Bylines, not Tombstones: Self-Protection for Journalists and Sources

The Tradecraft of Security

Journalists are Targets!

804 journalists have been murdered since 1992 because of the job they were doing, according to the Committee to Protect Journalists. Countless other journalists were verbally or physically attacked because of their work. Compare that to the 113 deaths the CIA says it has suffered since its founding in 1949.

Part of the reason Journalists seem more at risk is that federal agents are trained in, and practice, tradecraft. Journalists – well, not so much. Many gamble that nothing will happen to them.

Security should never be a bet or a gamble, a reliance on luck. Professional bettors are not gamblers. They know the odds. They understand how to count the cards. Tradecraft removes much, but not all, of the need for luck in providing security. Tradecraft eliminates the gamble when the journalist makes a security decision.

Tradecraft consists of the lessons learned, often by hard-won experience, that are passed from one professional to another. Tradecraft has been proved over many generations. While tradecraft rules can be broken successfully, they should only be ignored for good reason and with full knowledge of the dangers of non-observance.

Compromise on security tradecraft and, sooner or later, your own security will be compromised!

Security tradecraft:

- Minimizes risk to ourselves and everyone we talk to.
- Protects families.
- Protects our key sources.
- Protects materials, plans, and procedures.
- Denies opponents information about **our** vulnerabilities.

Security tradecraft is not like a guarantee on a car; it is more like proper maintenance – do it and the chances of a major problem are lessened. While threats are diminished, they never vanish completely – no matter how good the security plan.

There is no perfect security plan.

Security is extremely individualized. The problems facing one person are different – in most cases far different – than those facing another researcher. No "one size fits all" security plan exists, either. From the outset you must plan your own protection, based on your unique circumstances and use the tradecraft most applicable to your own circumstances. Nothing here should be considered "doctrine," but rather "best practices" when conducting investigative searches. This is a compendium of "thinking points." For instance, you must decide, early on, whether you want to try for anonymity or settle for some degree of privacy on the Internet

There is a marked difference between privacy and anonymity. A reasonable privacy level – there are many levels of privacy – is relatively easy to achieve. True anonymity is difficult, perhaps even impossible, for the average user in many cases. Anonymity means no one is able to track the user or see both what the user is doing and tie that activity back to the user personally. It does not mean that no one can see or record what is being done, rather that no one can connect you and your IP address to the activity.

Researchers and investigative journalists usually strive for anonymity but expect that in many cases what they will probably achieve is a high degree of privacy, a level approaching anonymity.

That said, don't be lulled by the word "privacy" and what seem like promises of privacy.

"Privacy modes" on some browsers often disable some cookie collection and prevent collection of some information about websites that you visited. But privacy modes do not stop search engines or the Internet service provider (ISP) from tracking your activity. Engaging "privacy mode" is a tiny, though sometimes useful, step in improving your security. Privacy modes do not prevent the ISP, search engines, or the sites you visited from seeing you and recording your activity.

Still, never reject any privacy-producing feature or technique. Protecting your privacy goes far to increasing your security, but it is not anonymity.

..*

Security falls into one of three categories:

- Basic security takes into account all major threat types.
- Enhanced security covers basic security, plus threats based on specific actors.
- High security covers both Basic and Enhanced security plus likely threats from organization or governments.

Many individual parts of your life and work need protection. List, for yourself, some of these, to see what specific things need protection:

- Notes and other resources.
- Sources and people we talk with.
- Families – ours and the families of sources.
- Plans.
- Day-to-day activities and operations.

Then mark down, next to each of those, the ways you and your employer are currently protecting them or plan on protecting them. Understanding your current security level is vital. You must understand what you are currently doing before implementing any changes or improvements.

People are important. Again, review for yourself the "people" part of your list and review specifically who needs protection as a result of your work:

- You.
- Your sources.
- Anyone with knowledge of your activities.
- Anyone considered close to you or your sources.

What are you and your organization doing to protect yourself and these people?

An back-up means of determining your threat level may be https://salama.io. We consider this to be an auxiliary starting point because the questions are generic and may miss your individual circumstances. While we would rely more on your individual appraisal than a computer algorithm, both approaches provide food for thought in determining your security needs.

As you go along you will discover an unpleasant truth – others may decide they have a deciding voice in selecting your security level. You probably do not have the last word about your own security. Organizations you work for, or are associated with, often want to determine security plans and decide what level of security they deem "safe enough." Before beginning to draft your own security plan it is wise to keep – in the back of your mind – some idea of how you will deal with any differences between your actual needs and the perceived needs of the organization. You may end up following their path, you may change or augment it, or ….?

If you don't think you need any help or improvement in your security, just look at one area we will touch more on later – your own computer. Can others tell much about you when you are on their sites? If they can identify you and tell where you are, you are vulnerable: See some of what the other side can see about you and your computer. At these sites determine what is readily known about you:

- What is My IP Address: http://whatismyipaddress.com
- Browser Spy: http://browserspy.dk/
- DigiCrime: http://www.digicrime.com/noprivacy.html
- IP-Address: http://www.ip-address.com
- IPCheck: http://ip-check.info/?lang=en
- IPchicken: http://ipchicken.com/
- JonDonym: https://anonymous-proxy-servers.net/en/help/security_test.html
- My IP Info: http://myipinfo.net/
- OnionRouting Privacy Test: http://www.onion-router.net/Tests.html

Your computer is only one of many areas where your security may be at risk.

..*

The Basic Security Level

At the most basic level there are a trio of security threats:

- **Environmental** – Fire, flood, power disruptions, natural disasters and temperature extremes. Solution: Take standard precautions and back up research results. Make certain the backup is in a location where the threat won't destroy the backup copy as well as the original.
- **Mechanical** – Disk failure, power surge. Solution: Use surge protector, know signs of disk disintegration, and back up to a secure location at least daily.
- **Human** – Site administrators, webmasters, hackers, subjects of articles, government or insider threats. All of these can steal information or see what you are doing. Solution: Use good security precautions and procedures.

Security plans must be based on a security mindset, a way of thinking that may not be normal but is not paranoid, either. "Normal" people don't usually concern themselves with security when doing research or using the Internet. They sign on their computer browser, look for information, and sign off without any thought of the dangers that may lurk there. For you, ignoring the need for security can be dangerous. At the same time, over-concern about security can immobilize your research efforts. A security mindset takes a realistic approach to the problem and allows you to find real solutions.

When the environmental and mechanical threat are met, it is time to go the human concern.

Business is considered by many to be the biggest snoop as firms try to achieve targeted advertising. If there is a way to improve profits by tracking you, your individual interests, likes, dislikes, and monetary habits and searches, business will be among the first to collect, buy, and sell your information. They, and governments, have developed an entire toolkit to thwart your anonymity and privacy. Governments, from China and Russia to the United States want to collect everything everybody does on the Internet. Governments use bulk surveillance and try, with some success, to get program developers to put in a back door in programs so they can track everyone. Governments seek to use only a small portion of that material, but they want to collect every click, every address, every message, every 1 or 0 that moves anywhere on the Internet. They seem prepared to save anything they collect in perpetuity, hoping that it might be useful later. Hackers, some of whom are employed by other sinister characters or have dangerous motives themselves, also have potential interests in the material researchers and journalists collect.

If there is a Golden Rule of security tradecraft it is this: Avoid attracting attention to yourself or your sources! Virtually every facet of security tradecraft comes back, in one way or another, to this golden rule. Much of the remainder of this handout will deal with the ways to make yourself less visible, less vulnerable, and less open to compromise by those who would do you, your sources and your medium harm.

A good defense is a planned defense, a defense based on critical information, risk, threat, vulnerability, and available countermeasures. Understand these security concepts. They are the foundation you will use in building the security structure that serves your unique needs.

- **Critical Information** – Information that could harm a researcher, reporter or editor, the organization or its work, or any of the other people you previously identified as needing protection.
- **Risk** – An event that could cause damage.
- **Threat** – Any adversary with both hostile intent and capability.
- **Vulnerability** – A weakness that could be exploited.
- **Countermeasure** – A procedure to reduce vulnerability.

Start your security plan by writing down the answers to these questions:

- Who are your adversaries, or potential adversaries?
- What do they want?
- How do they get it?
- How could you thwart them?
- What else can go wrong?

Understanding the identity, desires, and capabilities of your adversaries, or potential adversaries, is critical. What they want, their capabilities to get what they want, how they would get their way, and how you can thwart them, must be understood. Sometimes what else can go wrong is known – often it is not.

With the understanding of the adversary that is known or knowable, it is time to look at your own situation. There are a handful of inward-looking security steps, some of which you have already touched upon but may need to expand.

- Identify critical information to be protected (what do I need to protect?)
- Analyze threats and risks (who or what are they?)
- Analyze vulnerabilities (where are my potential weaknesses?)
- Assess risks (what the dangers?)
- Apply countermeasures (how do I reduce those risks?)

The information that an adversary needs to prevent your success – Critical Information – includes**…**

- Your interests.
- Your limitations.
- Your specific plans: Who, what, when, where, why, how.
- Your products and capabilities.
- The identity of your personnel and families.
- The identity of your contacts and families.
- Your security steps and methods.

Adversaries can be stopped by "countermeasures" such as:

- Communications protection techniques.
- Policies.
- Alertness and awareness.
- Reasonable suspicion.

Countermeasures need to become a way of life. Consider the threat when you use the computer or phone, answer stranger's questions, discuss work in public places, or engage in social networking.

Much basic tradecraft is often overlooked by most journalists. Shred and destroy all paper COMPLETELY. Putting notes and other important information in a trash can is insufficient. And take precautions against the insider threat – it does exist!

Adopt the "need to know" rule. People who don't need to know may be prone to talk in order to show how connected they are. Occasionally money, fear, or blackmail will make your associates talk about things they know, things they don't need to know, to people who have no right to know. Protect yourself and your associates. Don't tell people who don't need to know anything you have found out, or how your work is going.

Situational Awareness becomes a way of life. Situational awareness is always important. Determining whether your office or home is under observation, or has been entered, is one starting place. Checks should always be made to determine if you are being followed, either in a vehicle or on foot. **For more information on physical security, particularly as it relates to**

being followed and physically surveilled, see the associated handouts on surveillance and tailing.

Cleanliness is next to security. Never keep sensitive materials in a location that has little security. Keep your workplace tidy – everything in the right place – to determine whether it has been entered and searched during your absence. You can place items in locations or positions where they will fall over when disturbed. For instance, a straight pin can be placed so that it will fall out if a drawer is opened. Destroy everything that is no longer needed! Temporary hiding places should be prepared before the need arises. Permanent hiding places should be used for must-keep materials. These may be off-premises and difficult to access, such as buried materials.

It is important to have a secure room. Sensitive issues should not be discussed openly in the newsroom; neither should your plans, meetings or locations. Secure rooms should be on the inside the building and have no external windows. In the most sensitive cases the secure room should be locked and off limits to all but those involved in the investigation. All conversation about an investigation should take place in the secure room. It is wise to set up the room, or at least a part of the room, for access to secure computers.

In the more sensitive investigations, occasional sweeps of the secure room or areas where researchers work should be conducted for bugs or recording devices. While it is unusual to find any bugs or recording devices, they have been placed. What you will do and who you contact if a device is uncovered will be determined, in large part, by who you believe placed the bug. If you suspect a governmental entity is involved, obviously you would not report it to a government organization. If you believe it is some non-governmental group you may well involve police or other governmental agencies. But you also need to decide what to do about the discovery. Should it be ripped out, alerting the opponent that you found it, or should it be left where you found it? Leaving it in place may allow you to give false or misleading information to an opponent. If it is a type of device that requires periodic servicing, such as new batteries, it can be left in operating condition and cameras set up to see who will come again to service the device.

Destroy all unneeded documents as soon as they are no longer necessary to your work. This applies to both fiber (paper-type) and digital documents. You should also set aside some time each week or month to review all your document holdings and eliminate unneeded ones, particularly those that could endanger your personal liberty – or the freedom of your sources.

Communications, all communications between a source and a journalist, are highly risky for both. That is why you and your sources should always be asking yourselves "is this contact necessary?" If it is, plan it for security. Make the contact as safe as possible.

Communications are usually the weakest point in any security plan, providing bad guys their greatest opportunity. It is a weakness that adversaries often attack first. Adversaries want to know with whom you are communicating. That gives them a general idea of what you may be learning. In some cases that may be enough of a hint that they need to take what is euphemistically called "kinetic action."

Limiting all communications with sources is often wise. It is smart to ask "is this call or meeting REALLY necessary?" Remember: evidence of almost all communications are logged somewhere, whether with video cameras on the street or in a building, or electronically through phones, websites, chat providers, etc. Adversaries do not need to know the details of a particular communication to understand the threat you or your contacts pose; simply knowing who you are communicating with provides a good clue as to what you are learning from that source.

Personal meetings allow passing of greater amounts of information. Personal meet-ups are useful for putting correct emphasis on important information; they also facilitate immediate replies to your questions. For many journalists it is important to see and evaluate the information-provider. Face-to-face contact, or in the German *unter vier Augen* (four eyes only), is important, but it poses dangers for both parties. On the negative side, any meeting may arouse suspicion. In some cases meetings could be a trap or lead to an ambush of you or your source.

Meeting places with sources should always be thoughtfully prearranged. Pre-arrangement information should never be complete in a single message. Day and location should be given separately. Stated time need not be the actual time of the meeting, provided both parties understand how to modify the stated time. Adding or subtracting an hour or two to the time specified in the communications may cause interlopers to miss the actual meeting. When possible, the separate elements of the meeting's arrangement should be delivered through different methods such as the phone, email, or letter.

It is usually best for initial , where the two people do not know each other, to appear to be chance meetings. Passwords used in an initial meeting should never stand out. They should be appropriate to the time and location, and any activities going on nearby. Passwords must be chosen with care so that the reply could not be accidental. They should be short and spoken rather than being lengthy or involve gestures. Replies should be given at once.

First meetings should not be arranged at fixed points. It is often best to meet during a walk. For instance, one person may start from point X walking toward point Y while the second person starts from point Y and walks towards point X. If they fail to see one another they can walk back again one time. Another attempt can be made an hour after the appointed time. When meeting, greet one another as if it is an accident, chat for a moment while watching to see whether if you have been followed, and then go off together.

In subsequent meetings decide in advance whether the particular meeting should appear to be by chance or on purpose. That will determine behaviors of both parties and whether they need to carry items (newspapers, book, or briefcases) to swap.

So-called, but pre-planned, "chance meetings" can be staged on the street or at any location including art galleries, parks, common hangouts, and places of amusement.

Planned meetings can be held in appropriate public locations such as restaurants and bars, or in private locations such as homes and offices.

Pre-meeting visits to any link-up location may provide both cover and a chance to scope out the security of the area. Special attention should be given to avoiding video camera locations and places that would hide an interested onlooker.

Punctuality is important; watches should be synchronized from a common source such as a public clock. If one party fails to show up for a meeting the other party should wait or loiter in the meeting location no longer than 10 minutes.

Have a cover story for your presence at any meeting location. At any meeting, laugh and smile often; this suggests to onlookers that nothing serious is taking place. Never whisper at any meeting, since this invites attention and questions.

When safety is a consideration, danger signals to cancel or scrub the meeting – such as touching eyeglasses or putting both hands in pockets – should be agreed upon in advance. To guard against listening devices, where possible turn on radios or set up the meeting on a noisy boulevard (or if inside, turn on dishwashers or showers) to mask the conversation.

Finally, change meeting locations frequently.

Further information on physical surveillance and tailing is available through other handouts in this series.

Document or Other Information Transfers

Document transfers are sometimes conducted in an office or elsewhere. But when the transfer is possibly problematic, the transfer is often clandestine. Clandestine transfers are often done in a restroom or restaurant. Documents may be left in a briefcase that one person puts down while washing hands at a sink; the recipient simply picks up the briefcase and walks away. Or the documents may be concealed inside a newspaper or magazine that one diner gives to another. Often, when the documents do not require discussion, the people do not acknowledge one another. Try to make certain that no one else is around when a document transfer takes place.

Dead drops are usually the safest ways of transferring documents. In a dead drop the parties are never within sight or hailing distance of each other; there is not going to be a photograph of two people meeting. In fact, in a well-conducted dead drop there is no personal contact – sometimes there is never a personal meeting. The documents can be placed in a relatively secure location known to the other party. A sign – perhaps a pre-agreed number chalked onto a mailbox or the side of a building that the other person often passes – is used to alert that person to check the dead drop location. The person receiving the documents then goes to the hidden location and picks up what the first person left. Often the document recipient may leave a sign that the drop has been successful. Dead drop sites are generally in locations where relatively few people go. A dead drop site should not be selected where people never go or sites that are off-limits.

Intelligence agencies often use items like fake rocks or even what might appear to be dead birds. Everyone else may have to resort to less technically-advanced ways such as stuffing an item in the underside of a bridge structure or burying it in beach sand so many feet east or west of an identifiable marker.

Whenever conducting a meeting or a document transfer, always pay attention to gut feelings about safety and security…. They are usually based on something, some event, or observation that something isn't quite right, even if you cannot identify exactly what it is! Premonitions exist!

Online, there are a number of other tools that allow users to hide information "in the open" and share them without physical meetings. Many such tools fall under a category called steganography, or the technique of hidden writing. Steganography – also known colloquially as stego – has been defined as "security through obscurity." Stego, by itself, is not encryption although the message can be encrypted before it is put in a stego carrier. Sites such as OpenPuff can encrypt the file in a variety of different formats, which leaves the sender to choose the carrier-message format that works best with the enclosure.

Stego uses a carrier file that appears innocuous to contain the hidden message. No one except the originator and the intended recipient even suspect that a covert message exists within the file; moreover, a stego file is difficult for anyone without the access code to see, even if they knew or suspected that a stego message or file was being transmitted. Stego can be stored and transmitted within a variety of formats. Audio channels, visual channels such as pictures and videos, and even message headers can all be used as stego carrier files. These carrier files can be e-mailed, loaded into web pages, embedded in USENET files, and placed in files that can only be accessed using relatively little-used Internet resources. The type of carrier file used to contain the stego message, and the location of that carrier file, is extremely difficult to predict. Detection of embedded messages, files, or documents is extremely difficult, even for state-level agencies. **Further information on stego, and a primer on how to use it, is included in the Stego handout in this series.**

Many people concentrate on the World Wide Web (WWW, hereafter referred to as "the Web") as the place to find hidden messages, but OSINT professionals need to understand that virtually all parts of the Internet can be used as covert communications media. The Internet is actually a combination of many services, of which the Web is but one. The Web is often and incorrectly thought of as *the* OSINT resource, but just as there are non-Internet open source nodes, there are a number of Internet-related but non-Web channels for secret communication. These include:

- E-mail.
- Newsgroups.
- FTP.
- Telnet.
- Archie.

- WAIS (Wide Area Information Server).
- Gopher.
- Veronica.
- InterNIC.
- Finger.

Many of these Internet channels can be used as hidden pipelines or channels to communicate. Researchers should be aware of their potential in that role, as well as the difficulties, drawbacks, and problems associated with the more exotic, less-understood, and seldom-used channels.

Governments develop complex codes and ciphers for their people to communicate securely. Nongovernmental individuals and entities seldom have such exotic, made-to-order means available. They have to rely on a combination of ingenuity and the world of commercial encryption programs to provide a high level of security. Reporters are at some disadvantage when it comes to ciphers, of course. But some commercially available encryption programs deftly even government-level code breaking. While the strongest cipher can eventually be broken and the message read, it willoften take so long to do so that the information will be stale and therefore of limited or even no value.

Most, but not all, hidden channel communications rely on a combination of invisibility and encryption. That is, the message is both hidden and rendered unreadable except through some translation or decryption technique.

Of course, not everything in hidden channels is encrypted. For instance, one hidden channel uses a single on-line e-mail account that is shared among several people. One person writes a message in the shared account but leaves it in the e-mail folder as a draft. An associate who has access to the same account then signs in and reads the message in the draft folder, or leaves another message. Since the e-mail is unpublished and doesn't move through the usual digital channels there is a reduced chance of outsiders intercepting it.

Another technique of covert communication involves the use of special web pages. One method is to put the hidden page on a web site but keep out spiders and web search engines by special coding or, commonly, simply by not linking the special web page any other page elsewhere. Spiders and search engines gather their information by moving from one link to another; when there is no link, the spider doesn't go there. When a linkless page is created, the intended recipient of sensitive information is given the URL (web address) of the hidden page and accesses it simply by typing in that address. Information on such a page may or may not be encoded.

Another tactic is to create, in effect, two sites at the same address. In this system, there will be an innocuous cover page as well as the message-bearing page that the web site operator wishes to hide from certain traffic. Because the operator of the system (sysop) has the ability to detect where a site is being accessed from (i.e., where the potential viewer is physically located), the

operator can automatically direct people to, or away from, pages based on their location. Suspected users or those from an area that is thought of as antagonistic might be directed to one page; users from an area where supporters are concentrated might be directed to the message-bearing page.

Secure Drop

This is a messaging and document submission system operated by the Freedom of the Press Foundation. It is designed specifically for journalists and is available at https://pressfreedomfoundation.org/securedrop

Mail Issues

The outside of all United States mail is photographed by the post office.

Return addresses, personally identifiable information, and even fingerprints or other physical clues to a source's identity may be contained on the envelope. All envelopes, letters and enclosures received from any confidential source should be copied and the originals destroyed to prevent them from falling into any investigators' hands.

Keep in mind that modern copiers leave nearly-invisible identifying marks to show what machine printed the copy – much like typewriters used to draft a ransom note can be identified and matched to a document.

The hidden marks that identify the printer or copier are usually yellow, arranged in such a way as to tell investigators or properly-versed people about the machine that produced the print-out or copy. Since most companies and agencies log information about the printer user and time it is possible to narrow, if not pinpoint, the identity of the print requestor. When the recipient of the document keeps the original it poses security dangers to the source since the dot code can be used in identifying the leaker. Proper document handling of copied or printed documents is essential, as is speedy destruction of any documents, envelopes, or original materials. Where possible, it is best to reproduce the text of any documents by retyping – not on a copy machine – and then completely destroy the original and any letters, envelopes or materials that could link the document to the provider. Originals or any associated material often have genetic material or latent fingerprints that can pinpoint a source if adversaries are able to obtain them.

Printers also retain digital images of the pages they spew out, allowing for matches to be made that way. Recopying of documents should not be done on an office machine; copying should be done at a location the researcher does not normally use, such as an out-of-the-way copy site or a library. If people don't know where something was copied they cannot tie any copy to you.

Letters or other communications wrapped in tinfoil make it difficult for investigators to read the contents of the letter or enclosure without opening the envelope. Putting a tin-foil wrapped letter in an envelope and then putting the whole packet in a second envelope makes it more difficult to extract the letter clandestinely. This may be particularly important for letters addressed to a postal location that has been identified as being for information-providers. Keep in mind that

addresses suggested by media for whistleblowers may well be monitored to see what is coming in, and who sent it. Putting up a public address for purloined information is a flashing neon light that tells governments, "Watch me!"

While there are techniques that allow clandestine opening of letters to read the contents, that can usually be thwarted by thoroughly wrapping the item in tape. But that, too, is a broad hint that something important is inside.

Phone Issues

Remember that phone records are often used to link people!

Get, and use, burner phones for communication with key sources. What is a burner phone? In theory it is a phone that cannot be connected to a particular person. The key here is "in theory." Often, when setting up the burner phone, the user leaves clues – or outright pointers – to the person at the end of the line. Buying a burner phone, or the time on that phone, with a credit card, or linking it and the new phone's number to a phone number you already use, means the burner phone may burn you. Extreme care must be used in buying and setting up a burner phone if it will be used in dicey situations.

Burner phones are usually prepaid but their use generally requires some identity verification. As a result the entire set-up process becomes as tricky as scaling a 15,000 foot mountain without climbing gear. Cash transactions help when buying a burner phone, but stores that sell them generally have security cameras. Remember that facial recognition software will see right through most disguises. It is better to find somebody who doesn't know you and will never see you again to purchase the phone. Some buyers ask people on the street to buy and activate the phones, possibly for the price of a bottle or dinner. There are programs such as Spambox that forward e-mails and then wipe their systems clean. This is important when you need an untraceable e-mail for such things as signing on to a site or setting up a burn phone. Though not designed for this purpose it can be used as a work-around.

If you employ a burner phone, use it only for the research project and not for any other activity. When possible, provide risk-taking key information sources with their own burner phones and make certain they understand how and when to use it. And how and when not to use it! Use burner phones as sparingly as possible.

If you use a burner phone – or any cell phone for that matter – remove the battery whenever possible. This is particularly true when going to meet someone. Phones communicate with cell towers even when not in use. A phone may pinpoint your location even if you make no phone calls or supposedly turn the phone off. A contact's phone will also show where that person was if not disabled, potentially putting both of you in the same place at the same time.

If you have a phone or device that will not allow you to remove the battery, do not carry it to any meeting.

Since cell phones leave a permanent record of travels with nearby cell towers, putting it in a drawer at the office or asking a fellow researcher to carry it around while you go to a meeting with a source makes the situation more opaque to probers.

Keep in mind, too, that your phone can be turned on by people with sophisticated equipment and knowledge. Snoopers may know not only where you are, but they can also capture your conversation.

You may occasionally use a pay phone to call elsewhere – provided you can find one. But you must avoid leaving any traces of your use, including appearances on nearby surveillance cameras.

Make it a habit to try to spot security cameras both inside and on the street. Again, cameras provide an indelible record of where you are, who you may be with, and when. In theory, a clear security video could even be used to capture the conversation through lip reading.

Computer Security

The first rule of computer security is "protect your IP address," the address your computer has on the Internet. IP addresses are the digital equivalent of the physical address of your home or office. The IP address is where the various parts of the Internet send information. Protect your IP address as you would a Social Security number.

Before you even sign on to a computer you will encounter your first security stumbling block. In virtually every case, unless the computer was first set up with security in mind, it is leaking, seriously leaking, information about you that can be used by adversaries. That often includes your IP address,

Thinking about your research computer systems. That's right. Plural. Ideally you will have at least two systems. The ideal may be more rare than Kryptonite but it is worth talking about even if it is unlikely that most employers will provide a two-system setup. Some journalists who provide their own setup may be able to use a two-system approach, or maybe one day there will be a miracle and your medium's accountants will say "hey, that's not such a bad idea!"

One computer is the Research System and is the one used for going out to the world; the Production Computer never touches the Internet and is used to process data, store it, and write on. These two are connected by means of an Air Gap technique.

The Research System is the one used to access the Web, the one that will be used to conduct the actual research. It will have access to the Internet, but will be set up minimally, with security issues in mind. The Research computer setup should include:

- Commercial Internet access.
- Virus protection,
- Firewalls.

- End-to-End encryption.
- Password restrictions.
- Virtual Machine (VM) ware and other security software.
- Multiple web browsers such as Internet Explorer, Firefox, Chrome, Opera, (carefully selected add-ons) and Copernic Agent – free personal version at: http://www.copernic.com/en/products/agent/index.html.
- Disc Image plan.
- SOP to format the computer and reimage.
- Appropriate software to download various video and audio file types.
- Program to wipe the system clean after each use.

The Production Computer system setup – the second one – typically includes:

- Storage and indexing programs for research.
- Production programs to write reports and stories.
- Programs to read material airgapped from research computer – may have to be duplicates of many of those on the research unit.
- Virus protection.
- Password restrictions
- Secure data backup system.
- Program to wipe the system, and blank spaces, clean at the end of the day.

Note that the Production Computer is never linked to the Internet. That provides security against anyone hacking in and finding notes, drafts, or other sensitive information. The key is "air gapping" between the two computers. The Air Gap is a way of keeping information secret. An Air Gap uses two computers – one is on the Internet, the other is completely disconnected from the Internet. Information is moved from the computer on the Internet to one that is disconnected by burning a disk, using thumb drive etc.
The Research Computer is used to go out on the Internet and find material. That material is quickly – at least once each day if not more often – air gapped to the Production Computer, where it is stored and used to create stories, etc. The air gapped material is completely erased from the Research Computer after the air gap takes place. If anyone does hack into the Research Computer they will find no files of value or interest.

There is a workaround to the two-system setup when that is simply out of the question for monetary or other reasons. It's not nearly as secure as air-gapped systems, but it is usually a better alternative to working on system that is always connected to the Internet. In this setup the Research Computer is set up as mentioned above. After research is completed, any Internet cables are pulled or other links turned off. When all Internet links are severed, a hang-on hard drive with the programs and capabilities of the production machine described above is attached. All of the researched material is moved to the hang-on drive and worked on there. All production work is carried out on that hard drive. When the production work is finished the hard drive is disconnected and stored away from the computer, which may then be reattached to the Internet after it is thoroughly cleaned by a program such as CCleaner.

Sealing out Adversaries

Computer seals may be used to thwart anyone with physical access to a computer from compromising it or its contents. Seals – also called labels by some companies that sell them – are used to prevent anyone from opening the computer case or other equipment and installing such things as keyloggers that will record what is being done with the computer, or what is being stored on it. When properly installed the security seals show a code number; but if someone tries to remove the seal and open the case it changes in appearance to show that it has been tampered with. Security seals are not reusable; once affixed to a computer case they cannot be moved or removed without showing that tampering has occurred. They are commercially available through Internet stores.

Stop the Swap

Swap files are a potential threat if someone gains access to a user's computer – either physically or through on-line shenanigans.

Swap files are used to improve computer speed. When a computer system runs low on memory it will transfer information to the computer hard drive, using it for temporary random access memory. These transferred files, known as swap files, often contain bits and pieces of information that can be put together in ways the computer owner would not appreciate. Disable the swap file. Information is available on the Internet to explain how to do so with different computers, using different operating systems.

Safety Starts with Computer Settings

Make the Research Computer, in particular, as anonymous as possible. Let's go back to the point mentioned previously – it is now time to talk about computer set-up. That starts with the naming of the system when it first comes out of the box. Something like "John's Computer" – assuming John really isn't going to use the system – is a far better name for the system than "XYZMediaNewsroomUnit123." Have a professional install – and update – all operating system security updates and set secure browser options. Keep add-ons to a minimum as these often are insecure. Most add-on programs are not written by people who have security in mind; they have a "neat idea" and a smattering of coding knowledge. Remember that thoughtless computer settings and add-ons aid adversaries.

Encryption

Encryption is basic protection against thieves and snoopers. Encryption makes it ***harder*** for anyone to read what you wrote, have on your computer, or are sending or receiving from some source. Most modern encryption programs available in the United States are difficult to break; even government agencies have a difficult time with some encryption algorithms.

Visible encryption causes everyone who sees the message to wonder what is in it. Intelligence agencies, as a matter of policy, may retain all such messages indefinitely—hoping that eventually they will be able to break the site for and be able to decode in all the previous messages. That is tradecraft. When you send an obviously-encoded message it will attract civic

attention from many, particularly governments. They will be looking at your messaging. You are likely to have a file folder created about you in three-letter agencies and that folder will contain all messages that can be intercepted. In many cases even unencrypted messages that can be tied to you may be filed away.

Use Full Disk Encryption for the computer: This prevents anyone from taking, copying, or hacking into the hard drive and reading it. BitLocker, PGP, and TrueCrypt work on Windows machines. FileVault is available for Macs.

Use only End-to-End encryption for e-mails and Instant Messages. Try PGP for e-mails and OTR for instant messages. Sites have cropped up to make email communication safer. These include:

- ProtonMail: https://protonmail.com/
- Signal (Whisper Systems): https://whispersystems.org/
- Telegram: https://telegram.org/
- WhatsApp: https://www.whatsapp.com/

Use the encryption available in many programs for Voice Over Internet calls.

For general encryption, consider using Blowfish, Twofish, and Threefish algorithms. Almost any algorithm can be broken eventually, but these present difficult problems, even for many governments,

Somewhat along the same lines is a program that turns a short message into what appears to be spam, http://spammimic.com/.

PGP – Pretty Good Privacy for E-mail

No e-mail should leave your computer unencrypted. It's not that every e-mail you send is so sensitive it demands encryption; rather every e-mail shows your writing style, choice of vocabulary, and punctuation habits. That style is a marker. By gathering samples of your unique style and word-choice a determined and capable opponent with code-breaking capabilities can use the template of your unencrypted emails to help break your encrypted ones.

Encryption should be done on your computer, before the message ever goes out on the Internet where it can be seen by opponents. Decryption of messages is also safest when done offline. Messages should not be sent "somewhere else" on the Internet to be encrypted. The same rule applies for decryption. There are a number of useful programs that can be downloaded for on-site encryption/decryption, including mailenvelope. Enigmail's add-on works well with Thunderbird and Seamonkey. For all Windows systems a desktop application that is not linked to particular mail systems GPG4Win is usually adequate. This program is also useful for encrypting files. As with all systems and programs, there is a learning curve when using encryption. Proficiency comes with both study and use.

Some employers do not permit the downloading of apps or programs to a company system. This restriction creates the situation where encryption and decryption cannot be carried out on the user's computer. In that case, where circumstances and an employer force you to encrypt outside you own computer, programs like iGolder may be the option of choice.

The public key to the encrypted message must be furnished to the recipient of an encoded e-mail before the message can be read.

Because documents attached to an e-mail are not automatically encrypted in many cases attachments should be encrypted separately and sent with the email. The password to the encrypted document can be put in the carrier message and both can be encrypted at the same time.

PGP and GnuPG are widely-used e-mail encryption programs that have a history of successful use. They provide:

- Message security.
- Tamper protection.
- Identity verification.

Public Key Encryption

Public key encryption allows you and another person to set up a secret code key. More information is available by searching the term on the Internet.

Passwords and Pass Phrases

Passwords on your computer and at sites you visit are often your only safety feature. No matter where or when you "sign in," passwords are irritating and problematic to most people. You have heard the injunctions: change your passwords often, each site should have a different password, passwords should be at least eight (or 20) characters long; consisting of capital letters, small letters, numbers and signs; the password should never be written down; it should not be a recognizable word or words; it must be changed every six months, and the same one may not be used until there have been 10 iterations – yada, yada, yada.

The password rules have become so onerous that few people willingly follow all of them. In reality, passwords must be strong, but memorable. And, yes, each site should have a different password in case hackers make off with the site's password files – you don't want every site you use to become vulnerable because everything you do and every place you go is tied to a single, now compromised, password.

New studies suggest there is a better way, one not so complex or daunting that no one can possibly follow all the rules. Use a pass phrase or a pass code!

There are thousands of memorable phrases to choose from. Shakespeare or a favorite graphic novel may be the inspiration, but let's take a famous one from the start of WW II. The speech has this famous phrase: "a date which will live in infamy." That could become the pass phrase:

adatewhichwillliveininfamy. But is that really isn't secure enough. It can be cracked – perhaps not easily but it is vulnerable. So how about capitalizing the first letter (or last letter) of every word: ADateWhichWillLiveInInfamy? Or maybe every fifth letter: adatEwhicHwillLiveiNinfaMy. Or how about shortening it to the first (or last) letter of every word: adwwlii. Maybe we want to add some numbers and signs, but also capitalize every second letter aDwWlIi12071941! Or maybe you want to start, not with a phrase from a book, but a home or office address you used five years ago and a phone number from your childhood. The key is to make it possible to remember how to input the password. You know the phrase and how you altered it. You don't need to write it down. It's long and is not easily recognizable.

Or the password may be three or four unaffiliated words-globe1492TIMEsand. Consider using programs such as Diceware to create multi-word passcodes.

Password managers are useful in "remembering" your pass codes, but keep in mind that most sites where you are required to have to use a password or pass code also have a "forgotten password" link. A forgotten password may be upsetting, but it is usually not critical.

Password Managers

These are alternatives to a written list or memorization of long, random and complex passwords. To generate and employ such passwords, password manager programs were created. They generate passwords that are difficult to remember and hard to break. The sites will often fill in the unique password for you at sites you use. As useful as they are, however, keep in mind that you may be toast if you forget the master password to the Password Manager. Some key ones include:

- LastPass
- 1Password

Collection Methods Can Bite You….

Remember that collection methods might reveal critical information about you, your work or your interests. Such indicators may assist those seeking to neutralize your efforts. Purchasing documents or searching an Internet site are two examples of detectable research and collection techniques that could provide indicators of your interests. Using the same browser for your repeated Internet forays can be used to crack your anonymity. Having, and interchanging, several different browsers helps reduce the ability of opposition system operators to track you.

Profiling

Profiling or tracking puts together information stored on a computer – largely from cookies – in order to establish patterns of activity. The collection of the URLs of sites that were visited can be analyzed not only to show interests, but can potentially link with information that identifies you as the individual who visited the sites.

Cookies are small programs that are downloaded to Internet-capable devices by websites, applications, or platforms you access. Cookies are designed to tell the system operators about the device, and often about the browsing habits of the device user. They are frequently used as a recognition method so the website's operator can identify you.

There are different cookie "flavors," although any particular cookie may fall into more than one category.

First-party cookies come from a server or a domain managed by the website publisher.

Third-party cookies come from a server or domain other than the website publisher; this third party processes the collected information and may sell or use it for its own purposes.

When cookies are installed from a server or domain managed by the website publisher, but the information collected is managed by a third-party, they are not classed as first-party cookies.

Cookies are also classed by the length of time they remain active on the user's computer.

Session cookies sweep up and store data when the user accesses a website. They are usually used to store the data needed to provide whatever service is requested by the user and are active only for that single occasion.

Persistent cookies are stored on the device of the user. They can be accessed and managed over whatever period of time the emplacer of the cookie decides. The time can be short or the cookie could remain active for years.

There are a number of different roles for cookies.

Technical cookies allow the web user to effectively use the site. It focuses on technological needs of the site.

Personalization cookies allow users to access the service, personalizing it by matching the display to the requirements of the user's device.

Analytics cookies allow website operators to track and analyze the behavior of the users.

Advertising cookies control the advertising space that the publisher has included.

Behavioral advertising cookies store and use information about the user's activity by monitoring browsing habits and developing a profile based on those habits.

Cookies are neither good nor bad, it is the use that others put them to that determine that. Because they can be used to obtain, store, and use information about an investigator's or

researcher's on-line activity it is usually best to disallow cookies on your equipment. However, as with technical cookies, doing so might make a site totally or partially unusable to you. Cookie issues often need to be resolved at the time they arise. A major factor in any decision about cookies is whether the researcher believes the system operator who has access to your cookie information will use them against your interests.

It is a generally-wise practice to clean all cookies from your system after being on one site, before going to another site.

Digital Fingerprint, aka Footprint

You leave an information trail whenever you use the digital environment. It is commonly called a digital footprint, but is essentially a fingerprint. Many people can see and record that fingerprint. Who sees you (your IP) on the Internet?

- Administrators of websites you visit.
- Security Personnel at those websites.
- Internet Service Providers (ISPs) who can now sell information about your Web activities.
- Proxy sites used in the data transfer.

Records that can be, and often are, retained:

- Computer configuration (e.g. browser and settings, operating system, Internet Services).
- A profile of your interests, based on surfing habits.
- Detail of your pattern of searches and subjects of interest.

Your Online Persona

The online persona is your social identity, established in online communities and websites. It identifies where you appear to connect from and who you say you are when accessing sites/ It reveals:

- Type and version of your operating system and browser.
- Your Internet Service Provider name.
- E-mail verification.
- Your time zone and location.
- Your organizational affiliation.
- Cookies you have retained, which is one reason an investigative searcher clears the browser of cookies often.

The digital footprint and online persona, together, are used to identify you. Things most people would not imagine, including the time of day you come on-line to a site or the fonts selected on your browser, are used to create a profile that is can be matched to you. Profile builders also include such things as:

- Screen resolution.

- Metrics of Windows.
- Add-ons
- Extensions.
- Time zones.
- ISP.
- City.
- State.
- Country.

Internet Browsers Tell a Tale on You

Your browser is a tattle-tale and will tell website managers much of the information that goes into an online persona. This may include:

- IP Address.
- Sites visited today.
- Computer name (the one you want to show us as John's Computer).
- Browser type.
- Page referred from.
- Cookies.
- E-mail address.
- Etc.

See What the Other Side Can See

To see what the other side – including an adversary – may be able to see when you go to a site, try these:

- http://myipinfo.net/
- http://ipchicken.com
- http://www.ip-adress.com

Your Security Depends on Anonymity

Loss of Online Anonymity can compromise security. Think Risk Mitigation, not Risk Elimination

General Rules….

- Use two computers when possible: production and collection, and air-gap between them.
- When collecting, disable non-essential system or browser parts that record your activity.
- Use a masking program when possible to mask your affiliation.
- Use VMware to run a virtual machine, if available.
- Don't trust "privacy mode" alone.
- Be aware what your browser is disclosing about you.
- When possible, use cached copies of sites from search engines first.
- Link-shrinking is useful, but dangerous since it can easily be used for misdirection,

- Beware of referring URLs, which may actually be designed to misdirect. Copy URLs into new windows.
- Vary the visits to different times of day.
- Act casual!

Take all safety and security precautions; develop safe online habits

Safe Online Habits

- Be discrete, not deceptive.
- Do not use a personal home computer for research.
- Search the safest resources first; if you can find the information you need there you will not need to go to adversarial sights.
- Use strong passwords.
- Use a "No Name" operating system ("New User")
- Regularly update browsers and software.
- Limit time on high-risk sites.
- Consistently and constantly run virus scan.
- Clear the history often, sometimes after each site visit.
- Adjust Internet options and browser preferences to their safest ones.
- Do not click on titles of your search results, type the URL into the browser box.
- Avoid opening shortened URLs.
- In browsers that allow it, select "Private Browsing."
- Keep all connection details as anonymous as possible and set up PC as minimally as possible; avoid add-ons.
- Always refer questions to security professionals.
- Properly dispose of documents and media.

Key Techniques on Websites

Maintain enhanced security posture when on a website:

- Save the entire page or the site to avoid return visits and cut the time-on-site.
- Save the page and review later.
- Save site with Offline Browser.
- Use the PDFmyURL site.
- Clear the clipboard or ensure no critical information is there.
- Vary your movements on the site so that you appear to be browsing rather than looking for specific information.
- Avoid using a website's search box; this can provide information about you and your interests to the site management.

There are a number of techniques and resources that are usable in masking your identity. Select the ones to use in a particular case, based on the threat facing you. Remember, too, that mixing

up your techniques helps your security. Avoid being stuck on a single method, no matter how comfortable that may feel.

Some Search Engine Techniques

Minimize the collection of data profiles by search engine operators. For major search engines:

- Google go to http://google.com/history . Then log into your Google account. You should see your history. To remove it, click the icon that looks like a gear at the upper right of the page. Click "Settings" and turn off turn off search history. Delete your history from the database.
- Bing use https://www.bing.com/profile/history to turn off and eliminate your search history.
- Yahoo will not let you delete the search history they hold on you, but you can stop them from collecting search history materials in the future at http://search.yahoo.com/preferences/

- **Use privacy aware search engines to minimize your footprint**
  - DuckDuckGo, https://duckduckgo.com,
  - PrivateLee, https://privatelee.com;
  - Qrobe.it, https://qrobe.it
  - IxQuick,. https://www.ixquick.com
- **Another possibility – particularly if you want to use one of the larger search engines that do collect information** – is to use Disconnect Search at https://disconnect.me/search Disconnect Search searches major sites without leaving your search history or sharing your I.P. address. Chrome or Firefox users may want to consider a downloadable Disconnect Search browser plug-in.

Use an Anonymizer or Proxy

Anonymizers and proxies eliminate much, but not all, information about you. They may show you as originating from a location other than your true location. Remember, they often show that you are using an anonymizer, which is a tipoff and in some cases may prompt the site operator to bar you from the site.

These are intermediate server(s) that change the IP address. They may involve a single proxy server or several may be strung together. While proxy servers will change the IP address they leave, your clipboard, login information, and browsing history may still be revealed unless you eliminate those records from your search computer.

VPNs

VPNs –virtual private networks—send a different IP address to destination sites, much as Tor does. They hide your address behind their own. VPNs provide privacy but they do not provide anonymity. The VPN operator knows the user's IP address; after all, they need to forward the information to the user wants. Many VPNs will provide user information to governments. There

is no evidence whether some VPNs would surrender user information to non-governmental groups such as the Mafia, if given a reason they cannot refuse. VPNs are wonderful for privacy, but they do not provide anonymity. Still, particularly when used with Tor, they can be used to enhance security. VPNs usually cost money. They include:

- Anonymizer Universal.
- Giga News.
- Ironsocket.
- NordVPN.
- Express VPN.
- ProXPN.
- PureVPN.
- Ipredator.
- HideMyAss.
- Strong VPN.
- WiTopia.

Tor is Widely Used

Tor, also known as Onion, sites cannot be reached through the regular open web. Sites are like top level domains (TLDs) on Tor but can only be accessed through Tor's network. While using Onion sites it is well to remember that they were developed to protect the site administrators and owners, not the people browsing a site. Nonetheless they have proved highly useful for researchers, journalists, and information sources in some of the most restrictive and dangerous countries anywhere on the planet.

When using Tor it is always wise to test to see what IP address you appear to be coming from. Web sites such as whatismyipaddress.com and other websites listed earlier will show where you are ostensibly coming from.

TOR is not always easy to use to its most effective limits, but it is considered the best way of hiding who you are and where you are located. Information can be found at https://www.torproject.org/about/overview. A Firefox version called "Tor Browser Bundle" provides special resources and these are useful to media reporters.

Tor is a series of nodes which a search or message passes through – it is similar to a VPN in that respect. But the system is designed so that no relay node has the IP address of both the sender and recipients. Tor's "jumps" or "hops" from one node to another slow the transmission somewhat.

All programs and services are not compatible with Tor. Don't use P2P programs with Tor and expect to remain anonymous. Javascript is also an anonymity-breaker. BitTorrent isn't effective on Tor.

Use Tor when you want anonymity. Don't mix anonymity with activities that require you to be identified. Avoid giving out personal or compromising information while on Tor – this includes such mundane things as bank information or social media sign-ons. These are purposely designed to identify the user and defeat the purposes of Tor. E-mail over your ISP, even with Tor, may defeat the anonymity. Use Tor to access sensitive e-mail only when you are using secure e-mail sites. Avoid using the same browser for TOR that you use for your regular ISP searches. Adversaries can correlate information from cookies. For maximum safety employ the Tor browser bundle and the Tor Bridge Relay.

Other resources include:

- Tails secure operating system.
- SecureDrop.

Tails

This is a separate communications operating system for the computer. When the communication is completed, the operating system disappears from the computer and with it all evidence of the communications. Download to a thumb drive or burn a disk and use it from that location. The program is available at https://tails.boum.org/.

Tor Hidden Services

Tor Hidden Services make the website browsing even more difficult to trace. Addresses seen by sites managers will indicate to the manager that you are striving for anonymity. All interactions stay within Tor; DuckDuckGo is used as a search engine, which may limit the available resources.

Yet Another Security Measure…

The site http://pdfmyurl.com/ will create a pdf of the page you visit. The sysop of the site that is visited sees the address that pdfmyurl uses rather than your own address – and you get an exact copy of the page as it existed at the time it was visited. Note there is a downside: This site cannot pdf a pdf, and saved links will not work.

And Another One…

Use an "offline browser" This can collect and download an entire site in a matter of minutes. An offline browser limits the time you are on the site and allows you to look at the materials on the site at any time, without being connected to the Internet. Find offline browsers by searching them online. We use HTTrack Website Copier at https://www.httrack.com/

Instant Messaging

OTR employs an instant messaging program, encrypting the text exchanged by two people. Metadata of the chat may still allow others to see who is involved in the chat. For maximum security do not use an existing account linked with your name. For Windows and Linux, use Pidgin plus the OTR plugin on Google Talk, MSN or Yahoo Messenger. Alternatively use a Jabber/XMPP account over a provider http://www.jabber.org/

Voice over the Internet and Cells

Encrypted voice calls are safer. Ostel is usable on computers, Blackberry units, Android phones, iOS, and Blackberry units. RedPhone can be used on Android phones. Silent Circle is a multi-platform program, but is not free.

Lightweight Portable Security

LPS is a separate operating system for PCs and Macs that boots a thin Linux operating system from a CD or USB flash drive. Administrator privileges are not required. Nothing is installed on the computer. When the communication is completed, the LPS operating system disappears and with it all evidence of the search or communications. Download to a thumb drive or burn a disk and use it from that location. The program is available at http://spi.dod.mil .

Encryption

Encryption is Basic Protection against thieves and snoopers. Encryption makes it **harder** for anyone to read what you wrote, have on your computer, or are sending or receiving from some source. Most modern encryption programs available in the United States are difficult even for government agencies to break.

Use Full Disk Encryption for the computer: Prevents anyone from taking, copying, or hacking into the hard drive and reading it. Try BitLocker, PGP, or TrueCrypt for Windows machines or FileVault for Macs. Use only End-to-End encryption for e-mails and Instant Messages. Consider PGP for e-mail; you may want to try OTR for instant messages. Use the encryption available in many programs for Voice over Internet calls.

For general encryption, consider Blowfish, Twofish, and Threefish algorithms.

Firewalls are More-Than-Useful….

Firewalls are a must. There are many. Some are Review your choices on the Web, or by contacting your local computer guru. Popular ones include ZoneAlarm at http://www.zonealarm.com, Tiny Firewall at http://www.tinysoftware.com, and Sygate Personal Firewall at http://smb.sygate.com/products/spf_standard.htm.

Wireless Hotspots

They are prone to betray you and information about you. Avoid them at all costs.

Countermeasures Redux

Use multiple search engines and switch browsers often, after clearing your history. Proper browser configuration is important. Do not overlook that. Use obscuring search procedures and practice safe online habits. Check among your digital gurus for the best anti-virus software. Big advertising budgets and name recognition do not make you safer. Insist on the best. Anonymous Surfing Tools/Virtual Private Networks can be researched online. And if you use VPNs or Tor keep your publicly-known personal identity separate from any anonymous identity.

Sockpuppets – Alternate Identities

Sockpuppets are alternative – some would say fake – identities used on the Internet. They may be as simple as calling yourself "John Smith" on a Social Media site or as complex as creating an entirely new "life" on the Internet.

Sockpuppets are not identity theft. Legal sockpuppets are not based on a real person; they are, however, "whole cloth."

If you are allowed multiple personas – and many positions prevent that – you should develop as many as needed, plus a reserve, and change them when required. You can and probably should write down the details of different personas, refreshing your memory as you go online with any alternate identity. Try not to adopt the persona like an actor. Use an alternative persona as if it is real. Live the role when using a sockpuppet.

Sockpuppets are neither good nor bad. There are often good reasons for using a sockpuppet, just as there are bad ones. The bad reasons seem to predominate, however. One well-known television program specializes in proving that some on-line identities – sockpuppets – are fake.

Many government agencies do not allow their employees to create or use sockpuppets. Private employers, particularly in the media, frown – with great frowning – upon sockpuppet use by staff members. Many on-line sites prohibit sockpuppets under their terms of use. Keep in mind that using a sockpuppet may put a user in legal or employment jeopardy.

Nevertheless, if you spend much time on the Internet, particularly if you spend much time in Social Media, you are likely to encounter sockpuppets. Being able to identify a sockpuppet – and understand the reliability of that fake's message – is also important to the analysis for reliability. Whether you use one or not, a secure researcher must understand how sockpuppets are developed and used.

When developing a sockpuppet some researchers use a fake name generator on the Internet. These are easy to find, using that term in a search engine. Some provide additional life "details" along with the name.

The best sockpuppets tend to be reliably consistent – perhaps using a notebook that contains the elements of the "legend." An ability to refer back to the sockpuppet's "legend" prevents many mistakes. Most good sockpuppets try to stay as close to the truth, some element of the truth about themselves, as possible. The legend usually connects to some part of the effective sockpuppet user in some way. Skill sets depicted are usually those of the sockpuppet creators or those around them. This is necessary to create a feeling of "naturalness." Because people are sharp-eyed, deviations from past statements or even probabilities of differences are immediately seen. Particularly over a long term – where there are many data points – legends are often revealed for the fake they are.

Using a notebook that outlines the elements of a particular sockpuppet is almost required when the user creates more than one. It is too easy to confuse the attributes of one personality with those of another fakement. Having a string of fake identities is often a good idea in case one is outed – and that happens often.

Female sockpuppets tend to receive less scrutiny than male ones, but many males have a difficult time slipping into a female persona. Those who can do so, however, have a good success rate.

Many sockpuppets use E-mail addresses from "free" sites and that is one element to consider in analyzing for a sockpuppet. A working E-mail address from something other than a free webmail site provides good "cover" for a sockpuppet. While E-mail addresses from free webmail sites are not determinative of a sockpuppet, they are a datapoint that prompts many to delve further into the real identity of someone on the Internet.

Good sockpuppets have a home that they can describe inside and out, room to room, driveway to backyard fence. These description are often taken from real estate sites or photo-mapping sites, or both, allowing sockpuppets to describe the neighborhoods almost as well as a resident.

Sockpuppet users may claim to be from anywhere – but anyone who claims to be from or in a location that is not their own has some formidable steps to climb in making their artificial world seem reasonable. The sockpuppet user must digitally "live" in their claimed location. Employment, social happenings, news of local events, holidays and vacations, even the prevailing sense of humor may have to be displayed through the sockpuppet.

Religious, ideological and political affiliations need to be brought up over time. An "Internet person" lacking such links stand out as cardboard people. To a great extent that sockpuppet character needs a back story – without that they were "born yesterday." And an effective sockpuppet must have a future, a story that includes hopes, dreams and prospects. A long-term sockpuppet needs friends and enemies – the same types of interactions that everyone experiences every day. Are the conflicts passive or active – things like this and person's passions are found in good sockpuppets. They are missing from the poorer ones.

Timing of messages and Internet availability is crucial. Every person or sockpuppet has a way of making a living and hours and days must be set aside for that. If a sockpuppet's messages appear during work hours at the location specified in the legend, the sockpuppet must have a good explanation for that discrepancy. Somewhere along the line work will come up – everything from travel to and from work to events and bosses there.

The truly good sockpuppet will have dimensionality; the not-so-good one will lack emotions or will have a cardboard personality.

Well-crafted sockpuppets that socialize reveal, in some ways, why they want to interact with others. Their messages will display mood swings, highs and lows. Habits will become apparent in the best ones, even some commentary on diet and drinks will appear. Details like that may be a chance to unmask the sockpuppet. One of the most important spies in World War II claimed to be drinking wine with shipyard workers in England – but the clue that he was making up the whole story was missed and he went on to create an entire circle of informants who never existed, a pre-computer sockpuppet circle that was instrumental in misinforming the Nazi war machine about the timing and location of the invasion of Europe.

Better sockpuppets often do a lot of "liking" of other people's posts on Social Media as this tends to create a sense of community and often results in getting "likes" in return. That, in turn, affirms that the sockpuppet is a person.

Some subjects – weather, local events, and unusual natural or political events – will appear in a good long-term sock puppet but will be missing from the writings of a cardboard "person.

The lack of any picture is often a telltale sign that a Social Media site or connection is actually a sockpuppet. Even a picture of a pet, a car, or other abstraction seems to work almost as well as a portrait picture in "proving" any Internet profile is legitimate. While there are many people pictures on the Internet that could be used to authenticate a sockpuppet, one of the first steps in unraveling a false identity is finding where the sockpuppet's picture was stolen from. For that reason photos or pictures used for a sockpuppet should never have appeared on the Internet.

Cultural differences, even down to language and slang used in the area the sockpuppet is reportedly from, will be reflected in the better-crafted ones. Every bit as important as displaying the correct cultural norms is the adoption of subcultural behaviors and language. A lack of knowledge about group thinking, behavior, and terminology can be a clue to a sockpuppet.

Don't Just Hit the Delete Button…

Deleting a computer file is a misnomer. "Deleting" does not remove an item from the computer or thumb drive; it merely changes the resource's name so that it no longer appears on the computer's index. The name change also allows the space the file occupied to be overwritten sometime in the future. Hum-drum files and the most sensitive ones are not destroyed until the space they occupy on the hard drive is overwritten. Items only "deleted" can be readily found and read forensically. Until the space is completely overwritten, what was there can be discerned by a competent computer user with a minimum of forensics training. The original material remains and is accessible to a hacker who has broken into your machine or otherwise has access to the computer or a copy of it. Some programs, such as CCleaner, will overwrite that area three times with 1's and 0's, wiping the free space. Normally a three-pass wipe is considered secure. Security-smart users first clean their computer of temporary files and delete unneeded ones. Then they run a program like CCleaner to make all traces of deleted files disappear. Users will not be shocked that the overwrite process takes some time and is far from instantaneous.

The Step No one Wants to Take…

Publications, stations, and networks, often endanger their journalists – and some journalists wouldn't have it any other way. By-lines and on-air appearances by journalists often point directly to one half of the informant-reporter team. To prevent, or at least delay, identification of the person or people in contact with the sources and the ones who did the investigative work, a generic by-line such as "by an investigative reporter" or the use of a spokesperson who was not involved in the investigative work makes sense. Loss of a by-line or television exposure is important, of course, but not as important as a loss of freedom or even the loss of a reporter's or sources' life. Many news sites in high-threat countries such as Mexico or Syria have phased out bylines to prevent antagonists from identifying reporters, and through them the sources.

Learn the Tradecraft…

- CIMA Journalist Security Tools: http://www.cima.ned.org/wp-content/uploads/2016/03/CIMA-Journalist-Digital-Tools-03-01-15.pdf

- Committee to Protect Journalists: https://cpj.org/security/
- Committee to Protect Journalists Security Guide: https://www.cpj.org/reports/2012/04/journalist-security-guide.php
- Committee to Protect Journalists Resources and Manuals: https://www.cpj.org/reports/2012/04/journalism-resources-and-manuals.php
- Digital Self-Defense for Journalists:https://source.opennews.org/articles/digital-self-defense-journalists-introduction/
- Electronic Freedom Foundation Security for Journalists: https://ssd.eff.org/en/playlist/journalism-student#playlist
- Electronic Freedom Foundation "Surveillance Self Defense" Guide https://ssd.eff.org/en
- Freedom of the Press Foundation "Encryption Works" guide at
- Electronic Privacy Information Center: https://epic.org/
- Global Journalist Security: https://www.journalistsecurity.net/
- Global Journalist Security on Facebook: https://www.facebook.com/safejournalism/
- IJNet Eight Free Safety Manuals: http://ijnet.org/en/blog/tips-ukrainian-reporters-covering-conflict-plus-eight-free-safety-manuals-journalists
- IJNet Safety Toolkit: https://ijnet-journalism-safety.silk.co/
- Information Security for Journalists -- the Centre for Investigative Journalism: http://www.tcij.org/resources/handbooks/infosec
- International Consortium of Investigative Journalists: https://www.icij.org/
- Journalist's Resource Security Tips: https://journalistsresource.org/tip-sheets/reporting/digital-security-tips-protecting-sources-journalist
- Krebs on Security: https://krebsonsecurity.com/
- Media Associations on Global Journalist Security: https://www.openschoolofjournalism.com/resources/media-associations/global-journalist-security
- OSINT & Digital Privacy Forum: https://inteltechniques.com/forum/viewforum.php?id=8
- Project Eavesdrop-Episode 548:: http://www.npr.org/sections/money/2016/07/29/487970769/episode-548-project-eavesdrop
- Reporters Without Borders Online Security: https://rsf.org/en/online-survival-kit
- Security-in-a-Box page at https://securityinabox.org/en

VPNs and Other Services

- Anonymizer Universal: https://www.anonymizer.com/?gclid=CIO_1aqA7tMCFVFffgodQpYP9w
- Freedom VPN: https://campaigns.f-secure.com/freedome/sem/en_US/ls/?ecid=6617&pcid=6617&gclid=CLHPtc-p_NICFVecNwodOFIA3w&gclsrc=ds
- Private Internet Access: https://www.privateinternetaccess.com/
- Tor Browser (Onion Router) https://www.torproject.org/download/download

- Tunnel Bear: https://www.tunnelbear.com/

Concealment Annex

There are innumerable places to conceal material. The list below is from a basic United States government training program that shows would-be searchers key places to look. That is not to suggest that these places, if used to hide notes, would be discovered. Rather it shows the wide diversity of locations where contraband has been hidden, and well-trained investigators have found it. Inventiveness and out-of-the-box thinking are useful in keeping notes, information or other items safe. The only safe assumption the reporter can make is that anyone and everyone, including fellow journalists, may try to find out what you know and from where you got the information. Assume fellow journalists are as dangerous to you and your sources as the people who you are investigating.

One additional tip may be useful, when trying to hide real notes on something like a thumb drive put one of two in a "hiding place" where intent searchers are likely to find it. Material on the thumb drive should be innocuous and perhaps encrypted with a password that you are willing to give up, eventually, on demand. Searchers tend to relax their work once they think they have found what they are looking for; the item in the dummy hiding place may protect the real hidden notes or materials.

Homes, buildings and luggage items
telephone base and handle sealed cigarette package
inside and under wigs
under washbowl, sink or tub
base of lamp
closet clothing-waistbands, pens in pockets, sleeves, hatbands, shoes, gloves
flowerpots and window boxes
wall and ceiling light fixtures
prescription bottles
mattresses
behind picture frames, posters, or mirrors
flashlights
removable air conditioning registers
pet box
light switches
behind baseboards
inside hollow doors (removable top)
under carpets
inside hollow curtain rods and closet rods, shower curtain rods
inside stairway pokes

inside door chimes and doorbell
inside deep-well fryers
range hoods and filters
rolled up window shades
mailbox
inside knife handles
behind wall phones
inside transistor radio
hanging out window
sink traps
dog collars
refrigerator: underneath fruits, is vegetables, meat; taped under door, motor compartment
furniture upholstery
inside toilet tanks
magazines and books
bedposts
musical instruments and cases
false bottom on radiator covers
all kitchen canisters and containers
doorknobs
behind walls
hung behind curtains
inside TV and radio sets
inside false ceilings and chimneys
plumbing inspection doors
inside crucifix
golf bags
test tubes
inside cameras
taped to the top of toilet bowl
window ledge next door
in floor drain
false aerosol cans
florescent light tubes
toys and stuffed animals and games
in bandage boxes
top of window, door sills, moldings,
fire and water hoses
seller beams
Venetian blinds – top and bottom
inside clocks
child bank
agitator of washer
chandelier

inside trophies
inside rolled-up newspaper
electrical socket
stick deodorant containers
cold cream and petroleum jelly jars
taped in dressers and behind drawers
inside ceramic and clay figurines
inside candlestick holders
inside handle of carpenters toolbox
team to movable clotheslines
inside pipe racks stand
behind exterior brick near window
rifle barrel but played
inside rifle cartridge and shotgun shell
inside tinfoil to being ruled
zippered cushions and pillows
under panel of parquet floor
inside toilet bowl float
fuse box
fish tanks and bowls
hollow soap cakes
top edge of doors
hollowed-out furniture legs
salt-and-pepper shakers
hollowed fruits and vegetables
record albums
spice jars
wax paper dispensers
magnet boxes
fire alarm bell
false-bottom baby carriage and cribs
douche bags
dog houses
footlockers
35 MM film cans
within sanitary napkins and the inbox
rain gutters and rain spouts
hot-air ducts
hem of drapes and curtains
in the inbox of mattress frame
hollowed-out tree
shoe polish container and equipment
razor blade dispenser
stovepipes

garbage bags
pillowcases
furnace
seams of field cots and hollow cap of cot legs
attic insulation
inside hassock
hidden drawers in tables
inside TV to
inside color TV antenna
inside abandoned plumbing
in toolbox
inside letters
inside and behind vacuum cleaner bags
inside handle of vacuum cleaners
inside room dividers
inside patch-trap of antique rifle
inside Christmas tree decorations
behind kick plates of sink cabinets
conduit from fuse box
jewelry box
close hamper
in stove insulation and stove exhausts and drip pans
under lip ring of plastic trash cans
in toothpaste tubes
in surfboards
in electric toothbrush holders
talcum and cold cream containers
teabags
acoustical tile ceiling
holy Bible (hollow cover)
baked bread, cookies, and brownies
cookies and candy bars
art kits
dolls new line
fuel-oil heaters
psychedelic light housing
hollowed out flashlight batteries
hollowed-out pad of paper
seltzer antacid
base of rabbit ears antenna
in eggs
mixed with tobacco
taped to hat boxes
leg of bathtub

toaster tray
plastic rolling pin
razor blade disposal slot
shower head nozzle
chimney clean-out
hair dryer
clock
hollow cane new
pay telephone coin return
under corner of mailbox
shaving brush handle
miniature chess boards
behind and inside medicine cabinets
in closeline pipe
ironing board legs
bottom half of double boiler
typewriters, computers, and covers

Automobiles and Vehicles
dome, headlights, and taillights
hubcaps
inside horn
air filter
oil filter
spare tire – treads and well
windshield washer fluid container
shift knobs
instrument panel and ornamental objects on dashboard
cars with double sunroofs
ashtrays, in and under
picnic jug in trunk
false battery
under brake and gas pedals
frame
license plate
false heater hoses, heater
sun visors
under rugs
upholstery
behind bumpers
false dual muffler
hollow voltage regulator
heater
dance (air and heater)

radio speaker grill
on top of gas tank (suspended or concealed in compartment)
glove compartments – top of compartment or trap
convertible tops
false bottom of trunk beds
fuse box
backseat
floorboard
trunk
inside oil cap
Hide-a-key
Under seats
Cigarette lighter
carburetor
pill vials
Under tire air-valve caps
inside motorcycle handlebar tubing
Compartment under floor of older Volkswagen cars
inside tubing on roof rack
inside auto surfboard racks
motorcycle taillights
rocker panels
Tailpipe
insulation under hood
taxicab roof light
under chrome
key case
taped to the window
service station travel kits
false radios, stereos, CD players
armrest
inside flashlight
tied to axle

On Person
lipstick tube
cigarette lighter and packs
taped under Breast or brassieres
processed hair, hair buns, and wigs
rectum
vagina
nose
ears
mouth

cheeks of buttocks
lapel of jackets and coats
inside and back of watch and other jewelry
taped behind ears
cuffs and waistbands
pockets
shoes and socks
pill vials
inside sanitary napkins or tampons
hat band
film cans
baby's diapers
corsets
under false teeth
slit belts or zippered belts
belt buckles
behind collars and collard stays
foreskin of penis
under bandages
false limbs
glass eyes
hearing aid glasses
jock straps
swallowed, with string to teeth
between toes and taped to feet
tie knot of necktie, handkerchiefs
wallet
eyeglass case
contact lens case
inside pens and pencils
tobacco tins or pouches
money belts
lining of clothing
hollow end of cane or umbrella handle
in gum sticks
cigarette filters
compact
casts
in addressed envelopes
false buttons
in male girdle
in swim trunks
in stem of pipe
in gum stuck behind the ear

pinned to shorts
inside identification bracelets
inside feces bag
inside hollowed-out crutches
inside next and wrist lockets, bracelets, and charms
rings
earrings
tie pins, clasps, and cufflinks
fountain pens and pen barrels
inside fly flap of trousers
hearing aid battery box
thermos jug
liners of baggage
canteens
inhalers
lining of change purse
under insulation in motorcycle helmet
military insignia, lapel, and shoulder patches

--30--