individual diligence. We recognize that obtaining a timely, holistic, and coherent understanding of how to approach individual digital security and privacy is difficult and potentially inaccessible to the layman. However, these matters do not just concern government spies, murky organizations, or those conducting corporate espionage.

What we share here is not empty platitude or a mere "flight of ideals" - the values above are ones we strive to exemplify in living color. It is thus we publicly release this personal guide for digital security and privacy, the product of countless hours of research, design, iterating, consulting, and other labors.

None of the contents here are new or avante garde; rather, we draw from the experience and lessons learned by those who have gone before us, mixed with our personal experiences in our respective fields. We hope this work, however small, constitutes a valuable contribution to your personal, familial, or business' understanding of digital security and privacy.

Thank you for joining us on this journey in the art of signature management.

SIGNATURE
MANAGEMENT UNIT

DIGITAL SECURITY

PHASE 0:
Know your adversary

PHASE 1:
Secure mobile devices

PHASE 2:
Secure laptops & other devices

PHASE 3:
Stay sharp

WHAT WE BELIEVE

Everyone has the right to accessible, secure, private, and reliable communications that are free from government surveillance, hacker interference, or criminal disruption.

OUR MISSION & PURPOSE TODAY

We researched, wrote, and designed this guide with you in mind. While techniques change and adapt with advancements in technology, the fundamental principles behind them do not. Thus, we seek to offer a number of practical end-user ways that can be employed to manage your digital signature and, by extension, take an active role in maintaining your security and privacy.

The techniques covered in this guide, while seemingly innocuous as individual measures, are in their composite a significant signature management advantage. There is no one technique that necessarily outweighs another - each is important in their own right and serves to harden your security and limit your vulnerability or attack surface in one way or another.

All techniques here are publicly accessible and generally open source. Most are best practices captured elsewhere in the industry. Given the guide's compact and portable nature, we covered techniques in as much useful detail as possible. However, additional research may be required for deeper understanding.

We are available for any basic questions regarding implementation or additions.

DIGITAL SECURITY

DON'T LET BAD GUYS WIN.

PHASE 0: KNOW YOUR ADVERSARY

- What am I trying to protect?
- Where does it reside or spend time?
- Where are these things or people most vulnerable?
- To what are they vulnerable?
- What threatens or would want to threaten what I hold dear?
- What can I do to mitigate the risk of harm?

SIGNATURE MANAGEMENT UNIT | 2021

PHASE 0: KNOW YOUR ADVERSARY

Armor offers little defense against piercing arrows, much like the Maginot Line offered little defense from German invasion. Know your adversary, and you can hope to gain insights into his behavior, methods, and most likely courses of action against you.

Similarly, from what are you most at risk in your digital signature? What information or data do you wish most strongly to protect or keep private?

An accurate "threat model" is required to mount a sufficient and effective defense. Understand what you need to protect, identify where you're vulnerable based on the adversary's capabilities, and you're on the right track.

Our adversarial assumptions in this guide cover a continuum of threat actor capabilities, possibly represented by government surveillance, cyber-criminal activity, or any other criminals or unauthorized entities attempting to access your communications or track your digital footprint.

While little can withstand sustained, deliberate effort on behalf of a nation-state to compromise and exploit your communications, much can be done to manage your signature, reduce your exposure to a wide swath of digital hostility, and offer peace of mind, security, and privacy.

What follows are several hypothetical threat models useful for conceptualizing your adversary based on your unique circumstances.

DIGITAL SECURITY

THREAT MODEL #1

A MALICIOUS EX OR STALKER WON'T LET YOU GO

Laurel's ex was inordinately possessive, emotionally manipulative, and could not take no for an answer. He disregarded Laurel's requests to stop calling and texting her at all hours of the day. Their relationship had ostensibly ended months ago but he continued to call. She blocked his number, began paperwork for a restraining order, and otherwise did her best to keep her distance and be hyper-vigilant when entering or leaving her apartment.

Laurel never spotted her ex near her apartment or felt as though she was being watched from inside the building; yet, she would catch glimpses of him as he ducked behind buildings as she entered her favorite coffee shop on her days off. Laurel recalled he worked in IT, but didn't know much about specifics. Noticing this disturbing pattern, Laurel sought advice from a friend who had served in the military. He advised her to alter her routine, routes, and times of travel., and to exercise caution and awareness when entering or leaving her office or apartment. But her ex somehow always appeared shortly after she left her apartment.

Wondering whether or not he was waiting near the building, she frantically called the police, who eventually parked a squad car outside her building. They reported nothing, but this did not stop her ex from disturbingly appearing outside the window of a restaurant where Laurel sat with her friend over lunch later that same day. He appeared angry, pale, and had a frantic and desperate look behind his eyes.

Laurel wondered how her ex had known where she was, as the police reported seeing no one in the vicinity and Laurel varied her route, her time of travel, and routine entirely. She had never been to this restaurant before or mentioned it to anyone except her friend. The reservation was under her friend's name, and Laurel had come through the entrance at the back of the restaurant.

How was this possible?

Note: this is a hypothetical scenario and not indicative of an actual threat to you or your person. Each threat will be unique to your circumstances and assets or data you desire to secure.

DEBRIEF: THREAT MODEL #1

This threat model represents a very real and dangerous threat to an individual who desires not only privacy but physical and emotional security. Laurel's boundaries were ignored and practical attempts to block, ignore, or otherwise "deal with" her ex's inappropriate behavior were absolutely ineffective.

We recall that Laurel's ex worked in IT in some capacity, but this is not central to the story given the vulnerabilities he exploited do not require vast technical experience or skills.

Unbeknownst to Laurel, her ex was using a publicly available and easy-to-use technique to track her whereabouts and thereby locate her against her wishes: her ex was using Wi-Fi wireless network analyzers (known as "sniffers") to track and locate Laurel's phone. Neither Laurel nor the police ever spotted her ex in the immediate vicinity of her apartment, but he always knew where to go.

Because she simply forgot or was unaware of this technique, Laurel did not know that her cell phone, in all its utility, was being used against her by an adversary. Because Laurel did not turn off her Bluetooth or Wi-Fi after leaving her apartment, her phone automatically continued searching for the network it was just connected to. In so doing, her phone broadcast its unique identifier and the network it was seeking - giving Laurel's ex a surefire and guaranteed method by which to locate Laurel's phone (and Laurel herself).

The method used by Laurel's ex to track her is not relegated to overtly hostile actors alone. A similar technique known as location-based analytics accomplishes the exact same thing (for a different endstate) that Laurel's ex used. Oftentimes, this type of tracking and locating is used by retail locations or conventions for marketing to monitor who enters, passes by, or enters into their store or other location.

Using common and publicly accessible beacons, we can easily identify specific devices and eventually associate them to unique persons (their users), a major privacy risk.

DIGITAL SECURITY

THREAT MODEL #2

CURIOUS OR MALICIOUS FOREIGN GOVERNMENT OFFICIAL

Ken was a senior C-suite executive for a major distribution company with offices in the United States and Europe. Occasionally, Ken would travel to meet prospective clients or assess business development opportunities in developing regions, including the Middle East. Ken was sharp, experienced, and knew his way around the various airport lodges from frequent connections.

When arriving at a major Middle Eastern country, Ken was slightly delayed passing through customs and was asked by the local officers to step out of line and wait in an isolated waiting room away from the main arrivals terminal. Ken thought nothing of this as he was a westerner and businessman, and figured there was either a mix-up or random inspection of some kind that led to his selection.

After some time, two middle-aged men in weathered suits entered the room and asked him a series of questions. For his safety and security, they requested they place his bag outside the room. Ken did not like this idea but was unsure he could deny the request. The men smiled through their teeth and asked him routine questions of his stay, including which hotel his company had booked for him.

After some conversation and questions, the men stepped outside and quickly returned to notify Ken they had selected the wrong individual. They apologetically offered to hail him a cab and ensured he was escorted through the terminal to a waiting taxi. Ken shook their hands, thought nothing of the incident, and enjoyed the rest of his visit.

Several months later upon returning to the United States, the board at Ken's company was shocked to find their local Middle Eastern business partner he had met with just months earlier announced bankruptcy after local competitors cut costs and put them out of business, irreparably damaging their output and affecting U.S. operations.

What happened?

Note: this is a hypothetical scenario and not indicative of an actual threat to you or your person. Each threat will be unique to your circumstances and assets or data you desire to secure.

DEBRIEF: THREAT MODEL #2

Ken's experience is not unique to his fictional company, and incidents of corporate espionage, crooked foreign government officials, and criminal enterprises remains alive and well, however unapparent they may seem.

Unfortunately for Ken and his employer's local business partner, his company did not offer or have in place full disk encryption on company laptops. Ken thought nothing of this and figured his standard username and password was enough to keep unwanted users out of his company laptop.

When the customs officials removed Ken's laptop and bag from the room, Ken rightfully felt uneasy. Unbeknownst to Ken and almost impossible for him to detect, the customs officials had a forensics capability available to access his devices while he was conversing with the two officials. Whether or not they found something did not matter, for the officials used their governmental authority to ascertain Ken's hotel, where they easily could enter it at their leisure and investigate his devices further. Given Ken was in a developing nation, government officials and private citizens alike are looking to profit from wealthy westerners passing through. While this is not the norm, this position was abused for personal profit. The officials had obtained data of value to the company's local competitor, who used it to improve their own circumstances and ruin the local partner.

Had Ken been aware his username and password were no protection against this type of physical intrusion of his company laptop, perhaps he would have encrypted the hard drive, shut down the computer, and refused to leave his devices unattended. Not knowing his rights or having a privacy or digital security mindset, these lessons were lost on Ken until it was too late.

Full disk encryption, not leaving devices unattended, and being mindful of existing data on personal or company devices can prove highly valuable during any business or personal travel, both domestically and abroad. Privacy and digital security are not just discrete steps to take but a mindset to embrace.

THREAT MODEL #3

CYBER-CRIMINALS COMPROMISE AN INFLUENCER'S ACCOUNT

Samuel was not interested in privacy and used his spare time outside of school to amass a major Instagram following. His hope was to enter into the social media influencer business in order to talk about things that he was passionate about and that interested him. So far, Samuel had over 250,000 followers and wanted to keep going.

Most Samuel's passwords were stored automatically for him in his iPhone's keychain function, and most forms he filled out online were automatic to save him as much time as possible. Samuel had a pretty long password for his Instagram account, which he created years ago when his parents first let him get his own email account. He only used that email and kept it open for years, even though he was pretty sure he got "hacked" at some point, based on the number of spam emails he constantly received.

One day, as Samuel refreshed his Instagram feed, his account suddenly booted him and left him at the login screen of the Instagram app. Samuel hated when this happened but knew the app had to occasionally refresh or be updated, so he quickly started typing in his handle, tapped the password to enter it automatically, and tried logging in. Strangely, the app didn't recognize his password and said it was incorrect. Samuel began to panic slightly as he tried the same login once more. Still nothing. Something was definitely wrong. Samuel began to panic thinking of all the missed content and engagement opportunities he could never recover.

Almost at the same time, an email notification rang that grabbed his attention - his cell phone service provider (he was still on the family plan) just emailed him wanting to confirm that he indeed wanted to port his number away from their service. Before his eyes, Samuel's social media and personal accounts slipped from his grasp.

What was happening?

Note: this is a hypothetical scenario and not indicative of an actual threat to you or your person. Each threat will be unique to your circumstances and assets or data you desire to secure.

DEBRIEF: THREAT MODEL #3

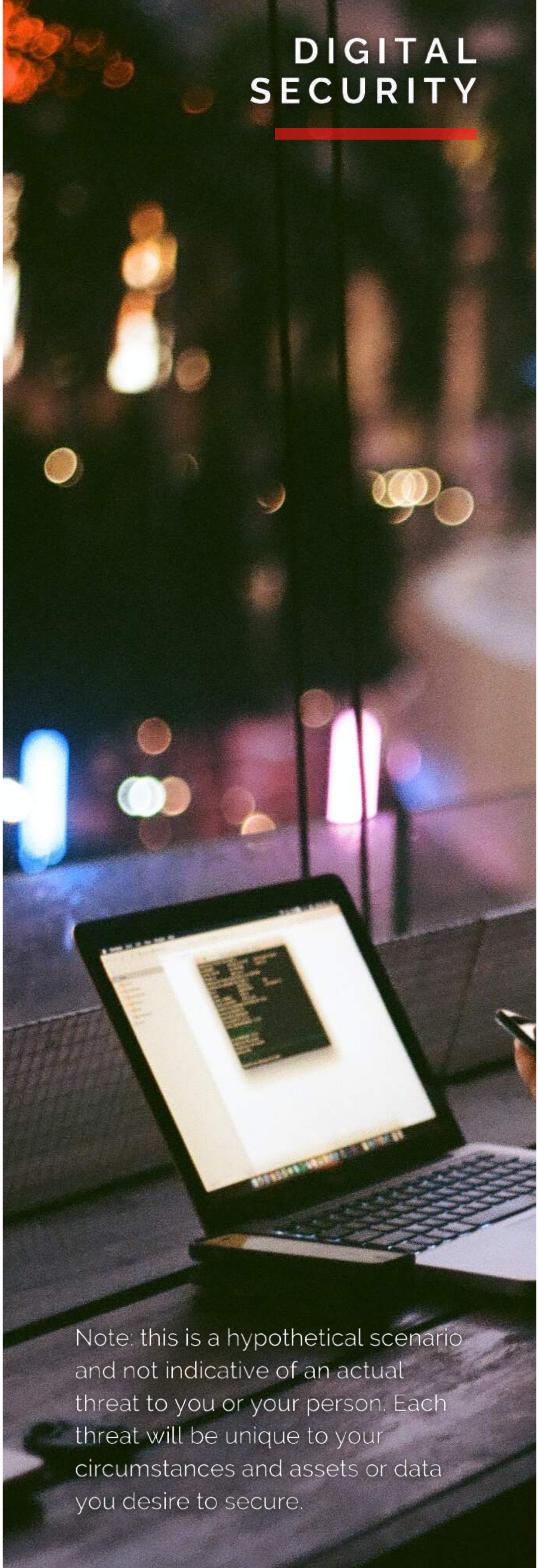
Samuel was like most of us who do not wish to be bothered with the inconvenience of security. We're not high profile people, we don't have any major corporate or government secrets, and we just want to use our devices and access whatever technology we need to.

Unfortunately for Samuel, a few bad practices caused significant damage to his abilities in the digital space. Because he was trying to build a public social media persona, most everything about Samuel's life was publicized online. None of his accounts were private, which was a deliberate choice on his part to engage more followers. Because of this and his growing following, Samuel became a target of cyber-criminals who used the information presented by Samuel (his location, lifestyle, and identity) to narrow their search for him online.

Once they obtained enough information to confirm his identity, the attackers went after the one thing they knew Samuel would pay the most dearly for: his social media following. After locating Samuel online, the attackers ascertained his phone number and other personal details. Launching what is known as a "SIM-swap" attack, the attackers contacted Samuel's cell provider pretending to be him. They then asked that his cell phone number be ported or moved to a new SIM card/phone they controlled. Having all the necessary information about Samuel they needed, the cell company complied, giving the attackers control over Samuel's phone number.

Simultaneously, the attackers obtained Samuel's email address, checked it with various publicly available databases of stolen data, and ascertained his old password, which they also could use to access his email at a later date. Because Samuel reused his passwords, this was an easy task when needed.

Once the attackers controlled Samuel's phone number, they reset his Instagram password by "forgetting" it. The text and code from Instagram went straight to Samuel's number - the one they now controlled. They then locked Samuel out of his account and could either sell it or demand payment for access back to it.



Note: this is a hypothetical scenario and not indicative of an actual threat to you or your person. Each threat will be unique to your circumstances and assets or data you desire to secure.

THREAT MODEL #4

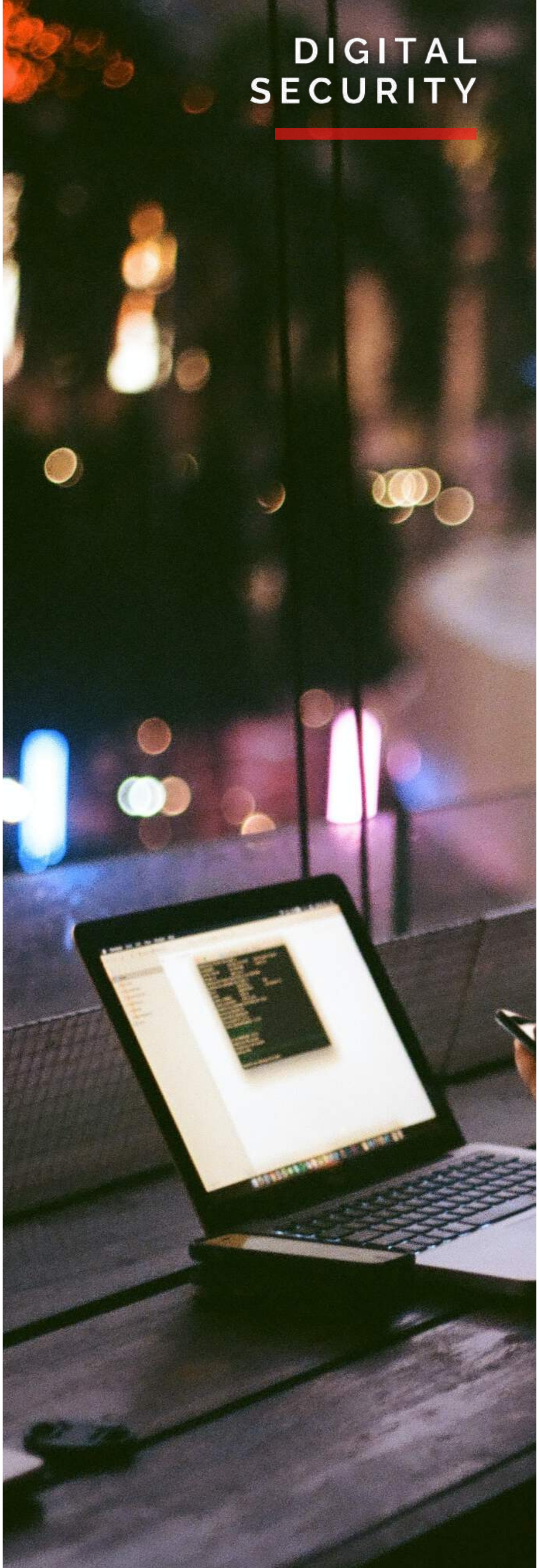
THE COFFEE SHOP HACKER

Hannah frequented the local coffee shop downtown for work or school, especially when she needed to leave her apartment for fresh air or a change of scenery. Most everything was done remotely or virtually, and coffee shops were great for the atmosphere, coffee, and delicious aromas they contained.

One day, Hannah's usual boutique coffee shop was closed, so she resorted to the popular Starbucks across the street. Settling down into a window seat with a piping hot cappuccino, Hannah opened up her Wi-Fi and looked for the free Starbucks Wi-Fi. She scanned the network options, noticed how many Starbucks networks there were, and connected to the top one titled "Starbucks Free Wi-Fi". Hannah then continued about her day and work, having no trouble connecting to any of the websites she needed, logging into her remote desktop for work, or accomplishing her usual banking or online shopping. Given the cafe was crowded and in the middle of downtown, many people came in and out, and Hannah often wore headphones to focus on the work in front of her. Midway through her work, she lost internet connection and had to reconnect to the Starbucks Wi-Fi, but thought nothing of it as she had a deadline to work on.

The next day, Hannah woke up to no fewer than five emails, three missed calls, and several app notifications from her bank regarding several major credit card purchases in question. Hannah had just woken from sleep and was extremely confused what purchases the bank was looking to verify. One notification was an online purchase for a several thousand dollar television purchased from Amazon and shipped with same day delivery to a local Amazon locker. Hannah had no clue how this order was placed and frantically called the bank to see if there was some mistake made.

What happened from her day at the cafe?



DEBRIEF: THREAT MODEL #4

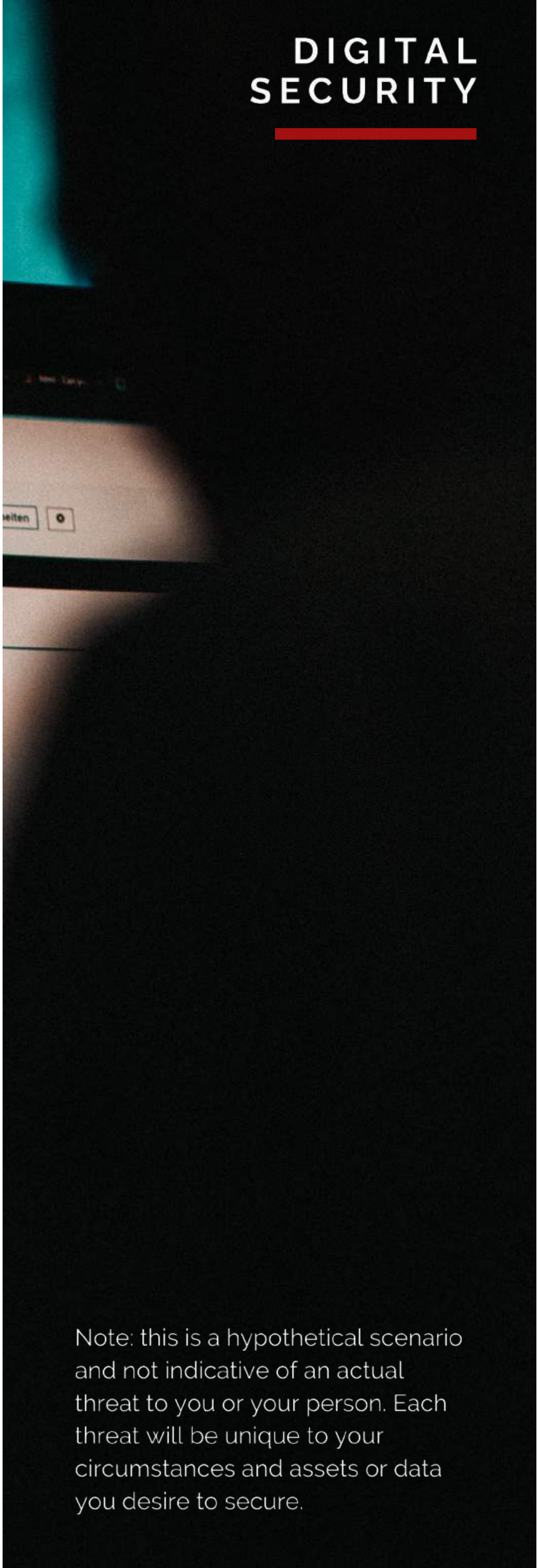
Hannah was in need of Wi-Fi and figured she would find it at Starbucks. Hannah did, in fact, access a Wi-Fi connection, but it ended up costing her more than it would have had she only relied on a few basic digital security and privacy practices.

Unbeknownst to Hannah, the Wi-Fi network she first connected to at Starbucks was not, in fact, under friendly control. Rather than the usual corporate network managed by the Starbucks store itself, Hannah fell prey to a style of "man-in-middle" attack. A criminal, knowing many people connect and have a need for public Wi-Fi, had setup a Wi-Fi network and insidiously named it after the location near which they sat.

In the hopes of luring unsuspecting victims like Hannah, the attackers - because they controlled the network and router to which Hannah connected - were able to capture and view all of her internet traffic, including her login credentials (i.e. for Amazon) and some banking information (i.e. credit card number). Because the attacker was in close proximity to Hannah at the time, they figured she would likely be sleeping throughout the night and waited to act on the information they had pirated before exploiting it.

When Hannah suddenly lost internet, it was likely the attacker shutting down the network and leaving the store. Because routers and antennas can easily fit in a backpack or messenger bag, the attacker would have been able to blend in with other coffee drinkers and would not have raised any suspicions.

Had Hannah used a virtual private network to protect her traffic, not relied on unsecured public networks for her internet connection, or at least confirmed the name of the store's actual network, Hannah could have easily thwarted this type of attack, and could have slept well knowing her sensitive information was not compromised.



THREAT MODEL #5

AN INNOCENT WOMAN HAS HER REPUTATION DAMAGED BY DOXXING

Caitlin worked as an accountant at a major firm in the city. She was payed well, found her work fulfilling, and enjoyed going on bike rides on the weekends. There were a series of trails she could ride that took her through the parks and green space around the city, where she had lived since graduating university.

On Saturdays, Caitlin would hop on her bike for a quick ride to the nearest park and trail. She locked her townhouse, carried her bike down the few short steps, and was off on her ride to enjoy a beautiful sunny day. Caitlin usually wore typical cycling clothes during her rides, and was greatly looking forward to some time in nature. She put her phone on silent so she could listen to music and ride without any distractions. Occasionally, the office liked calling her on weekends for clarifications ahead of a deadline, and Caitlin wanted to dedicate the time to her ride through the parks.

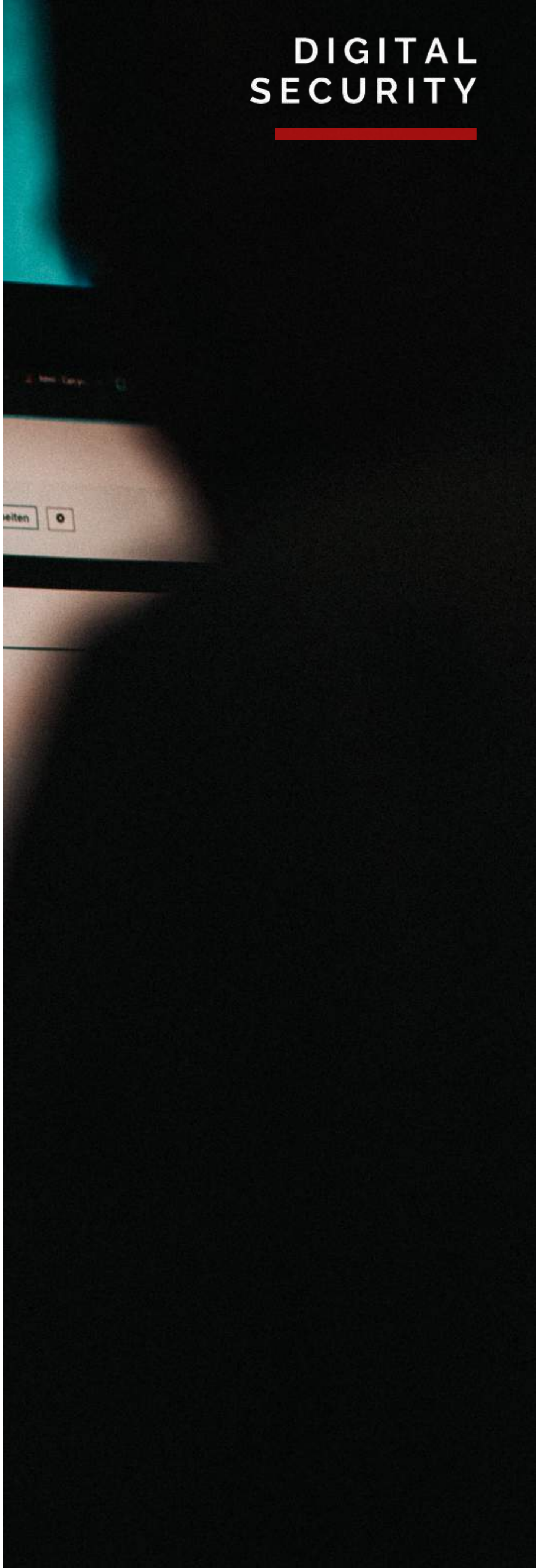
Caitlin set off on her ride and had a great time. She rode for several hours, and returned around mid-afternoon to her townhouse. Taking a swig of water, she took her phone off silent and mentally braced herself to see one or two emails or missed calls from her supervisor.

Instead, Caitlin was shocked to see that her phone was overwhelmed with notifications. Her Twitter direct messages, her email, her texts, and her calls had anywhere from twenty to thirty-five notifications. Caitlin's heart began to race as her mind spun into overdrive - did she miss a deadline? Did somebody die? Was there another terror attack in the city? What was happening?

Panicking as she opened her Twitter app, Caitlin was perplexed to see that none of the messages were from people she knew. Similarly, she was suddenly receiving all sorts of emails from random people who were calling her vicious names. Texts were no better. She was being called horrible things and was even receiving death threats.

What happened during her ride?

Note: this is a hypothetical scenario and not indicative of an actual threat to you or your person. Each threat will be unique to your circumstances and assets or data you desire to secure.



THREAT MODEL #5

By all accounts, Caitlin seemed like a reasonable, average individual looking to enjoy an innocent bike ride on her Saturday off from work. And indeed, she was reasonable and did enjoy her ride. What Caitlin did not anticipate or prepare for was the threat of her being "doxxed", a practice where an individual becomes the target of online harassers who seek as much personal online information on a person that they can, and then publicly post the information online for others to bully, harass, threaten, or otherwise hold her and her personal information at risk.

Like most of us, Caitlin, a successful mid-level accountant, had a moderate online presence in the form of a few social media accounts, a mortgage to pay for her townhouse, a phone bill, and several personal or work emails.

Unbeknownst to Caitlin, during her ride, she was misidentified as a different woman (who was also biking) who had committed a hate crime against an elderly couple and was actively being sought by the Park Police, who posted a plea for help on their public Facebook page. Seeking a form of people's justice, various individuals who saw the plea for help conducted their own form of digital "investigative" work to find the woman and hold her accountable.

Known as doxxing, this practice immediately caught Caitlin in a vulnerable place, given she very loosely matched the initial description of the actual perpetrator provided to the Park Police, who in turn shared that with the Internet in the hopes of finding her.

Because Caitlin tracked her rides with the fitness app Strava, all her rides were saved online for her. Unfortunately, this was also public information, which mistakenly led an online vigilante to her Strava profile, which in turn revealed her name and picture, which led to her Twitter account, which led to her location, thereby contributing to her misidentification as the woman who conducted the hate crime. In horror, Caitlin quickly called the police but the damage had already been done. The Internet mob had taken over, found her address, phone number, and email, and even friends and family were asking her if she had done the horrible crime.

Note: this is a hypothetical scenario and not indicative of an actual threat to you or your person. Each threat will be unique to your circumstances and assets or data you desire to secure.

THREAT MODEL #6

A PUBLIC FIGURE IS COERCED BY ORGANIZED CRIME

Luis was the rising star in the District Attorney's office and knew he had only a few years remaining before he was positioned to take over for the current DA. Luis put all his effort and time into work, and hoped that he'd get his own corner office after reaching his dream job.

Luis was on the straight and narrow because he had to be for work. He primarily prosecuted organized crime in the city, and loved going after the local crime bosses and their extortion, narcotics, or trafficking rings. Watching their smug faces shift to immediate concern when his office charged them with significant time behind bars in the courtroom was something Luis relished.

Luis had his own place that was big enough for his two young children when it was his turn to care for them. He didn't speak with his ex-wife much when she dropped them off every other weekend, which Luis was sad about but did not dwell on - work was his true love. That, and his children.

Luis sat down one Wednesday morning to go through correspondence from the city when his secretary delivered a bouquet of flowers to his desk with a note. Grinning as his secretary closed the door, Luis shook his head and initially assumed this must be some kind of joke from the office, who knew he had no need of flowers and had mild allergies. Keeping the flowers at arm's length, Luis plucked out the card, and began to read it.

The blood drained from Luis' face and his hands started to shake as he read the letter again and again rapidly. He was furious but also terrified for one of the first times in his life. In no unclear manner, an anonymous sender had included his address, phone number, and two pictures of his children in the card, with the words: "you have a lovely family. Stay safe!" written menacingly in red ink.

How could they threaten his family?

DEBRIEF: THREAT MODEL #6

Luis was a smart, capable, and career-oriented professional. He did not participate in shady activities, and had goals and objectives for his life and career. However, Luis worked in a very public capacity, and was bound to upset somebody over the course of his professional duties working for the DA's office.

What Luis did not factor into his risk calculus was the desperate and great lengths to which his adversaries would go to silence, neuter, or otherwise control his efforts to place them behind bars. While he thought nothing of it, Luis actively worked against organized crime syndicates to impact their bottom line, which they were not pleased with.

Therefore, when the time came for to create an effect that would dampen Luis' enthusiasm for his work while also sending a strong message, it was not difficult for his adversaries to locate his home address and to discover his greatest vulnerability: his family.

Luis was at a slight disadvantage due to being a public figure working for the DA. However, this does not mean he was powerless to mitigate the risk of "blowback" (or harm from his work). Knowing that he was at greater risk and a public figure, Luis could have taken steps to protect his online signature. While most his time went to work and he did not have an extensive social media presence, Luis had lived at his home for awhile, and had never taken the time to discover how much information about his limited personal life was accessible online.

Despite working near the courthouse where there was constant security, and despite receiving physical security and awareness training by his office, Luis failed to see how he remained vulnerable online. All the training and safeguards at work became moot when criminals elected to target him at home, where his guard was down, where there was less security, and where his most critical asset - his family - frequented.

Had Luis taken concrete steps to evaluate his online signature and remove or suppress various publicly available information, it could have complicated his adversary's efforts and protected his family from harm.

AFTERMATH

PHASE 0: LESSONS LEARNED

No matter your station in life, everyone stands to gain from digital security and privacy. The techniques in this guide could be applied in any number of ways to mitigate the risk of harm. Here are a few techniques (the more the merrier) that, when properly applied, could provide security against our general threat models*.

THREAT MODEL 1: STALKER

- #1: turn off Bluetooth and Wi-Fi
- #9: protect true dialed number
- #14: review Wi-Fi settings of all devices
- #29: Faraday bag to prevent tracking

THREAT MODEL 2: ESPIONAGE

- #5: ensure devices are encrypted
- #6: enable USB-restricted mode
- #28: physically secure devices
- #31: enable firmware password

THREAT MODEL 3: CYBER CRIME

- #9: protect true dialed number
- #16: lock down social media
- #19: suppress online PAI**
- #22: enable two-factor authentication

THREAT MODEL 4: CAFE

- #7: employ a VPN
- #15: always browse securely
- #26: employ card masking
- #27: use a mobile hotspot

THREAT MODEL 5: DOXXING

- #9: conceal your true number
- #11: beware "leaky" apps
- #16: lock down social media
- #19: suppress online PAI

THREAT MODEL 6: COERCION

- #19: remove online PAI
- #29: minimize surveillance
- #30: consider "toss" devices
- Share techniques with family

*The number of techniques listed here are not all-inclusive.

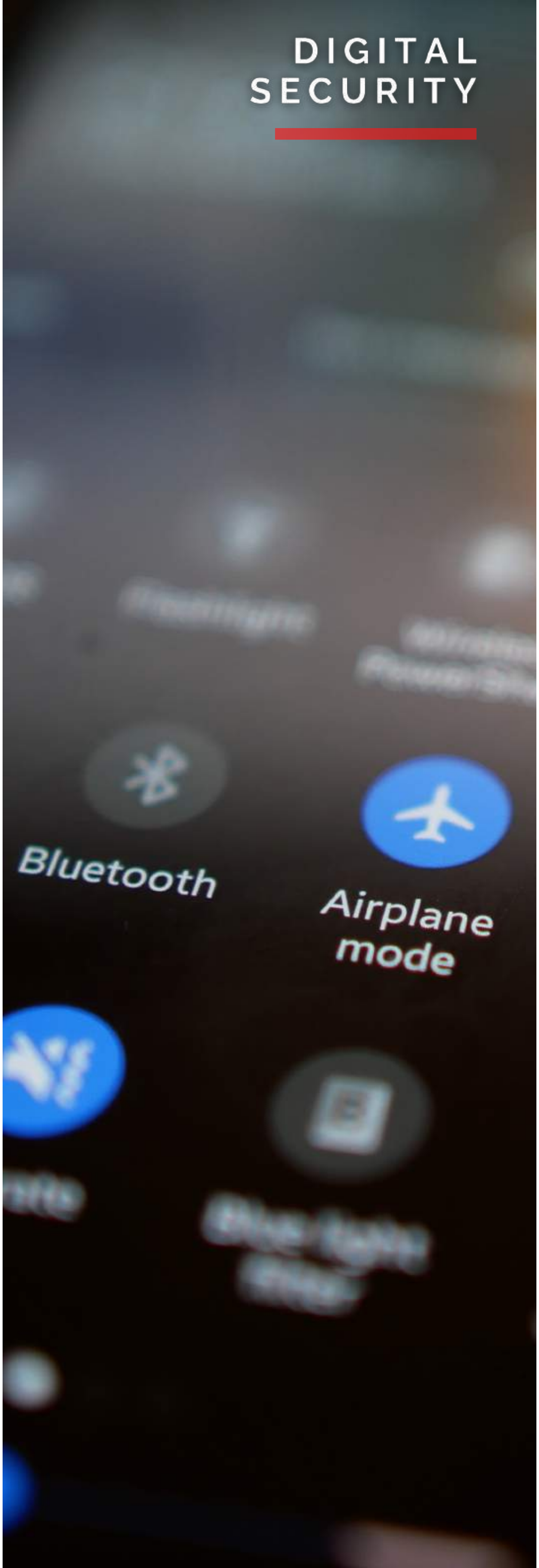
**PAI is defined here as publicly accessible information, or the data available online or found from open sources.

PHASE 1: SECURE MOBILE DEVICES

The majority of digital security techniques in this section pertain to your cell phone or other mobile devices. During business and tourism travel, personal cell phones often accompany individuals and families. While valuable for communications, navigation, general connectivity, and other daily uses, traveling with personal devices does expose you to a number of risks.

The following section identifies several categories ranging from strategic best practices to specific tools that can be employed to reduce your digital footprint (or "signature") and scrutiny from governments, hackers, and criminal organizations.

All recommendations are presented agnostic of priority; when feasible, all should be employed in order to best manage your signature. The exemplar device for this guide is an iPhone; while specific menu options may vary from other manufacturers, concepts do not.



TECHNIQUE #1

WHEN NOT IN USE, COMPLETELY TURN OFF WI-FI & BLUETOOTH

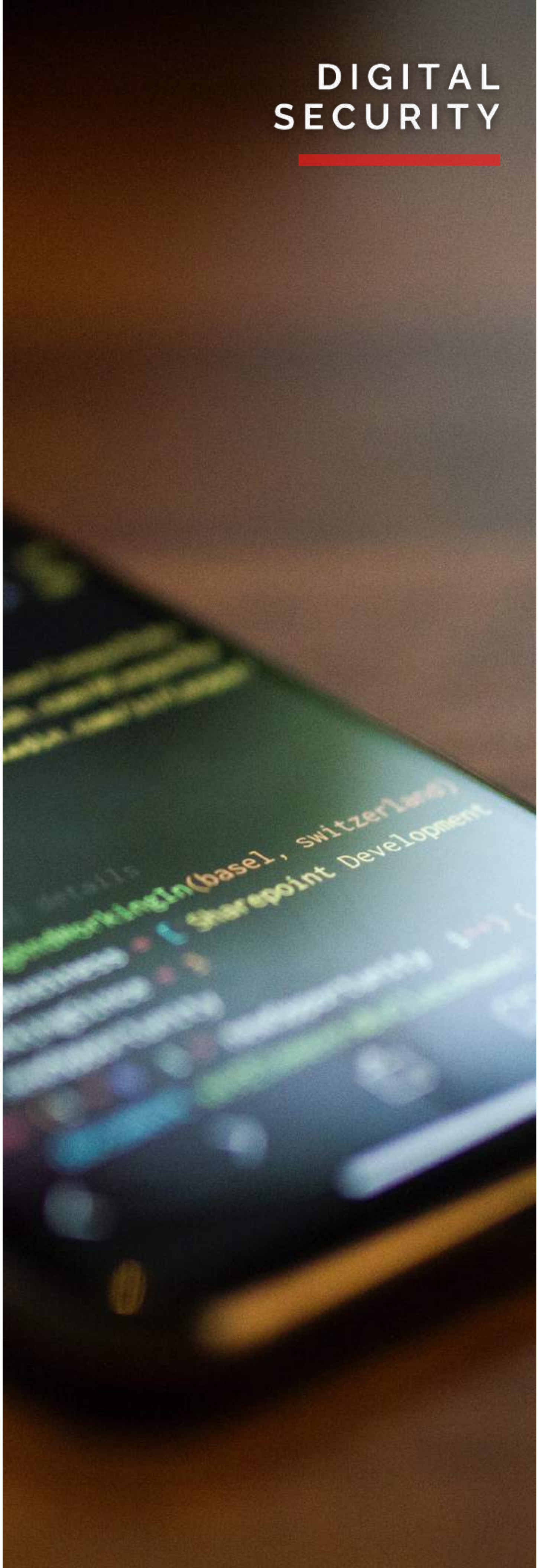
Bluetooth and Wi-Fi cannot simply be deselected; you must enter your settings and turn them completely off at any time when not in use, i.e. connected to an access point/router or other device.

The design of Bluetooth (802.15) and Wi-Fi (802.11) standards allow for devices to be tracked employing a number of publicly available wireless network analyzers, the majority of which include basic details such as: SSIDs (network names), signal strength, MAC addresses (unique identifier for devices connected to the network), and security status. This is common in cyber espionage, hacking, penetration testing/security audits, and mobile location analytics marketing.

When a cell phone has the Wi-Fi enabled but is not connected to the network, various packets are broadcast from the device; these packets can be passively captured by the wireless network analyzers to identify the device's unique address (MAC), and which access point (AP) it is trying to reach, i.e. the name(s) of networks it has connected to previously. Similarly, this information can be captured from various apps to provide the same search/tracking capability back to the device.

This provides instant pattern of life for the device's owner as well as a unique identifier for adversaries to search for, locate, and track. Apple recognized this vulnerability and attempted to obfuscate the MAC addresses of its devices through MAC randomization, pushed in an update to the iOS 8.0. Security firm test results of this feature were mixed, not counting their observation that whenever connected to a network, the device's true MAC address was broadcasted.

It is highly recommended users manually turn off Wi-Fi and Bluetooth settings when not actively in use.

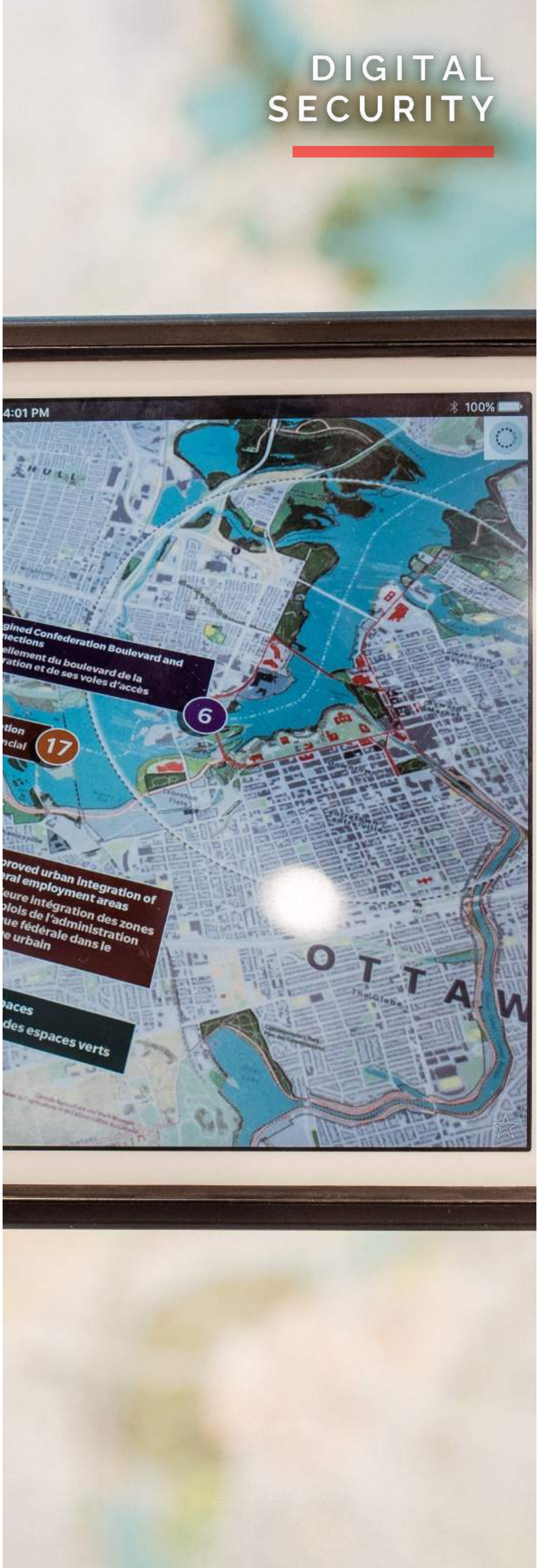


DIGITAL SECURITY

TECHNIQUE #2

DISABLE IPHONE ADVERTISEMENT TRACKING

Go to Settings>Privacy>Advertising>[select] Limit Ad Tracking>[select] Reset Advertising Identifier.


4:01 PM
100%
HULL
gined Confederation Boulevard and
nections
ellement du boulevard de la
ration et de ses voies d'accès
6
tion
ncial
17
proved urban integration of
eral employment areas
eure intégration des zones
plois de l'administration
ue fédérale dans le
e urbain
paces
des espaces verts
OTTAW

TECHNIQUE #3

CONTROL IPHONE LOCATION SERVICES

Limit access to location services to only the apps absolutely required to function (i.e. Google Maps in a foreign country). Further, ensure apps that do have access to location data only have it while the app is actively being used (i.e. Uber). For navigation specifically, when possible, create caches for maps or other navigation functions to minimize active location tracking of your device.

Device applications rarely require access to location data other than for advertisements and marketing or selling your data to third parties. Minimize your exposure to these practices by controlling your location services.

TECHNIQUE #4

DISABLE IPHONE APPLICATION BACKGROUND REFRESH

Go to Settings>General>Background App Refresh>[turn off everything or limit to trustworthy apps]. If not disabled, apps will send automatic periodic updates to the developer; refresh updates vary in content but are generally not critical to end usage of the app, and are not required.

See Technique #11 for additional information regarding how apps and other third parties can abuse your privacy and digital security in exchange for financial gain.

TECHNIQUE #5

SET PASSWORD OR PASSCODE ON ALL DEVICES

This is an obvious but overlooked practice generally disregarded due to complacency. Devices, particularly iPhones, are encrypted and relatively difficult to access without the user's permission, but only when they are locked.

It is highly recommended you set a password or passcode on all devices to secure and encrypt them. For additional security, consider employing a passcode comprised of at least eight (8) digits, as it exponentially increases security due to the difficulty in decrypting a longer PIN. It also masks the length of the passcode that additionally thwarts unauthorized users from attempting to guess one's passcode length upon visual inspection of your device, let alone the passcode itself and the longer PIN.

TECHNIQUE #6

ENABLE USB-RESTRICTED MODE

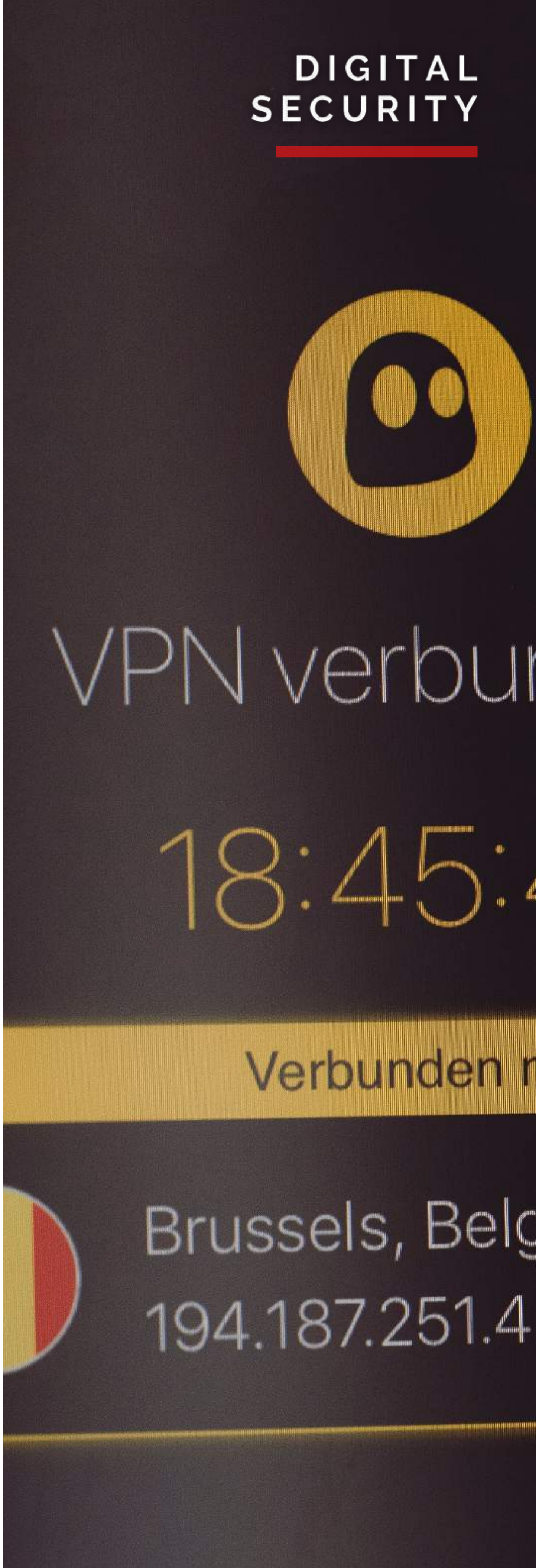
Modern cellular devices offer encryption that requires potentially cost-prohibitive commercial solutions to defeat. If a device's password or passcode cannot be obtained, whether through coercion, trickery, or willful surrender, the device will be entered through the Lightning USB port. This bypasses various control measures and provides some limited, but highly effective, device data that could prove useful to threat actors.

USB Restricted mode offers additional protection for devices so they cannot be accessed via the Lightning USB port, so long as the device as been locked for one hour.

While commercial solutions to defeat this feature continue to evolve and probably remain relatively cost-prohibitive for other-than-developed countries, USB Restricted mode is an additional safeguard against this privacy violation.

It is highly recommended devices remain locked - or better, powered off - preceding and throughout the duration of border crossings and customs. See Technique #30 regarding a more involved option to minimize the risk of exposing your personal devices and data to unauthorized third parties during border crossings or international travel.

DIGITAL SECURITY



TECHNIQUE #7

DOWNLOAD & EMPLOY A VPN AT ALL TIMES

Cellular devices on more advanced technology protocols (e.g. 4G, LTE, etc.) offer relatively advanced encryption on their networks. However, access to these networks varies based on privacy laws & individual civil liberties of the countries in which the carriers conduct business. Regardless of location, users are highly recommended to connect to a VPN. VPNs provide an added layer of privacy and security (but not anonymity) by encrypting device communications.

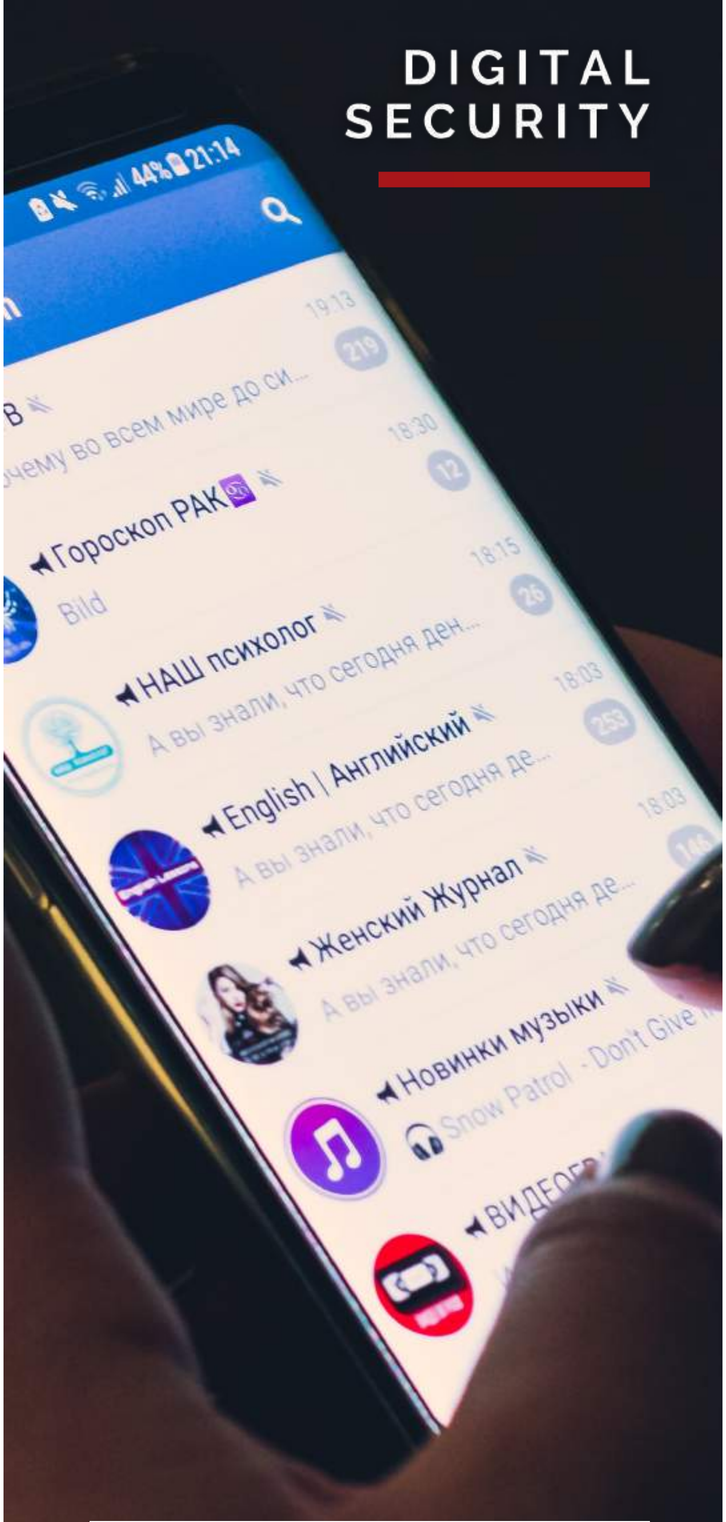
There are various encryption technologies available; in its most basic explanation, a VPN creates an encrypted tunnel from the user's device to the Internet. In addition to encryption, VPNs mask or "spoof" the user's Internet Protocol (IP) address based on where the user wishes to route their internet traffic. Various VPN providers offer cost effective services for access to servers across the world.

Two highly recommended and not officially endorsed services are offered by London Trust Media, Inc. - Private Internet Access (PIA) VPN, and ProtonVPN. PIA services can be purchased anonymously using a number of widely accepted store gift cards, are cost effective, and maintain high standards for respecting user privacy and data (e.g. cannot access their own traffic and do not store data on their servers).

It is highly recommended users employ a VPN at all times, especially in unsecure environments such as public hotspots, coffee shops, airports, hotels, etc.

Secure and Free VPN service for protecting your privacy

ProtonVPN is a security focused FREE VPN service, developed by CERN and MIT scientists. Use the web anonymously, unblock websites & encrypt your...



Speak Freely

Say "hello" to a different messaging experience. An unexpected focus on privacy, combined with all of the features you expect.

TECHNIQUE #8

COMMUNICATE WITH END-TO-END ENCRYPTION

A highly recommended and not officially endorsed service that provides end-to-end user encrypted communications is provided by the Signal Private Messenger (from Open Whisper Systems) application. On an encrypted and secure platform, Signal offers messaging, calls, video, pictures, and other data transmissions.

Chief in this service are the end-to-end encryption between users and a high regard for user privacy and individual liberties (e.g. Signal does not store data on its servers and cannot access it even if demanded by law). The app is available in mobile or desktop configurations.

Signal does require a phone number upon initial registration; this is to verify ownership of the device being registered. However, after registration, the app will not rely on or require that number to function. For example, if the app was downloaded and registered to a user's US number but the user travels abroad and purchases a local prepaid SIM card and plan for the same device (i.e. swaps out SIM cards), the app will still function as normal.

By contrast, WhatsApp messaging app does require registration and access to the same number in order to function. However, this can be useful when working or traveling abroad for an extended period, where the user wants to maintain access to private Signal messages but does not want to give their US (or original registration number) out to anyone else. In this instance, the user can provide their local number (that WhatsApp requires and uses) while still maintaining the same access to Signal they had with their original US number. While Apple's organic iMessage function also offers end-to-end encryption and is privacy oriented, iMessage and SMS messages are also backed up on iCloud; by contrast, Apple has no access or backups of third party apps like Signal. It is highly recommended users employ Signal in conjunction with a VPN for maximum signature management.

TECHNIQUE #9

PROTECT & CONCEAL YOUR DEVICE'S TRUE NUMBER

There is little reason for entities outside your inner circle to possess your dialed mobile number, the number assigned by your cell carrier that, when dialed, connects directly to your device. The numbers assigned by major cell carriers typically associate immediately to your name, address, date of birth, and even social security number, based on the information provided to cell carriers upon initiation of service. This information then becomes publicly accessible as data is shared, sold, brokered, or otherwise exchanged among third parties.

In order to protect your privacy and minimize tracking, harassment, telemarketing calls, and other undesirables, employ a service such as Google Voice, Blur by Abine, or MySudo to mask your device's true phone number.

Google Voice, Blur, and MySudo are three recommended and not officially endorsed solutions that enable users to generate their own virtual or internet-based (Voice over Internet Protocol, or VoIP) phone number. These numbers can be configured to auto-forward to your actual device (or be accessed through an application on your device), thereby connecting any calls or text messages. Function may vary depending on international travel.

Additional options exist through virtual office companies such as Regus, which offers paid call answering and forwarding services to the user. This is more useful from an organizational or business perspective than individual use.

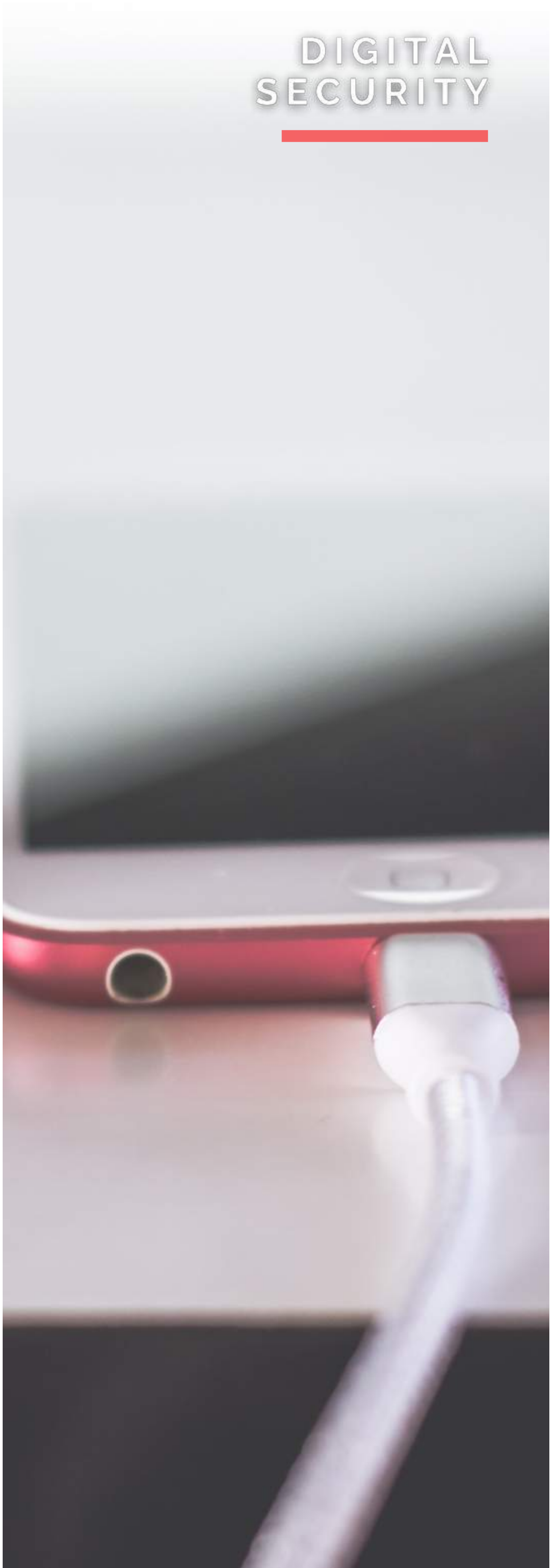
It is highly recommended you establish this practice and employ when interacting with hotels, restaurants, Ubers, unwanted social interactions, and the like. It is also highly recommended you register your number with the national Do Not Call Registry to limit number exposure to spam and tele-marketing calls.

Google Voice

Smart voice calling on all your devices

MySudo

Send private messages, manage multiple phone numbers and email addresses, and create custom personal identities that last as long as you need them.



TECHNIQUE #10

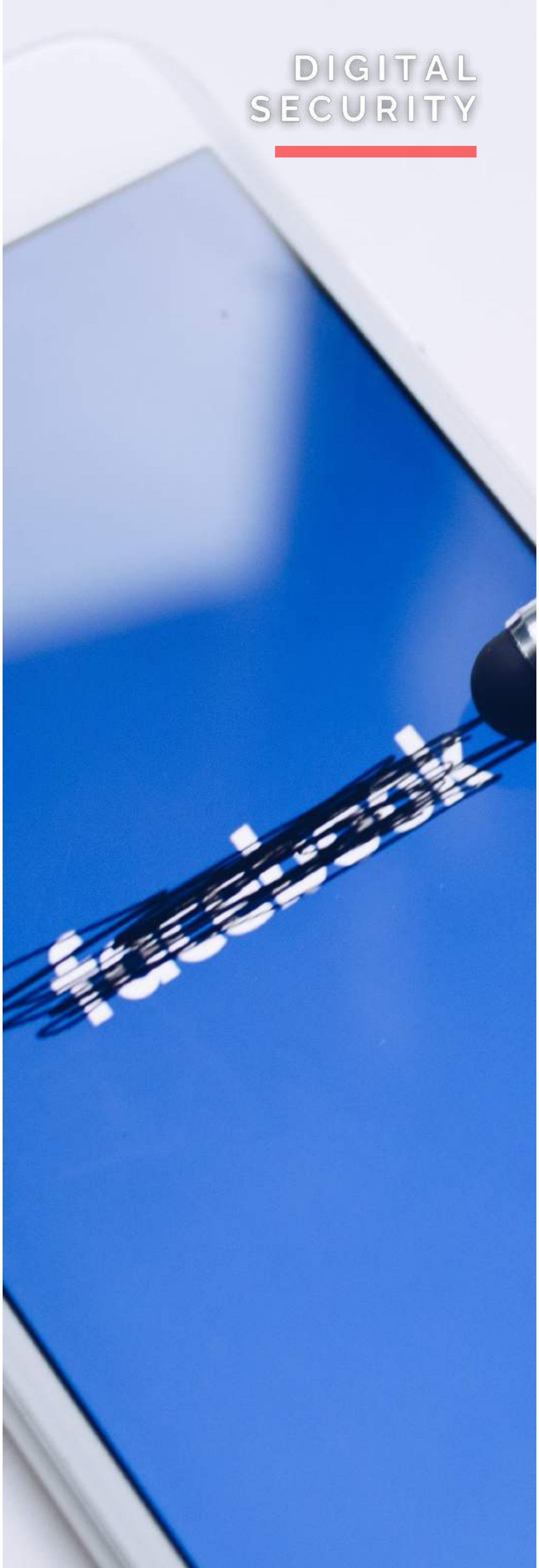
BE MINDFUL OF WHAT YOU PLUG INTO YOUR DEVICE

At some point, all of our devices run low on power and are in need of a charge. Be wary of what you use to charge your device, or of any external attachment that has a physical connection to your device.

For most people, this means the free and accessible USB power charging stations seen at airports, hotels, and other public locations.

Be mindful of what you plug into your device, as criminals and governments are able to modify these stations or inputs and use them to install malware or extract data from your device.

Employ a simple solution by bringing your own charger and plugging into a wall outlet, use a portable battery pack, or purchase a device that blocks data transmission and only allows for charging.



TECHNIQUE #11

BEWARE OF "LEAKY" APPLICATIONS

Phone (and other) applications we download to our mobile devices may be used daily or very rarely, but all apps typically need access to sensitive data on your device - often including your GPS location/position, personal information, user credentials, IP address, etc.

When we install these applications, we agree to the app terms of agreement and privacy policy. However, be mindful of which apps you allow this access, as extensive research has shown how countless applications leak user data to undisclosed third parties.

Most applications sell, share, or otherwise disclose user data to third parties in order to provide insights that can be used for targeted advertising, mobile location analytics, and marketing; however, more nefarious uses such as surveillance and espionage have also been noted.

It is recommended users take stock of the quality and quantity of applications on their devices, and at a minimum review the terms of agreement and privacy policies of those applications in order to become educated on what personal or potentially sensitive data is being shared with more than just the app developer.

For additional security and privacy, review the apps you download to your device(s) and remove those you do not absolutely require daily. Further, consider employing apps like Little Snitch, LuLu, or Lockdown Privacy to block all application tracking, advertisements, malware, and other general leaky app activity.

TECHNIQUE #12

DISABLE SIRI AND OTHER 'VOICE ASSISTANTS' ON ALL DEVICES

Mobile and computing devices often are accompanied by voice assistants such as Siri (Apple), Alexa (Amazon), and others. It is highly recommended you disable and limit all access to your device in the settings for optimal privacy.

While voice assistants promise hands-free and entertaining engagement to shop, research, or accomplish basic tasks like placing phone calls or transcribing messages, they pose a serious privacy concern due to their accesses and management by the companies that support and market their use.

All voice assistants require microphone access to your devices in order to listen for voice commands. This audio captures all conversations within range of the microphone, as the device must wait to hear and recognize the various voice commands that activate it (i.e. "Hey, Siri").

Additionally, this audio is recorded by the various parent companies and used to inform research and development for artificial intelligence, voice recognition software, and other efforts to personalize user and computer interactions that comprise the user experience. Often, this is done for the sole purpose of targeted advertisements but also constitutes a grave threat should the data be in the hands of or accessible to hostile state or non-state actors for the purpose of espionage or surveillance.

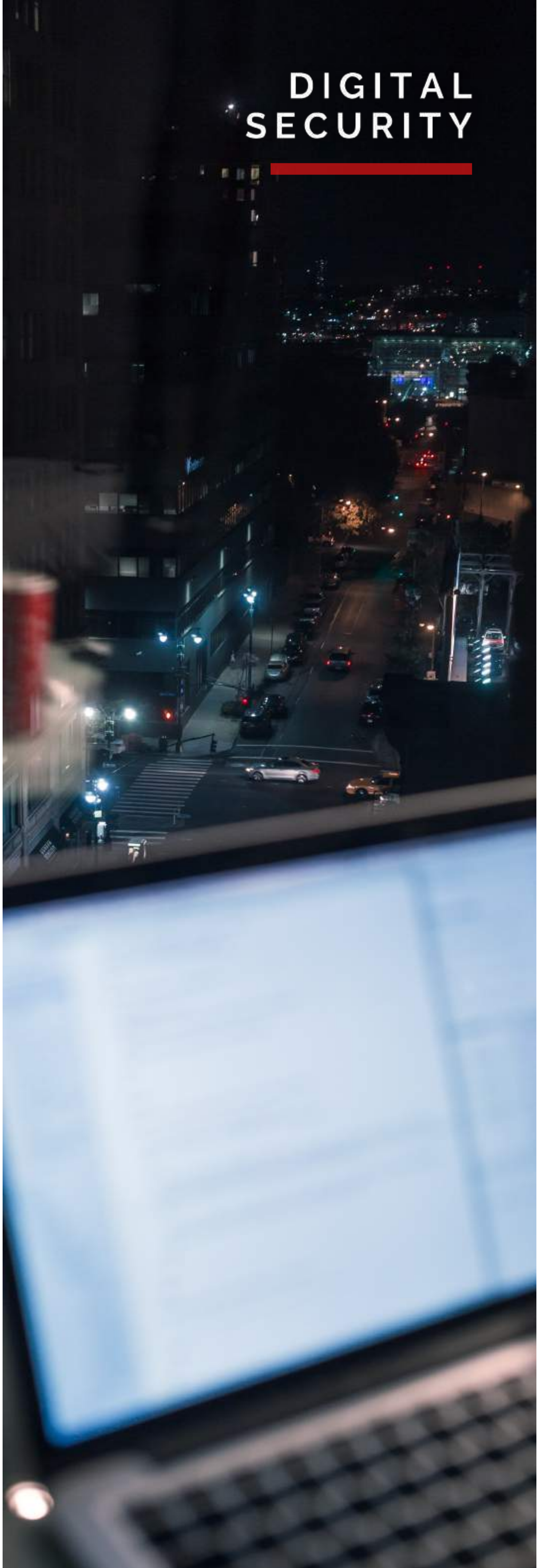
Just last year, Apple apologized for the revelation made public that Apple contractors were able to access Siri voice recordings and listen to private conversations recorded of Siri users. Such blatant infringement of user privacy is not uncommon with voice assistants.

Please learn how to disable Siri on all devices here.

PHASE 2: SECURE LAPTOPS & OTHER DEVICES

The majority of techniques are applied in a mobile device, end-user context. Our expertise is not focused on more network or computer-based security.

However, given the ubiquitousness of smart devices and their capabilities, there are a few noteworthy considerations identified that will assist you in managing your signatures online and elsewhere, regardless of the type of device. What follows are other techniques critical to digital security that augment, overlap with, or extend beyond a typical cell phone.



TECHNIQUE #13

COVER THE WEBCAM ON ALL DEVICES WITH A FORWARD-FACING CAMERA

The FBI recommends placing a piece of tape or cloth over any forward facing cameras, integrated or other, of all devices in order to prevent unauthorized and unwanted recording.

It is possible to activate devices' cameras without the indicator light illuminating. This practice has been used to conduct harassment, blackmail, and other forms of coercion from nefarious actors and is easily preventable.

TECHNIQUE #14

REVIEW WI-FI SETTINGS OF ALL DEVICES

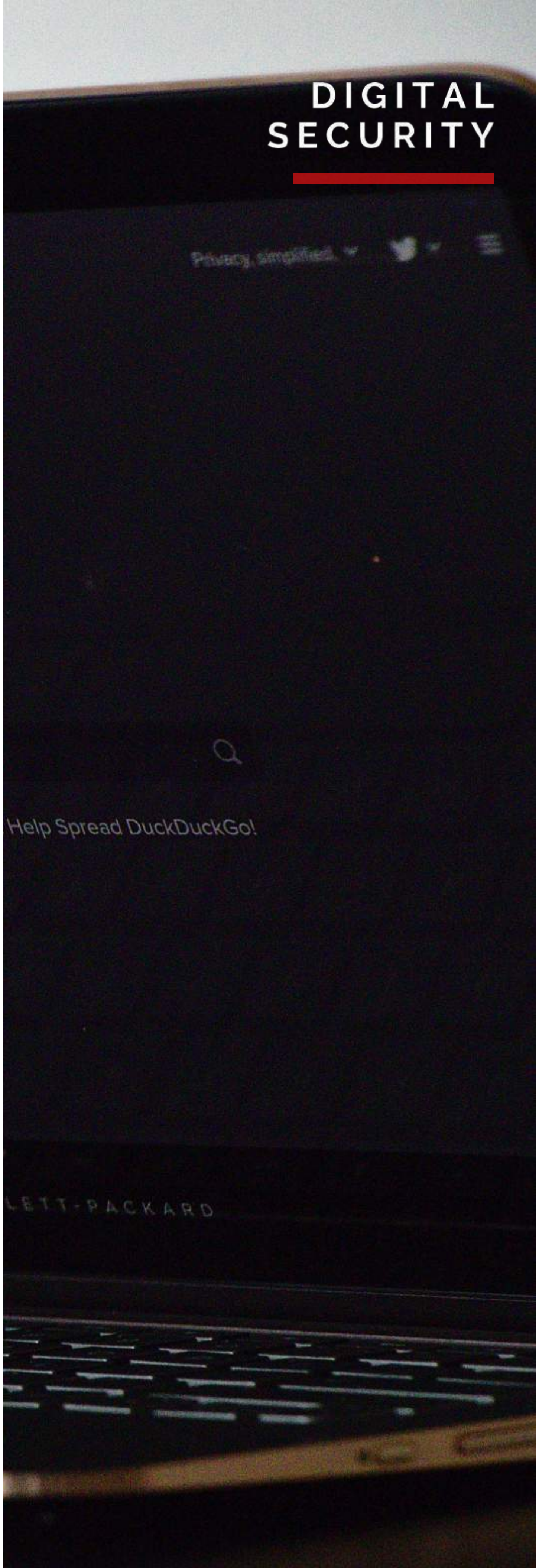
Laptops have the end user in mind and automatically save all networks it has connected to; while convenient for automatically connecting to home or office networks without having to enter a password every time, it also presents a possible security vulnerability.

Similar to cellular device Wi-Fi, a device that maintains a running list of networks it wishes to reconnect to is a significant risk that provides pattern of life for the device's owner as well as other unique identifiers for adversaries to search for, locate, and track.

Since most networks are clearly identifiable (e.g. Starbuck's Wi-Fi, Marriott Downtown Washington, etc.), where a device spends time can be readily ascertained.

It is recommended you ensure device Wi-Fi is disabled when not in use (albeit a lesser concern for a laptop which will likely not be running when not in use) and also enter System Preferences>Network>Advanced>[Delete Old Networks].

See Technique #1 for application of this practice in a cellular context; please note that the same method(s) of exploiting this vulnerability apply, meaning the efficacy of the technique applies to both cell phones and laptops or other Wi-Fi and Bluetooth-enabled devices.



TECHNIQUE #15

USE SECURE INTERNET BROWSING AT ALL TIMES

In addition to a VPN-encrypted device, it is highly recommended you download Mozilla Firefox as well as browser extensions that enhance your browsing privacy and security experience. Several exemplary browser extensions are: HTTPS Everywhere, Multi-Account Containers, U-Block Origin, Nimbus Capture, and KeePass-XC.

A highly recommended and comprehensive list for browser setup can be found in this amazing and detailed book.

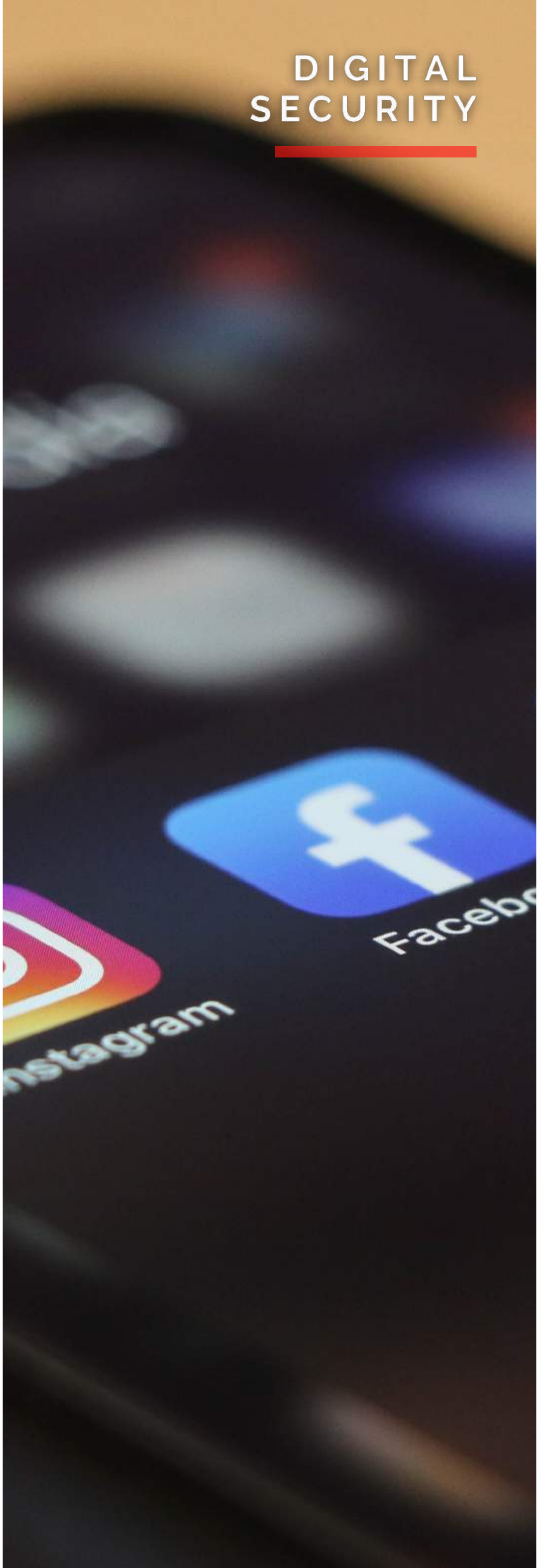
Other options for more private and secure browsing include using the Safari browser with DuckDuckGo as the search engine, or using DuckDuckGo's mobile application for browsing (cellular devices).

Additional information regarding web-browsing and digital privacy in general can be found at privacytools.io, included in the References section of this guide.

In general, these extensions ensure various encryptions on websites when browsing i.e. SSL or other, and block various advertisements, cookies, and other trackers of user internet browsing activities.

DuckDuckGo — Privacy, simplified.

The Internet privacy company that empowers you to seamlessly take control of your personal information online, without any tradeoffs.



TECHNIQUE #16

MAINTAIN LOW PROFILE ON SOCIAL MEDIA

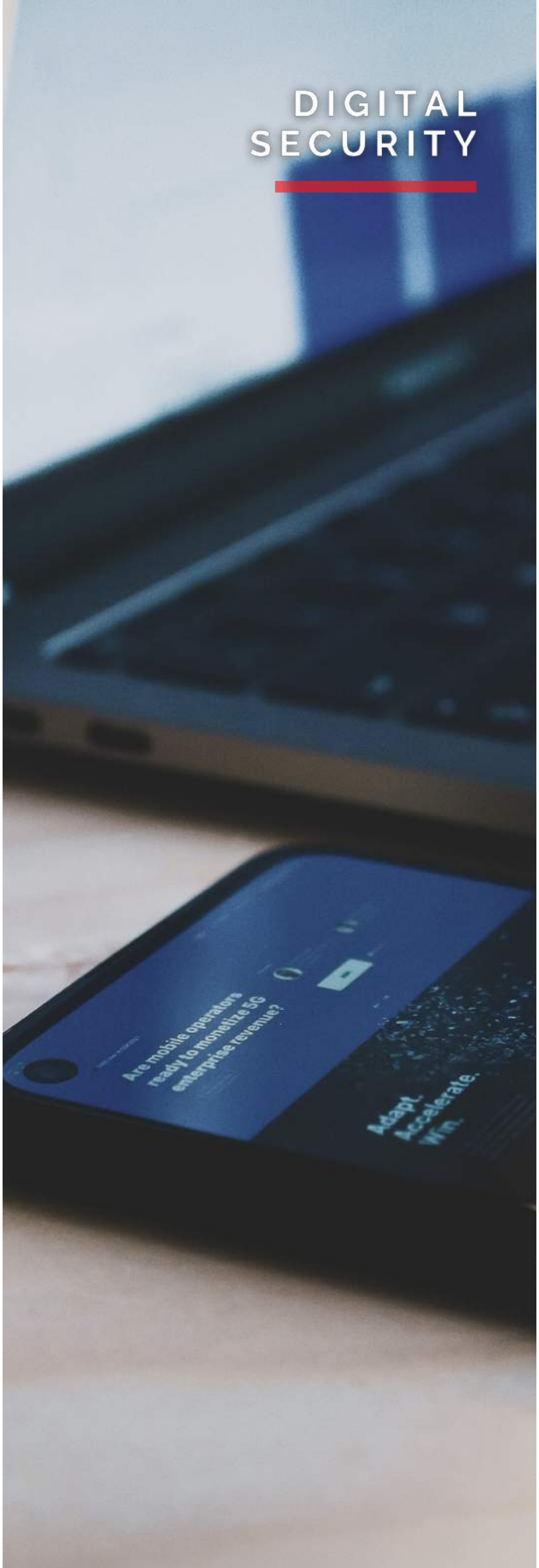
It is highly recommended you do not maintain public and open social media profiles unless they are sanitized of personal information and follow strict posting practices that limit exposure of location details.

Further, accounts should not use full name or any other personal information therein i.e. birthday, anniversaries, etc.

This is for obvious privacy reasons but is primarily to mitigate vulnerabilities associated with the targeting of accounts by criminal or other investigative elements.

Also ensure security and privacy settings are set to highest levels in order to avoid "leakage" of email or other account information.

For example, there is a feature in Twitter's password reset function that, if not changed in your settings, will leak a partial email address used to register the account, which provides additional data for any targeting efforts against social media accounts.


Are mobile operators ready to monetize 5G enterprise revenue?
Adapt. Accelerate. Win.

TECHNIQUE #17

COMMUNICATE USING SECURE EMAIL AT ALL TIMES

It is highly recommended that premium email services featuring end-to-end user encrypted messaging are used.

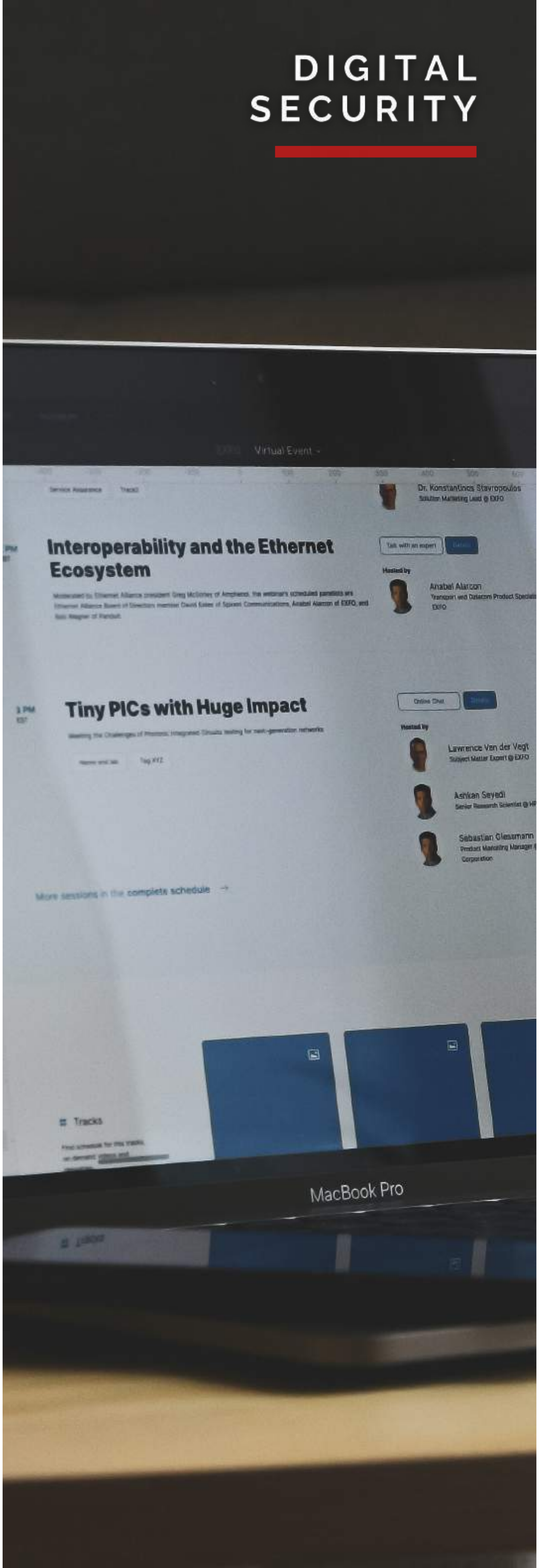
A highly recommended and not officially endorsed service is ProtonMail, a Swiss company with very high regard for user privacy.

ProtonMail offers excellent security features to include the option to send encrypted emails to non-ProtonMail users (requiring them to enter a password to decrypt the email and view its contents), as well as self-destructing messages.

Gmail is an additional option but has previously used users' email content for targeted advertising.

Sign Up for ProtonMail

Sign up here to get your free encrypted email account!


Virtual Event
Interoperability and the Ethernet Ecosystem
Tiny PICs with Huge Impact
MacBook Pro

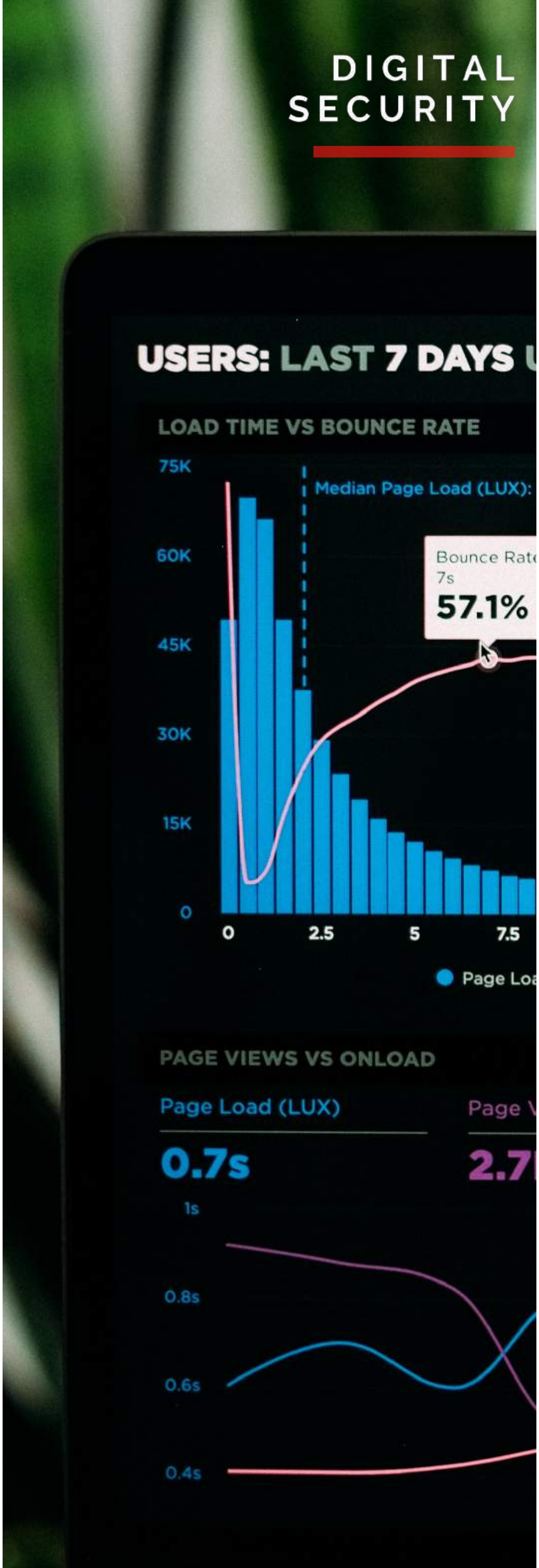
TECHNIQUE #18

CHANGE THE NAME OF YOUR NETWORK & DEVICE

Upon setting up a new device, change the device name to remove personal or equipment-related information i.e. Joe's MacBook Air or Susan's iPhone 6.

These will be visible when Wi-Fi and Bluetooth are enabled and provide easy identification to nefarious actors dealing in stolen electronics.

It is recommended users enter System Preferences>Sharing>[Change] Computer Name.



TECHNIQUE #19

REVIEW & OPT-OUT OF PUBLIC DATA MINER LISTS

There are countless entities maintaining publicly available data for free or paid access records, such as Spokeo, Whitepages, and others.

Personal information such as home phone, list of previous addresses, current address, relatives, approximate age, and other information is generally present.

It is highly recommended you manually opt-out of these services or purchase a service to conduct these purges in order to remove public listings.

One recommended and not officially endorsed service is Abine's DeleteMe. SMU also conducts data removal and online privacy management activities. Inteltechniques.com, included in the References section of this guide, generously offers a free and comprehensive guide for user-conducted data miner opt-outs hosted on their website, which we also highly recommend and for which we remain grateful.

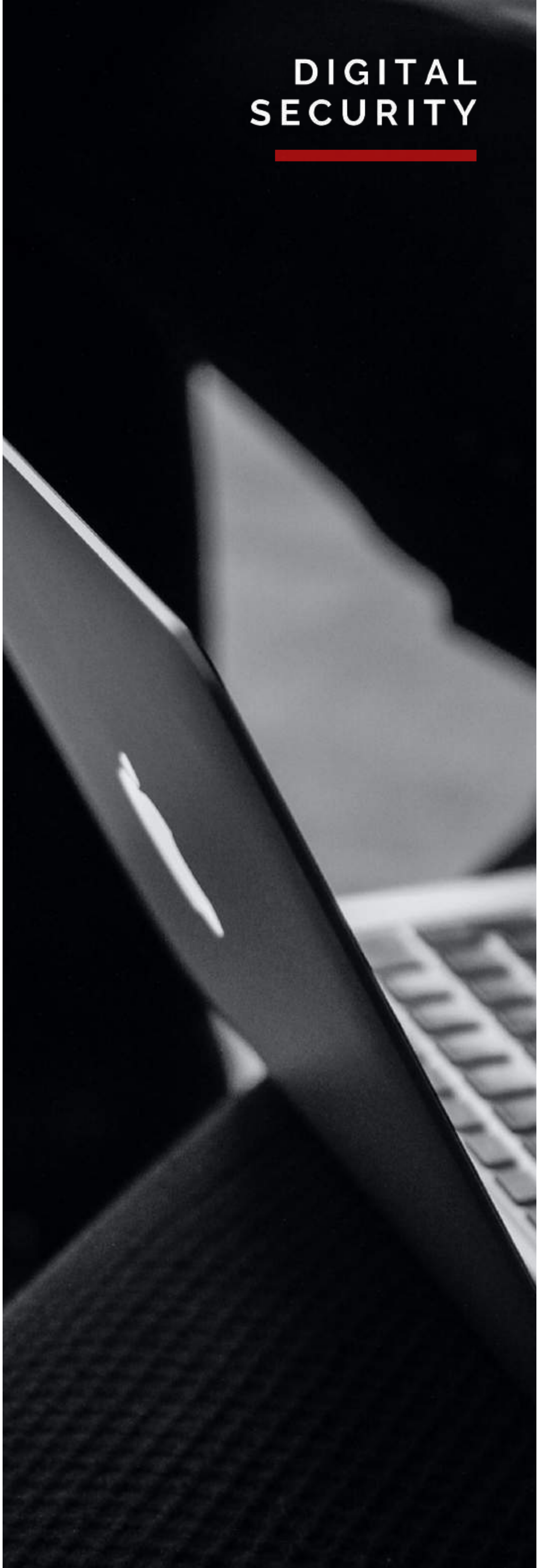
TECHNIQUE #20

ENCRYPT LAPTOP WITH FILEVAULT

Contents of devices must be encrypted to prevent unauthorized access while the device is locked or powered off.

FileVault (Apple) can be enabled by entering System Preferences>Security & Privacy>FileVault. Microsoft offers similar encryption through its Bitlocker service.

As with cellular devices, it is highly recommended devices remain locked - or better, powered off - preceding and throughout the duration of border crossings and customs.



TECHNIQUE #21

ENSURE STEALTH MODE & FIREWALL ARE ENABLED

These settings ensure that while connected to a network, the laptop will not accept any unauthorized connections.

Enter System Preferences>Security & Privacy>Firewall, and ensure it is enabled.

TECHNIQUE #22

ENABLE TWO-FACTOR AUTHENTICATION (2FA)

Multi-factor or two-factor authentication (2FA) is an additional security measure employed to strengthen the traditional login authentication of username and password.

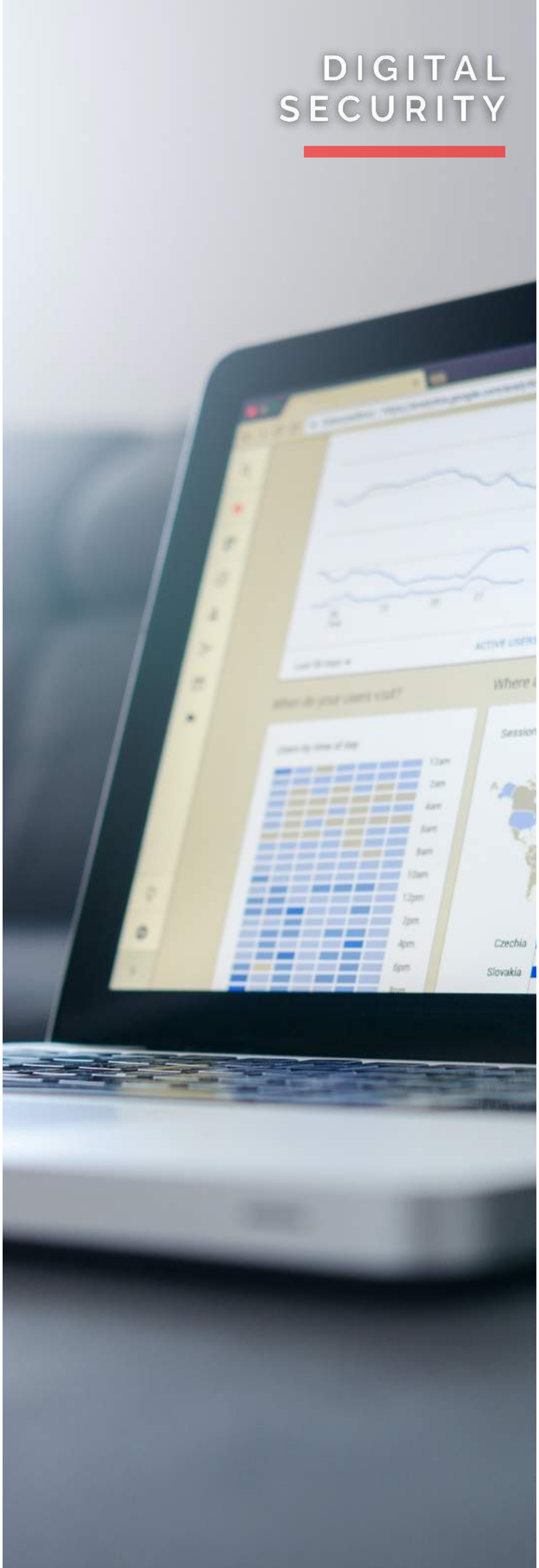
As technology and cybercrime advance, so must security. 2FA is one such advancement and comes in software, SMS, voice, hardware, biometric, or push notification forms.

The vast majority of accounts from email to banks offer 2FA and it is highly recommended users employ 2FA on as many accounts as able for additional security.

One recommended but not officially endorsed hardware option (more resilient against man-in-the-middle and phishing attacks) is Yubico's YubiKey (used by Google) for 2FA. YubiKey relies on U2F (an open and strong authentication form) for 2FA.

YubiKey - Fast and Simple Two-Factor Authentication

yubico.com



TECHNIQUE #23

EMPLOY A PASSWORD MANAGER FOR ACCOUNTS

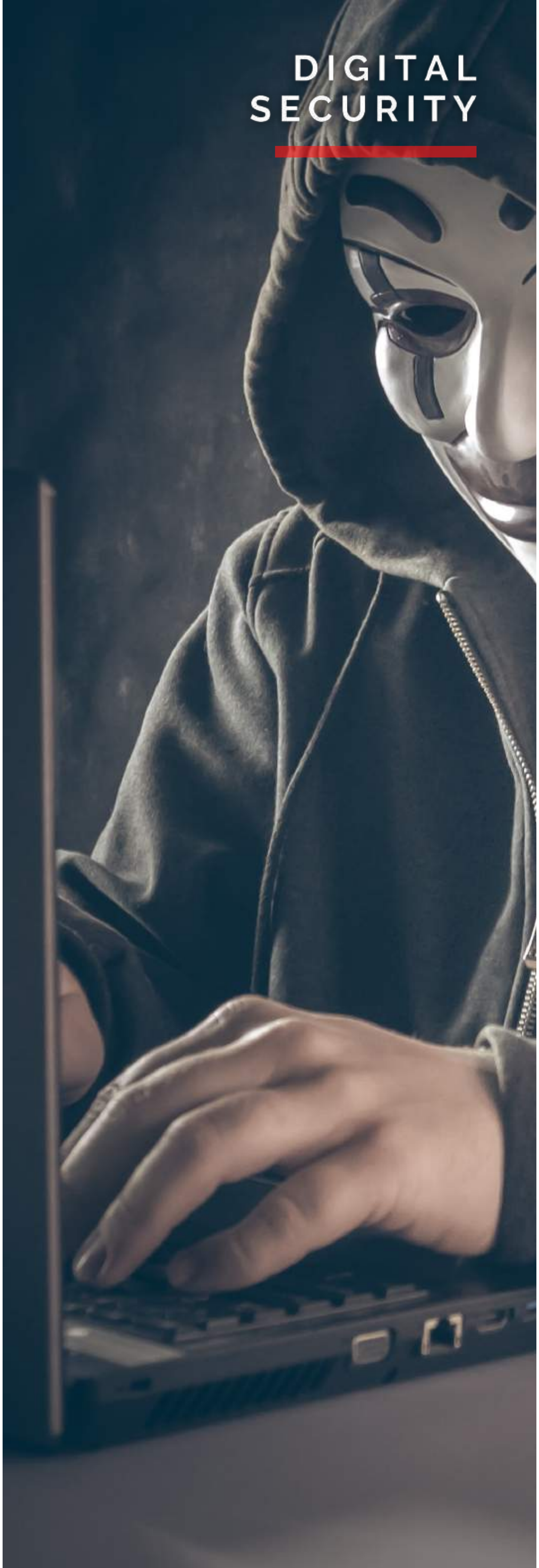
The rise in password complexity requirements is a result of ever-advancing cybercrime/threat capabilities. Increased threats impose convenience costs on users, which leads to exploitation when users become lazy or desensitized to threats.

Password managers are solutions designed to securely store your passwords, randomly generate new passwords for accounts, improve ease of access to accounts (i.e. automating logins vs. manual username and password entries), store secure notes, and other services to include VPNs, password sharing, and other functions.

A recommended but not officially endorsed password manager is Dashlane, which offers the majority of functions described above. There are countless password manager options available, and we advise you to conduct your own research to determine which password manager best suits your needs. A key criteria for selection weighs the more secure offline password manager options (i.e. KeePassXC) with online variants that synchronize across devices (i.e. Dashlane).

It is highly recommended you employ a password manager in conjunction with previously described techniques for optimized signature management.

Password Manager App for Home, Mobile, Business
dashlane.com



TECHNIQUE #24

DO NOT TRUST UNVERIFIED SOURCES

A primary method for gaining access to a target's device is through highly personalized phishing attacks. These attacks are delivered via messenger (i.e. WhatsApp), email, or other vector to you, the user.

Attack sophistication is largely dependent on threat actor capabilities; however, an exemplary software used by various intelligence and law enforcement agencies in such attacks has been (allegedly) used for cross-border mobile surveillance (in manners contrary to international human rights law versus their ostensible national security purposes), and possesses powerful capabilities.

It is highly recommended you only click on links or products from verified and trusted sources, and that any unverified or untrustworthy source is immediately disregarded and reported.

This is an obvious but overlooked practice generally disregarded due to complacency or fear.

TECHNIQUE #25

MANAGE PHOTO METADATA

Photo metadata, according to the FBI, are sets of data describing and providing information about an image. Many devices, including smartphones and digital cameras, embed various information into the images they capture, which is stored in a format called Exchangeable Image Format (EXIF).

It is possible to extract EXIF data from photographs using publicly accessible and free websites, which often provide contextual information that could illuminate one's location, date and time the photograph was taken, and other information.

Ensure devices are not storing metadata such as location, or "strip" the EXIF data from the image prior to uploading online.

For iOS devices, navigate to Settings>Privacy>Location Services, and ensure the Camera app is disabled. This will prevent location metadata from being stored by your device's camera when taking pictures.

TECHNIQUE #26

LIMIT DEBIT & CREDIT CARD TRACKING

Ensure financial institutions do not share your information or conduct tracking of your financial circumstances by limiting their ability to market your debit and credit card data.

It is possible for select institution account holders to submit opt-out requests directly with Visa and Mastercard in order to prevent your personal information from being included in "data analytics" activities conducted by these companies, who profit from sharing it with affiliates and non-affiliates for targeted advertising purposes.

For additional privacy, consider employing a card "masking" service that uses a trusted third party to issue you a virtual masked card (similar to a virtual gift card that does not share any actual true banking information to the merchant) for online purchases. Instead of entering your credit card information for purchases, use the virtual card to conduct the purchase, thereby "masking" your true credit card number and preventing it from being tracked or stolen. After the purchase is complete, the virtual card is "closed" and your data is protected. Companies such as Blur by Abine or MySudo both offer card masking services. Please note utility may differ when attempting to make "international" purchases due to anti-fraud and money laundering regulations.

To opt-out of Mastercard, click here.

To opt-out of Visa, click here.

TECHNIQUE #27

USE A MOBILE HOTSPOT FOR ADDITIONAL PRIVACY & SECURITY

In addition to browsing through a secure, privacy-oriented browser (e.g. Firefox Focus or DuckDuckGo) and employing a Virtual Private Network (VPN), a personal mobile hotspot can be used for internet access when public WiFi is unsecured, compromised, or unavailable.

During travel, you can anonymously purchase a mobile hotspot using local currency that leverages cellular infrastructure for a data connection to the internet. Use of a mobile hotspot provides mobile internet access (in areas where service coverage exists) in addition to limiting the need for or reliance upon potentially unencrypted public WiFi (i.e. in local cafes, train stations, airports, etc.). Use of a mobile hotspot that is under the user's control minimizes the risk associated with Man-In-the-Middle, Evil Twin, or similar type attacks.

Use of a mobile hotspot does not guarantee anonymity on or offline however, given the hotspot itself possesses various identifiers that, similar to other mobile devices, can be used to physically and technically track the device (see Technique #1 for Wi-Fi and Bluetooth tracking vulnerabilities). However, a mobile hotspot improves access to the internet in a mobile configuration and adds an element of privacy by controlling any users' devices access to the internet. It is an access point in the user's control, not one for public use.

As previously stated, ensure the hotspot is only accessed through a VPN and that the hotspot itself is password-protected / secured to prevent unauthorized access.

TECHNIQUE #28

PHYSICALLY SECURE ALL ELECTRONIC DEVICES

Depending on the location, electronic devices belonging to travelers may be physically accessed by security services or border control agencies hoping to glean insights or information from their owners - ostensibly for security and safety purposes.

During travel, this most often occurs during border crossings or in hotels. As was previously stated, an effective manner to access a device is physically, often through the lightning USB port (if an iPhone, for example). A similar concern exists for laptops and other mobile devices.

As such, it is not recommended that electronic devices are left in hotel rooms or other "public" locations during travel, even if devices possess full disk encryption. It is not advisable to present adversaries with any access to devices whatsoever if preventable (i.e. if not being coerced or pressured during a border crossing screening).

If possible, bring devices on one's person or in personal bags throughout the day, to ensure they remain under positive control. Conversely, should devices be left in a hotel room unattended, the user should assume the device is compromised and behave accordingly with respect to sensitive, proprietary, or other personal use of the device.

Note: While this guide does not prescribe legal advice regarding consent to security service or law enforcement searches of electronic property, additional resources can be found from the Electronic Frontier Foundation.

TECHNIQUE #29

MINIMIZE SURVEILLANCE & TRACKING WITH A FARADAY BAG

The nature of mobile devices are such that they possess a myriad of easily accessible means by which to track or locate a device to a relative degree of accuracy. Several of these methods have been previously mentioned, including the risks associated with unconnected Bluetooth or WiFi configurations on a mobile device.

To prevent any tracking of a mobile device when not in use, it is recommended you employ a Faraday bag or sleeve to block all radio frequency signals from being transmitted or received by the mobile device.

Faraday bags instantly block all radio frequency emissions from mobile devices (laptops, key fobs, cell phones, etc.), including: WiFi, Bluetooth, cellular connections, satellite (GPS) and other navigation services, radio frequency identification or near field communications, and any other form of emission on the electromagnetic spectrum.

Use of a Faraday bag makes devices "invisible" to electronic surveillance and tracking attempts, and is greatly useful for ensuring private conversation and an inability to be technically tracked while the bag is in use.

Faraday bags from Silent Pocket are highly recommended but not officially endorsed for users seeking to employ this level of privacy and digital security, and is highly valuable particularly during international travel.

DIGITAL SECURITY

TECHNIQUE #30

CONSIDER EMPLOYING "BURNER" OR "TOSS" DEVICES

Should travel lead one to an aggressive, hostile, or sensitive region that is not disposed to respectful or friendly interactions with westerners, it is advised for users to consider establishing one-time or temporary electronic devices for specific trips or locations.

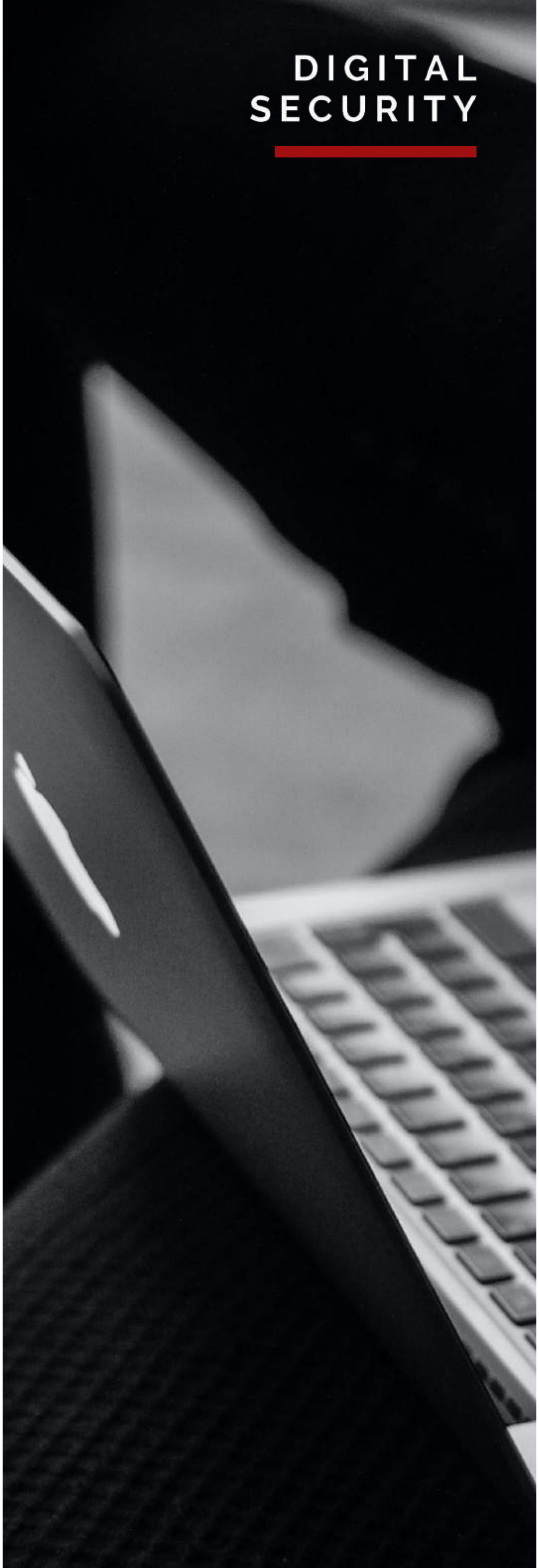
Known as "burner" or "toss" devices (typically phones), these electronics serve as a means of communication and connection without the extensive or unnecessary exposure of personal data to potential adversaries.

There are a number of considerations to engage prior to employing this technique, given a fresh device with little data or history could raise unnecessary suspicions of travelers seeking to avoid law enforcement or security service scrutiny. However, compartmentalizing one's electronic devices in such a manner does add a significant layer of defense to one's security and privacy posture, and greatly reduces risk of exposing personal, sensitive, or proprietary data.

An additional critical consideration for this technique is the requirement to compartmentalize all other aspects of communications along with the devices. This technique is invalidated if one obtains a toss device and proceeds to access one's personal email account from it. All communications and other accounts must be compartmentalized along with the physical devices for maximum effectiveness.

It is recommended users exercise prudence and deliberate thought when considering this technique, taking into account the information and privacy of the individual or entity this technique would protect, as well as the perception of potential adversaries when encountering this technique during international travel or at a border crossing.

DIGITAL SECURITY



TECHNIQUE #31

SET A FIRMWARE PASSWORD ON YOUR DEVICE

When powering on your laptop or computing device, there are different "boot" options that allow one to select which computer disk to start up. On an Apple device, for example, this usually boots automatically to a designated startup disk for you, the user.

However, it is possible -- without a firmware password in place -- for an unauthorized individual (i.e. a hacker, border control officer, foreign government official during travel, etc.) to access your computer through other, non-secured disks/locations (i.e. through other hardware on the computer). With free and readily-available boot programs designed for password recovery, an unauthorized individual with physical access to your computer is able to reset the default administrator account without ever needing your designated password. A firmware password mitigates this vulnerability by asking for a password before a user can boot to any disk or device.

It is highly recommended users set a firmware password on computing devices, which prevents users without the master password from being able to access or start the computer from any other disk than the designated start-up disk. This is a hardware-level security password that closes all gates to your device except the one you choose to keep open. After this firmware password is correctly inputted, it then leads to the normal username and password login to access your specific computer disk/account (i.e. the typical Apple user login screen).

Detailed instructions for implementing a firmware password (for an Apple device) can be found here.

PHASE 3: STAY SHARP

We've presented a handful of useful techniques with which to secure your cell phones and other mobile devices. However, now isn't the time to rest on your laurels. We've taken the initial steps, and now we continue down the path of growth by way of further learning. Stay sharp.

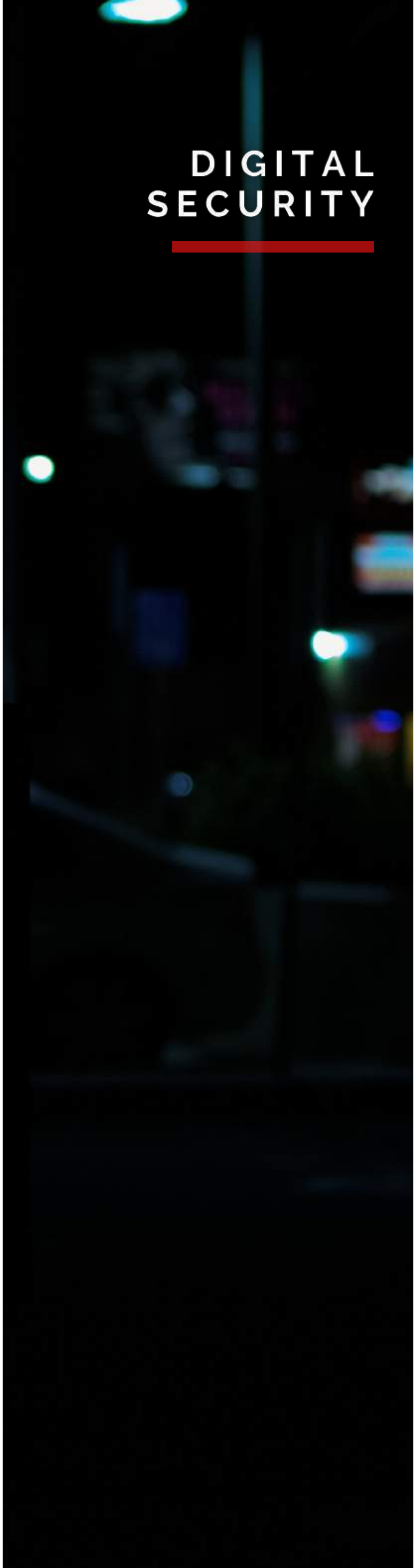
The contents of this guide were derived strictly from publicly accessible information sources and through research conducted using open source means - the Internet. Which means there's much more available to access.

As has been previously stated, none of the information presented in this guide is new, and mostly constitutes best practices based on current threat models that give you the edge in privacy and digital security.

We encourage you to learn as much as possible about these techniques and their criticality in enhancing your privacy and security. As the digital landscape continues to evolve and grow, the need for privacy and digital security grows with it.

There are countless resources available, a few of which are listed below. We cannot recommend them highly enough as deep wells from which to draw additional context and knowledge of digital security and privacy:

privacytools.io
tacticaltech.org
The Crypto Paper
Security in a Box
Surveillance Self Defense - EFF
Intel Techniques



DISCLAIMER & ACKNOWLEDGEMENTS

Copyright for this work remains with Signature Management Unit, as filed with the United States Copyright Office. However, we freely disseminate this guide and its contents to the public as expressed in our Manifesto and the purposes stated therein.

Despite the contents of this guide being derived from publicly accessible information sources and through open source means, the initial content received a local security review to comply with various regulations and ensure the protection of sources and methods. Further, this guide and its contents do not represent the U.S. Government or any official opinion(s).

We do our best to ensure the accuracy and quality of information and services we recommend, but are still only human. There is more than one path to the top of the mountain, and we welcome respectful discourse pertaining to technique improvements or other growth of our own skill sets and knowledge.

We intended for this guide to be comprehensive, relatively standalone, and portable. That said, the contents are not all-inclusive.

We could not and did not do this by ourselves. A heartfelt thanks to all those who proofread, edited, read, helped research, offered suggestions, or otherwise shaped this product with their keen eyes, expertise, and experience, including but not limited to: Stavros, Josh, Nick, Alex, Peter, Joe, Tom, Jess, Parker, Steve, Red, Lizzi, Kyle, Hans, and others!

DIGITAL SECURITY

HOW CAN WE HELP?

Please do not hesitate to contact us with any questions or comments, technical or other, pertaining to the contents of this guide. Digital security and privacy are very much active efforts that require thoughtful care, which we strive to make easier for you here in this format.

Signature Management Unit
Great Lakes Region
(202) 952-1511
contact@signaturemanagementunit.com
www.signaturemanagementunit.com