SAFETAG Self-Assessment Checklist (DRAFT)

SAFETAG (Security Auditing Framework and Evaluation Template for Advocacy Groups, https://SAFETAG.org) is a Creative Commons-licensed framework which aims to make traditional penetration testing and risk assessment methodologies more relevant to small, non-profit human rights organizations based in (or operating in) the developing world.

This guide simplifies the vulnerabilities that the SAFETAG process tests for, and focuses on providing a systems administrator a clear list of changes based on common findings from SAFETAG audits to upgrade their organization's digital security setup.

Even this streamlined checklist is somewhat long, as local context defies a simple to-do list. Nevertheless, each major section concludes with a "checklist" of the core tasks to perform.

Neither SAFETAG nor this guide are intended for non-technical audiences — but both strive to be clear, understandable, and actionable by a much broader audience than those who would traditionally self-identify as a "penetration tester", "white-hat hacker", or even a "system administrator" (in the case of this guide).

This guide follows, loosely, the SAFETAG framework's sections (methodologies). It skips past the testing framework and steps to create evidence of a risk to focus instead on a broadly applicable set of good practices. The four sections "target" different aspects of security - first risks that could be exploited without any physical access to the organization or its personnel, then moving to attacks that require some amount of proximity or even direct physical access. Advanced — or even simply curious — users of this guide are encouraged to dig deeper by visiting the full SAFETAG framework at https://SAFETAG.org.

[[TOC]]

1 Remote Risks

These risks combine the SAFETAG “Research” and “Remote” methodologies, covering risks against attacks which are able to be performed from anywhere in the world - they do not require specific proximity to the organization’s offices or personnel.

One of the most difficult tasks for a system administrator is to switch their mindset and think like an attacker when checking their own security - this is one of the most valuable reasons to work with an external auditor who can come in to the task without any “insider” knowledge. Nevertheless, the first phase of assessing your security should be to simply research everything that is knowable about the organization without any privileged access. The website of an organization (as well as other online and social media presenses) is a rich source of information, often including the names board members and organizational founders and leaders, connections with other organizations and individuals (through social media accounts of the organization as well as personal accounts of staff members), addresses, key organizational details (founding date, key phrases/mottos), and even organizational registration and tax information in many countries.

In addition to this openly sourced data, there are specific remote attacks which can be targeted at your organization. Starting with a website address, it may be possible to get a list of sub-domains associated with that address - so if www.sample.org is your organization’s website, an attacker would be also interested if there was an ftp.sample.org or an intranet.sample.org. There are two ways to test for these secondary sites. The first is simply to have a list of likely subdomains (admin, cms, ftp, intranet, staff, inside, portal, web, mail, webmail, email…) - SubBrute (https://github.com/TheRook/subbrute) is one of many tools, and it will try and guess 30,000 subdomains in around 5 minutes. The second way is to request a “zone transfer” (https://en.wikipedia.org/wiki/DNS_zone_transfer) from the name server (https://en.wikipedia.org/wiki/DNS_server) which manages your website. These are increasingly turned off or restricted by default, but it is worth checking with whoever manages the name server(s) for your domain(s) to make sure.

Web

Each subdomain presents a new potential “attack surface” and provides a possible path to malicious actions. It is simply not the case that a “secret” subdomain that’s unlisted is unfindable, and webmasters and system administrators should take equal care with all of their web properties, and shutting down or preventing outside access where possible. The below pointers apply, then, as much to *www.sample.org* as to *oldwebsite.sample.org*, *beta.sample.org*, *super-secret-intranet-for-staff-only.sample.org*, and so on.

If any of these servers (even “skunkworks” or testing sites) are hosted internal to the organization — in a back office or server closet — realize that remote access to that server places an attacker inside your firewall and directly on your network, with the potential to also install malware directly from a trusted “internal” site.

Remote: Web Checklist

- [ ] Update any “front end” software (often a CMS like Drupal or Wordpress) *Note that “static” HTML sites can benefit from increased security and resilience to DDoS attacks.
- [ ] If the site is using custom software (built by a consultant or one company), strongly consider moving to a more well known or hosted platform.
- [ ] Make sure the server software itself is up-to-date
- [ ] Do you have SSL enabled for at least site login (to protect passwords) - if not, your site administration and user passwords are sent in the clear and are easy to intercept.
- [ ] Do user accounts get locked out if they try to log in incorrectly too many times?
- [ ] Can you restrict non-public sites to be accessed only locally at the main office, or through a VPN? What additional layers of security can you apply?
- [ ] What other ways do site and server administrators access this server? Are any of them unencrypted (FTP being a common culprit)? Disable any unencrypted access methods and move to encrypted options (SFTP/FTPS, SSH…).

Email

Your email server is (by design) knowable by looking up the “MX” (Mail eXchange) address for the website. The above bullet points are worth checking as well for your email and webmail servers. In addition, it is important to make sure that not only does your email server support encryption (SSL/TLS/HTTPS), but that it in fact requires it. Without forcing an encrypted connection, an attacker with proximity to your network or users (including at a coffeeshop) — or with access to your ISP — could intercept your email password (which is often connected to other valuable accounts), but also the entire content of your emails).

Further, it is important to deactivate accounts which are no longer used, as well as regularly rotate the passwords of any “shared” accounts (like info@, help@…). It is better to find ways (such as using a distribution list or an email-connected “ticketing” system) to not need to share accounts. When a staff member leaves an organization, their account access (email and beyond) should also be terminated according to an organizational policy, such as an immediate password-change by the system administrator (allowing for an “out of office” auto-responder) for 30 days, then archiving of the account and forwarding further emails to it to a superior for an additional 90 days, then complete termination of the account.

Remote: Email checklist

- [ ] Try to connect to your email servers accessible via non-encrypted channels, disable them if they are available.
- [ ] Ensure that encryption required for login/authentication
- [ ] Regularly change any generic/shared email accounts, or use lists to manage this functionality more securely
- [ ] Deactivate all unused email accounts according to an organizational policy

2 Proximity Risks

These attacks cover the SAFETAG “Perimeter” methodology, and require an attacker to be physically near to the target (either the offices, people, or their homes). It is important to note that most of these attacks do not require long periods of proximity, but only a few minutes of information gathering up front.

Wireless Networks

Wireless networks should be secured with WPA2 encryption. WEP and MAC address filtering offer no security against an attack. Even WPA2 encryption should be protected by a strong password - four or more words or an uncommon phrase with a few special characters added in, is generally secure. Simply one or two dictionary words with a date added on is very common, and very susceptible to brute-forcing. An attacker need only a few minutes within range of the target wireless network to capture enough traffic for their computer to try millions of combinations of possible passwords. After a few hours (or days for stronger passwords), the attacker can return and join the internal network without any difficulty.

Some of the most common wireless passwords for organizations are a part of the organization's name, address, or mission statement combined with a year (either the year the organization was founded, or within the past 10 years). So, Sample2013 (organization name + a year, so also Sample1999, Sample2000, etc.) or 123mainstreet (Sample Org's address) would likely be a few custom password segments an attacker would add in to a large dictionary of common passwords.

Of course, who has access to the password is also important - if you have guests coming by the office, they should be given access to a "guest" network (many wifi routers now come with this built in), which segments them off of the core network. The office wifi password should also be changed with some frequency to limit access by former staff members or anyone else who has gained knowledge of the password.

Proximity: Network checklist

- [ ] Secure your wireless network using WPA2
- [ ] Disable WPS
- [ ] Create a separate guest network with access limited to only the Internet; don't ever share your office wireless network with guests.
- [ ] Use a complex wifi password that does not use dictionary words (or at least uses four or more!), parts of your organization's name, a year, or the address of your office.
- [ ] Change the wireless password at least once per year, preferably quarterly.

Remote access

This collection of possible attacks includes a variety of ways an attacker might remotely access your network. As such, it is somewhat connected to purely remote attacks, above, and also network-access attacks, below.

For direct attacks against your office's network from the Internet, an attacker would have to know your IP address. Most ISPs rotate your IP address regularly - from as little as every hour to up to weeks or months. "Static" IPs are often included with business-grade connections, and are important if you are running services (email, websites, etc.) from your offices. The downside of a static or infrequently-changing IP is that it is slightly easier to attack, but even with a "dynamic" IP address, there are ways to find your office's current IP - Skype (as one example, working as of March 2014) can leak your public IP address.

You have more to be worried about than just targeted attacks, however. Bots regularly scan for common ways to break into any machine connected to the Internet . For an office, this means having a firewall and making sure that it's active and well-configured. Most routers and modems have some form of firewall built in; while they're not ideal, they provide a decent level of protection. Use a remote scanning tool to double-check your settings (GRC's Shields Up! provides a web-based tool: https://www.grc.com/x/ne.dll?bh0bkyd2)

Proximity: Remote Access Checklist

- [ ] Make sure all of your network equipment (modem, wireless router, firewall, etc.) is using updated software
- [ ] Change the default passwords (http://www.routerpasswords.com/)!
- [ ] Ensure your firewall is active, and double-check the expected settings using a remote tool. Be aware of and limit open ports in your firewall.

3 Network and Physical Access

This section combines the “Local” and “Physical Access” sections of SAFETAG. It is worth noting that successful proximity attacks against a wireless network are likely to grant network access to an attacker, and that further attacks could quite easily set up long-term remote access to the network. However, many of the defenses against both these more remote attacks, and defenses to improve your security against equipment seizures, are similar.

Infrastructure

For offices with shared resources based around one more more servers, those servers provide a very valuable target for an adversary to obtain valuable information about the organization and its partners, as well as to surveil or alter the work of the staff. Servers should be kept in a secure, locked enclosure with access limited to only those who need actual physical access to the machines.

Backups

Organizations should follow general best practices to ensure their servers have not only electrical or battery backup systems, but also regular data backups, with at least one copy of the data kept outside of the office in a safe location (bank safety deposit boxes or a fire-proof safe at the home of a director are common). Given that both the server and the backups contain highly sensitive data, the drives and data should be encrypted, making it harder for an adversary to access the data by stealing the device. Encryption complicates backup schemes, making it all the more important to conduct a backup test, guaranteeing that critical data can be restored from the backups (especially in the situation where the office servers and the backup software itself is lost/confiscated).

Internal Network Services

It is relevant to consider that a well-resourced adversary can, with targeted effort, connect to an organization's internal network through the attacks detailed in the Proximity Risks section above. Reducing the points of potential vulnerability (turning file sharing off of any computer that is not sharing files, for example), and taking steps to minimize sensitive data that is accessible on the network are the best defenses against this. Having sensitive data reside on a specific (encrypted!) external hard drive that is only connected to computers which are not also at the same time connected to the network is an implementation of this which does not overly complicate an office's workflow. This also means changing default passwords on network routers (They're well known: http://www.routerpasswords.com/).

Network and Physical Access: Infrastructure Checklist

- [ ] Have a power backup system (UPS, standby generator, or a combination) to protect your servers from electrical failure
- [ ] Back up your servers (and office computers as well). Encrypt the backups, and test their viability! Save a recent backup copy off-site at a less vulnerable location and rotate this backup at least every 6 months.
- [ ] Physically protect your servers and backups (locked but ventilated cabinet, room, etc.)
- [ ] Ensure that the servers are running updated software and are regularly receiving updates.
- [ ] Focus on using or migrating to well-maintained and updated software and

applications.

- [ ] Have a regular (at least quarterly) review of who has access (both physical and via login rights/passwords)
- [ ] Monitor specialized security alerts for the server software and any install applications
- [ ] Minimize the number of applications used to the bare minimum
- [ ] Find ways to remove highly sensitive data from the network
- [ ] Double-check, using security auditing software such as Metasploit, that the servers are up to date and running only the expected applications

Computers and Software

Similar procedures and warnings apply for the computers used by an organization's staff - the top concerns are using legal/licensed software (protip: If your copy of Windows cost $1, it is probably not correctly licensed!), having software and training to resist malware, and drive encryption.

Licensing and Updates

No matter what operating system your staff works with (including Mac OSX and Linux variants) keeping up with updates is absolutely critical. Many small and lean organizations have a mixed collection of organizational computers and staff using their own personal devices part or all of the time - not to mention the role that personal smartphones now play in accessing work email and more. The advice in this section applies to all devices. Policies, supported by reasonable support, are important to ensure that no staff, contractor, or volunteer works on sensitive material using a system which is not up-to-date with legal/licensed software. Organizations like TechSoup (http://www.techsoup.org/) can help non-profits in getting proprietary and often expensive software at more reasonable rates.

Anti-Virus and Anti-Malware

Virus and malware defenses are critical. While the architecture behind MacOSX and Linux make it more difficult for malware to cause damage, they are by no means immune to the threat. All computers should have anti-virus systems and malware detection tools in place and constantly up to date. Many commercial tools require ongoing, paid subscriptions to access the latest lists, and provide no effective protection without those updates. Even free versions often require attention to re-validate your account and ensure ongoing updates. It is important to review these tools and make sure they are updated at least monthly. The Security In a Box section on malware provides not only a more in-depth look into this challenge, but also guidance on specific tools to use: https://securityinabox.org/en/chapter-1

Disk Encryption

The most recent releases of all major operating systems include built-in support for hard drive encryption. MacOSX has the easiest implementation of this with File Vault 2. For Linux, it is quite easy to set up during a fresh install. Windows 8.1 includes BitLocker for even the "basic" version of their system, with the caveat that you must share your decryption key with Microsoft (presumably so that they can support you if you forget it). The professional version of Windows 7 and 8 include BitLocker with this key escrow as a non-required option. Hard drive encryption is a computer's only real protection for the contents and metadata it contains once it has been lost or confiscated.

Unencrypted data are vulnerable to any number of simple attacks, the two most straightforward being: 1) rebooting the computer from a USB stick CD-ROM or DVD

containing an alternate operating system, then copying all of the data; or 2) removing the hard drive, inserting it into a different machine, then copying all of the data. These techniques, which work on nearly any computer, even if a strong login password has been set, are effective and widely used, but they require extended physical access to the device. A slightly different attack is the Inception attack, which only requires physical access for a few minutes. It, too, works regardless of login/screen-lock passwords, and even out of date encryption software — though only devices with Firewire ports or expansion slots (ExpressCard, CardBus, PCMCIA, etc.) are vulnerable.

The steps required to defend against all of these threats is the same: encrypt your data using the latest versions of tools like Microsoft's BitLocker, Apple's FileVault2 or the open-source Truecrypt application, combined with using the most up-to-date versions of the corresponding operating system software. The Inception Firewire attack is particularly illustrative, however, because it serves as a reminder that merely setting up an encrypted volume is not enough. In much the same way that a lock does little to protect your home if the door to which it is attached remains open, data encryption is rarely effective while you are logged into your computer. Even if the screen is locked (which would foil the "reboot" and "hard drive removal" attacks described briefly above), an attacker may still find a way to access your sensitive data, while the computer is up and running, because the decryption key is present in the computer's memory. (This is how large-scale encryption actually works. Information remains encrypted at all times, on the storage device where it lives, but you are able to access it while you are logged in, or while your encrypted volume is "open," because your computer decrypts and encrypts it on the fly.)

Other Software

In the same way that the most up-to-date versions of operating systems and anti-virus tools are important, the same goes for all software on one's computer. Minimizing the "extraneous" software, and ensuring that it is being regularly updated, is key. Only download software from trusted sources, and when possible verify downloads using their md5 "hash" using a tool like the File Checksum Integrity Verifier (http://support.microsoft.com/kb/841290)

Services

Any third party service - gmail, dropbox, facebook, twitter - and even explicitly high-security providers like lavabit, hushmail, and "private" VPN providers - is susceptible to various risks. Recent revelations about the capabilities of governments - primarily the US - show that government-level actors have great leverage to force even well-meaning service providers to give out sensitive information about their users. That being said, many companies do work to protect their users to the fullest extent they can, and can be very strong advocates in providing services which are secure against most attackers and even most government-level attackers. It is important to balance the security these do provide against the actual threats you and your organization face.

Many services provide much more monitoring of suspicious activity and active

management of the service itself than an organization would have the capacity or funding to support - this is most often true with email services and file sharing/collaboration tools. The downside of hosted services is that they are hard to manage from an organizational standpoint; inevitably former employees will still have access to documents long after they have left, and there is no easy way to enforce a password policy. Users could potentially log in from public computers and save their password by accident, exposing data.

These risks must be balanced per organization, and based on the tools and services needed by the staff.

Office Computer Physical Security and Backups

Local, physical security is also valuable in a variety of threat models. Office computers should automatically lock themselves after a relatively short amount of idle time, and always when sleeping/hibernating, forcing a password to be re-entered afterwards. Using cable locks to secure computers, laptops, and other mobile hardware such as external hard drives to furniture may also be useful against theft and to reveal attempts at tampering.

If staff computers are regularly backed up to an office server or third party service, checking to make sure the backups are secured in a way that is consistent with the rest of your security practices is important.

Network and Physical Access: Computers and Software Checklist

- [ ] Upgrade to licensed copies of all operating systems
- [ ] Encrypt hard drives, using TrueCrypt or built-in encryption tools like BitLocker or FileVault
- [ ] Disable FireWire drivers if not needed (see http://www.breaknenter.org/projects/inception/#Attack_mitigation)
- [ ] Set system updates to automatically download and install
- [ ] Install anti-virus systems and ensure they also automatically update. Monitor their license status to ensure that this continues
- [ ] Install anti-malware tools
- [ ] Run both anti-virus and anti-malware scans regularly
- [ ] Backup staff computers in a secure, encrypted method
- [ ] Only download software from trusted locations
- [ ] Be intentional with which third-party services (gmail, google drive, dropbox, skype…) you use, and apply the same user management care to them as you do to your email access
- [ ] Password-lock computers when not in use
- [ ] Turn computers off at the end of the day, consider physically securing them to furniture

4 People, Travel, and Mobiles

These questions go beyond the core focus of SAFETAG, and are meant to encourage system administrators to think about the importance of how and where staff are connecting to their central services, and what this means within the context of what threats they are concerned with.

Hiring and Support Services

The staff you hire to help you with your digital security needs are key. Establishing trust is very important, and finding ways to mitigate risks while increasing your security and understanding the balance of some reduced functionality and ease of use is important. Even long-serving, highly-trusted staff members can become points of vulnerability - limiting the ability for any one person to secretly access systems or data through policy and practice is the best defense.

Even for support personnel, any technician who has extended access to your computer or access to the administrative passwords is a risk. Preferring computer work to be done on-site (in a shared, open area or conference room) is one of many ways to reduce risk. If off-site servicing is necessary, removing the hard drive before sending it is one option (if the problem is not software related, of course).

People, Travel, and Mobiles: Hiring and Support Services Checklist

- [ ] Establish a hiring policy and practice which incorporates trust through references or other methods
- [ ] Reduce the ability for any one person (even a trusted staff member) to have private access to secure data or systems
- [ ] Prefer services, particularly computer repair services, to take place on-site or in the company of a staff member

Personal Digital Security Staff

Passwords

First off, let's talk about passwords. They are the painful bane of existence for most users - length and complexity requirements lead to difficult-to-remember strings of nonsense, which discourages using different passwords for different services (important to protect yourself when one service gets breached, as is a sadly common event).

Asking 5 digital security experts about passwords will get you 10 answers. The best answer depends on what you and your users will actually adopt and take to heart that improves your security.

The single most important aspect of password security is length. For any password you'll only type in a few times per day, creating a *pass-phrase* makes it much more secure. An easy to remember sentence, with even just a few random characters thrown in, provides an immense level of protection against automated password-cracking software. Password cracking software takes two main approaches brute forcing and dictionary attacks. Raw brute force attacks always will work, but take exponentially longer against long passwords. Anything eight characters or less, even with symbols, mixed case, and numbers, will take less than a day against a hacked/leaked password file, while a simple phrase ("the eagle has landed") would take aeons. However, against a dictionary attack, where selected lists of words (all english words, the top 1000 passwords from previously leaked password databases, etc.) are used to speed this process up, and some are bringing in phrases from popular literature to begin to wrestle with phrase-based passwords. Regardless, length with some variation (if you're using words that can be found in dictionaries, or sentences from literature) are your friends.

More difficult to keep up to date with is changing passwords on a regular basis. From a pragmatic standpoint, passwords protecting sensitive data should be changed regularly (every 6 months). For organizations, this should be set as an automated task by the system administrator. Forcing this too often will generally result in lost passwords, or poor quality passwords, or both. Organizations also need to be careful with password reset policies. Tools which use questions ("What is your favorite color?") are surprisingly easy to guess or research the answers to, and care must be taken to select questions which elicit unique answers using information which is not public.

Password management tools, such as KeePass, can be a huge benefit to managing many different passwords, as well as making password resets less painful. Security in a Box maintains a solid chapter on good password use, as well as how to use KeePass: https://securityinabox.org/en/chapter-3 . https://www.grc.com/haystack.htm provides a nice "calculator" of sorts to play with different types of passwords and see their strength against password cracking tools.

One last note with passwords is that, finally, many online services have adopted "two factor authentication" which provides a mobile app or SMS follow-up to logins, especially from unrecognized devices. This provides a life-saving second line of defense against password hacking.

Working Remotely and Traveling

Sometimes, we all just need to connect to the Internet, and are not at home or at work. There's an open wireless network, or we're at an airport, or a café, or in a meeting or conference. It's important to keep in mind that in these cases, not only is the manager of the network able to watch (and in some cases, redirect, block, and manipulate) your connections, but everyone on that network, if motivated, can do the same. Networks without password protection are even more vulnerable to their traffic being sniffed. There are frightening tools which are easy to use and abuse to track all unencrypted traffic that goes across a network, and tools which can trick a user who thinks they're going to a secure site to instead be redirected through an insecure path - such that they "see" the site they expect, but with all of their (presumed secure) traffic being vulnerable to an attacker.

The best protection against most of this is to always use a VPN (Virtual Private Network) when connecting from a network you do not trust (or, ideally, any network other than ones you manage). VPNs create a secure tunnel from your computer to the VPN server. Many home routers can be configured to provide a VPN, so that anywhere you are in the world, you can look like you are connecting from your home. VPNs are also popular for offices, allowing remote access to local "on-network" resources.

It's important to note that VPNs do not provide anonymity, they only create a pipe from where you are to somewhere else on the Internet, but that somewhere else - especially if it's a commercial VPN provider you've paid for, sees your traffic just as easily as someone in our hypothetical café above. For further discussion on ways to secure your traffic from eavesdroppers and become more anonymous when online, see https://securityinabox.org/en/chapter-7 and https://securityinabox.org/en/chapter-8 .

For systems administrators, it is important to consider what information users might access remotely, and make sure that they are forced to use secure channels for any sensitive information or organizational services - from email to ftp, anything that has a password is a potential leak.

In addition, content saved on laptops - documents, emails, spreadsheets and more - are at risk, especially when the laptop is "out and about", and border crossings or other security checkpoints are often places where normal protections against property seizure are not present. There is no foolproof protection against this, though the hard drive (and any other media!) will prevent unauthorized access to the contents (but the owner may be forced to give out the encryption password, and if the computer was not fully off, there are other attacks).

It is generally ideal to simply not travel with sensitive documents, and to not trust any device that was taken from your sight. Some laptops, like the chromebooks, are designed to be very secure against malware or hardware being added to them.

Behavior

Finally, there is a vast trove of potentially risky information that is easily leaked as staff members go about their daily lives.

Online social networks like facebook and twitter are very valuable for keeping in touch and spreading news, but are also very easy for any adversary to use to explore your network and find collaborators and partners. While sites like http://actualfacebookgraphsearches.tumblr.com/ make light of this, searches like "Employers of people who have been to ЄвроМайдан – EuroMaydan" work quite well, and are easy to abuse to put pressure on individuals or organizations who have expressed their beliefs on Facebook.

A classic, persistent, and powerful threat organizations face is "Social Engineering" (https://en.wikipedia.org/wiki/Social_engineering_(security)) - the act of using often elaborate and well-researched confidence scams to gain access to sensitive and useful information, from gaining account passwords to simply causing a user to open an email attachment which surreptitiously installs a remote access tool.

There is no technical response to behavioral challenges beyond the important basics of having up-to-date computer software with updated anti-virus and anti-malware scanners. The best defense is ensuring ongoing education and awareness of your staff to always question email attachments and other in-bound, unsolicited contact from anyone claiming to be connected to a service, bank, or similar. The best response to any of these is to end the conversation and call the service using a known contact number directly. For attachments, using a preview service like Google Drive, or a Virtual Machine to "sandbox" suspicious documents can help.

People, Travel, and Mobiles: Personal Digital Security for Staff Checklist

- [ ] Create unique passwords for each service or website
- [ ] Make your passwords long, but memorable. Use a combination of four or more unrelated words. See https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html for further discussion.
- [ ] Consider using a password manager to help create and manage multiple highly secure passwords
- [ ] Change passwords, at least for high-risk services, regularly (annually at the *very* least)
- [ ] Support staff having access to a VPN, and encourage its use when connecting from public networks (cafes, airports, hotels…)
- [ ] Be on the lookout for attempts to gain valuable information - especially passwords - through "social engineering" attempts

Mobile Devices

In high-risk environments, mobile phones are particularly problematic. The government and your mobile network operator tend to have easy access to records of the location of the phone, call, data, and SMS logs, and can even track content if dedicated. Pirate towers are unfortunately easy to set up by a dedicated adversary and can force the phone into unencrypted communications, as well as provide good access to “man in the middle” attacks. Even phones with open source operating systems, or using custom ROMS like CyanogenMod, are susceptible to many attacks due to the “baseband” system accessible only by the operator.

With that as a disclaimer, mobiles are essential to most people as tools of communication in both their personal and professional lives, and these are most often mixed together in the modern smart phone.

In an ideal world, organizations would provide managed, locked-down smartphones to their staff, and those would be the only ways to access organizational data. These would be remotely-wipeable and configured carefully. The reality is that most staff members would rather add work email and messaging to their existing, personal device rather than carry a separate device. However, it can be difficult to convince users to allow centrally-managed security procedures on their personal phones.

Most smartphones have built in device encryption, but it is only “activated” if there is a passcode lock on the phone. This should be a minimum requirement.

If the organizational email server is correctly set-up, it will only allow encrypted communications. Staff should be aware, and know to not try and override these settings, and to never trust unencrypted email connections. Some email server solutions allow the server the ability to remotely wipe the device and/or the email on the device.

Secure Communications on Mobile Devices

There are good applications for secure, mobile communications, but mostly for the Android operating system. ChatSecure (versions available for both Android and iOS) supports encrypted communication over popular chat protocols such as gchat and facebook. It also interoperates with CSipSimple for secure voice calls (over the data network).

There are some mobile security applications worth mentioning, to better manage lost/stolen devices and reduce the risks involved in these. Prey and Lookout are independent implementations of this system, and both the Google Play store and Apple have built-in capabilities as well.

Mobiles and Wifi networks

Each wireless device maintains a “memory” of what networks it has successfully connected to. When it is connecting to a network, it sends out “probes” to all of the networks it has in this memory. These probes can reveal personal, organizational, and

locational information that, taken in context, can be dangerous or lead to other vulnerabilities. This applies to laptops as well as mobile devices.

It is important to note that this data gets broadcast widely, and can be collected without any network access, only proximity to the device. For most devices, deleting networks from the “saved” network list will stop them from being probed. Obviously, this can be an annoyance for networks you regularly connect to, so renaming these networks to non-revealing names would help, as would creating non-name-associated “guest” networks for colleagues connecting to your home network. On iPhones and iPads, it is not possible to selectively remove historical networks unless you are currently in range of that network.

It is however possible to remove all history: go to Settings > General > Reset > Reset Network Settings . When you take this step, it is worth going through this reset multiple times – approximately once per year of device ownership, as the first reset appears to only remove recently-connected networks, and older networks will be broadcast.

People, Travel, and Mobiles: Mobile Security Checklist

- [ ] Enable a passcode lock and ensure the device is encrypted
- [ ] Any cell phone - even basic “feature” phones - provide location tracking information to the mobile service provider (and likely the local government)
- [ ] Cell phone calls and SMS are not secure, but programs like RedPhone, TextSecure, and ChatSecure provide encrypted alternatives
- [ ] Devices broadcast the history of wifi network names they have connected to. Clear network history regularly.

Appendix I: General Resources

- Security In A Box (https://securityinabox.org/) has multi-language guides to installation and use of most popular digital security tools. http://www.speaksafe.internews.org/ provides a similar, slightly more focused version.
- Guardian Project has a series of useful tutorials for mobile device security at https://guardianproject.info/apps/tutorials/
- EFF (https://www.eff.org/) and Access (https://www.accessnow.org/) both maintain tools, documents, whitepapers and post updates on digital security and advocacy topics
- My Website Is Down (https://github.com/OpenInternet/MyWebsiteIsDown) offers a walkthrough of responding to website challenges, focusing on distributed denial of service attacks
- Kali Linux (http://www.kali.org/) is a distribution of Linux that can run from a flash drive or be installed to a computer which builds in many useful network and security testing tools.
- TAILS (https://tails.boum.org/) is a distribution of Linux that can also run from a CD or flash drive, which routes all communication through a secure network - very useful in recovering from a situation where you suspect a compromise.
- Level Up provides further resources for training users on digital security: https://level-up.cc/