Digital Information Security:

Explaining the Two Main Issues & How To Deal With Them

While the current political climate in the US is spawning mass interest in digital security, the situation as it stands has been created over the last 20 years or so, with concern and activism around the issue rising with the tide of technologies that are fueling the problems.

Here are the two types of security issues I want you to understand, and below are a few top-level actions you can consider taking.

> *Issue one:* Protecting identity info, whereabouts, and sensitive text (credit card #s, SSNs) in your email or browser from malicious intent, surveillance, or censorship.
>
> *Issue two:* Lessening the motherload of trace information that's collected about each digital user to reduce the consumer identity data which companies sell, and which can be misused both intentionally and unintentionally.

What's so dangerous about digital?

The most nefarious dangers generate from lack of expectation or awareness of the possible risks or outcomes of your actions. Many of us lock our houses because we expect that someone might try to enter our home. Many of us lock our email accounts with passwords.

But, the information we share, by emailing (at all), using public wifi, creating search records from our internet, all is essentially open to folks who know how to look at the networks we use to transfer that information. So, whether you just don't want your credit card info or identity stolen, or don't want a government to interfere with your movement work, digital network *use* is a risk.

Furthermore, many of us do not -- and can not -- lock the information we share digitally or via phones. It's this ambient data that can be used to keep tabs on us, develop digital traces used to describe us, and deliver segmented ads and media, creating an echo chamber of our "persona interests".

Worse, advances in data processing technologies lead one data scientist to refer to uses of the information collected from and about each of us digitally as a "weapons of math destruction," capable of *generating* inequality. Many others agree.

What is Digital Information Security?

Like any kind of security, it’s *being aware of the risks around you and responding to those with your actions*. Every organization, and person, will have a different set of risks, and so a different set of reasonable actions to secure your digital information to your satisfaction.

As digital security expert Rose Regina described, this assessment is called Threat Modeling, and it’s a process that you return to rather than a “one thing” you can do once. You make a mental model of what you think is happening so you can respond. Each of us already knows how to take stock of the possible risks around us: go back to the example of locking your house. What else do you do to secure your home? Has that ever changed depending on where you live? When you travel?

Digital Information Security is something you start on, work on, and do your best with. You can’t be 100% secure 100% of the time. But you can be MORE secure & private in your digital communications and more aware of the digital trace you leave, so as to be more in control of it.

What Can I Do?

PERSONAL: Some First Steps

Comms are only as safe as the person you’re communicating with. If that person is, say, Twitter, or someone who forwards (or releases) emails or messages to the FBI, then they’re not secure at all. Trust is part of security.

1. Issue One: Personal data

    - Please, please, please NEVER EMAIL PASSWORDS or SSNs. Think of email like a postcard: possibly read by anyone who it breezes by.
    - **Only use “https” sites** if you’re entering sensitive info →
      https://
        - Try using the HTTPS everywhere plugin to encrypt everything you type
    - **Trust no public wifi!** Sorry but the way networks work, it’s not terribly hard to get onto a network and capture the information sent through it. Or, put another way, expect any wifi you are on that’s not known to you to be trustworthy to be potentially tracking everything you type and do. #sucksIknow
    - **Check if your email address and password has been part of any data breach (**MySpace, LinkedIn, Dropbox, Tumblr) at https://haveibeenpwned.com/ *and change your damn passwords* if it has!

- **Trust no random USB.** People put nasty scripts on those things.
- **Set up a VPN** (virtual private network, more on what those are here), which will encrypt and anonymize your internet doings. Try:
  - Lantern or Viking VPN (no connections associated with names, creates random traffic, no logging) or MulleVad (sweden)

- **Don't click random links in emails you didn't expect to get and then submit your login info** (or worse, identity info) because that is a scam

- As always, **if something is free: you are the product.** You, and/or the information you share to get that free thing. *I'm looking at you Mint.com...*
- *Many more resources below...*

2. Issue Two: Trace Data

   Always ask: what info is this company collecting on me, and what is it connecting to? What is it saving and why? What websites am I visting? What's trackable? Learn more from Tactical Tech on your Digital Trace.

   - **NO LOCATION.** Deny! Turn off! Do not allow! Sharing your location is basically saying "yeah please send me ads about a nearby ______ and assign me to affinity groups nearby. Please put me on a location-specific list of people like me that you can find and contact easily." Eek!

   - Try to **avoid using social media profiles to log into other sites.**
     - #1 you're avoiding lulling yourself into accidentally giving your fb password away in a scam window someday and
     - #2 when you do this, you're creating the data profile for the company, connecting even more of your interests & habits. Why give them this?

   - **Allow access to random app? Nope.** Think twice before you click yes. Do you really want to share alllll your data/phone records with something unknown you'll use once?

   - *Many more resources below...*

ORGANIZATIONAL: Some First Steps

If you'd keep your personal info safe, I'm guessing you'd do the same for people you work with, right? *Especially* if those people are your clients/friends? And ***extra especially*** if these folks are at all marginalized populations on whom you collect information identifying them as such?

1. Issue One: Personal data
    - Someone at your org should be thinking about information security, and everyone should be thinking about privacy.

    - Please, please, please **STILL NEVER EMAIL PASSWORDS OR SSNs.** Someone downloads it on their phone on a compromised public wifi? *Whoops*.

    - Also, **don't email spreadsheets as attachments.** Why? Because if your email is intercepted in transmission or delivery, you've compromised all the information in the spreadsheet. A registration form? Eek. A link to a private google sheet or dropbox file is as trustworthy as the companies who host them, so probably ok unless a sapina comes out.

2. Issue Two: Trace Data
    - Many of us need to have social profiles for work-related purposes. Check out the privacy settings on your profiles and lock down where you can.

    - **About the cloud: DUBIOUS.** Who owns that cloud? What are they doing with the information you put in that cloud? Do you trust them not to compile and sell your data? Do you trust their security? Do you even need your information in their cloud? Can you download your data? What if they start charging 3x the rate?

I Have the f*&#--its and I Don't Want To Do Any Of This
People sometimes skip digital security because it can seem overwhelming, or because there's freaky words like "threat" "vulnerability" and "defense" all over it. While I don't want to alarm you, I do want you to know there's a reason it's described like this.

Sometimes a sense of incompletion exhaustion takes over, "well, it's too late anyway who cares?" approach. Anything you do, or any precaution you take resulting in a thing you don't do, will improve your overall digital security. Literally every keystroke or click matters, even one.

Final thought: Look, the most vulnerable thing is you! Convenience is your enemy!

Go Forth!

While this topic deserves more depth than I have given it here, there are currently MANY resources being developed for all kinds of users to understand and implement improved digital security.

READ MORE HOW-TOs
Tactical Tech's My Shadow Curriculum & Training Materials (A++)

Hackblossom's DIY Guide to Feminist Cybersecurity (A++)
EFF's Guide to Security for LGBTQ Youth (A)
EFF's Surveillance Self Defense Kits (A -- a little dense, but I believe in you)

READ MORE SMART LISTS BY SECURITY NERDS

Digital Security training resources for security trainers, Winter 2016 Edition
A 70-Day Web Security Action Plan for Artists and Activists Under Siege

DO MORE

- Get a password manager // Use Little Snitch if you have a Mac to see what's going out // Have a backup (or 2) of your computer // Encrypt your computer