MAKING A MAP OF YOUR DIGITAL UNIVERSE

Cybersecurity can feel like an overwhelming and scary topic. In the face of a constant onslaught of data breaches at large companies, it may seem naïve for us mere individuals to think there is anything we can do to effectively protect our identity and our data in cyberspace. If you dare to read up on the topic, you will find a hodge podge of "how to" articles whose details are out of date, and checklists of best practice guidelines that range from implausible ("memorize a freshly random 15-character password for each website you visit") to contradictory ("use a password manager … and never create a single point of failure").

Checklists can be helpful in settings where evolution is slow or infrequent, or when a small number of steps will have a large impact. But in cybersecurity, technology is evolving rapidly, and there are few individual recommendations that stand the test of time. But as in nearly every discipline that appears complex at first, there are underlying core concepts which are flexible, powerful, and long-lasting.

Learning concepts takes time. And effort. And focus beyond the level of reading a tweet or a bullet point. And your time is valuable! There are so many areas and skills you could choose to learn. Why chose cybersecurity? You might think it's the kind of thing best left to experts, and the time it would take you to improve could be put to better use.

But most skills can be broken down into digestible pieces, and often there is great value in mastering a few small pieces, even if you don't make it all the way to the end. It is easy for us to underappreciate this. Why learn to play an instrument if you aren't going to be a professional musician? Why learn to speak a bit of a foreign language if you aren't going to be fluent? But still we do these kinds of things all of the time. And they exercise our brains in new ways, and often enrich our lives in ways we couldn't have anticipated. One barrier to learning a musical instrument is that you have to put in a lot of time up front before you get to a stage of practicing that is enjoyable. One barrier to a learning a language is that you often don't get frequent opportunities to put your knowledge to use, and hence you forget things because they are not sufficiently reinforced. In learning about cybersecurity, neither of these barriers exist! You can very quickly get to a stage where you will start to see benefits and have fun with your newly acquired knowledge, and the multitude of daily interactions you already have with technology will provide a nearly constant stream of opportunities for you to solidify and expand your understanding.

So let's get started!

First I want you to start making a mental inventory of the most important devices, websites, and digitally managed accounts that you interact with frequently. Maybe you have a smart phone. And a smart watch. And a smart fridge. And a smart dog who has figured out how to use the voice control for the grocery interface on the smart fridge to order extra bacon with a perfectly tuned bark. That last example is probably less relevant, but I like to imagine such things.

Maybe you have several email accounts, an amazon account, a Facebook account, and an online banking account. A defunct Myspace account if you are old, a hip Snapchat account if you are

young. Maybe you have a usb stick on your keychain with important information on it, maybe you have a "hardware security module" you were given at work for "VPN access" that you have never bothered to learn how to use.

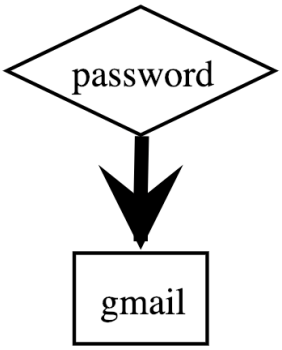
These kind of scattered objects and digital identities populate the broad landscape of your own digital life. It's likely to feel very cluttered as you start to fill it in. With all of the clutter distracting you, it can be hard to see the forest through the trees.

So let's begin to identify some basic categories and structures in your digital life, to help make sense of it all. One basic category is **devices.** These are the physical objects that form the interface between humans and cyberspace: our phones, our laptops, our smart tvs, surveillance cameras, etc. Another category is **accounts.** These are the digital identities that we use for services like email, online banking, online shopping, and so on. We access these identities through the physical devices we directly touch, but they transcend those devices and live more broadly on infrastructure that we don't physically control or interact with directly. Another somewhat more nebulous category is **information.** This covers passwords, answers to security questions, phone passcodes, and other things of this nature. Any comprehensive map of our digital lives will likely include many things in each of these three major categories. The categories aren't perfect - some crucial things might not fit obviously into them: is a fingerprint closer in spirit to a piece of information? Or to a device? But still, keeping these three categories in mind is a good way to make sure you aren't ignoring any major components of your technological landscape. Going forward, we'll refer collectively to objects like devices, accounts, and information as "assets".

Now that we have a rough sense of what individual assets serve as our personal landmarks in cyberspace, let's think about the common relationships between them.

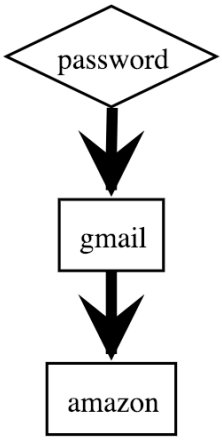
One very common and important relationship is that of **control.** If you leave your email account logged in on your laptop, and your laptop is not password protected, then this means that physical access to your laptop can be used to **control** your email. And similarly, if your email account can be used to reset the password for your amazon account, then access to your email can be used to **control** your amazon account.

We can visualize this kind of control relationship as a directed edge between two nodes in a graph, which is fancy math speak for an arrow from one dot to another:

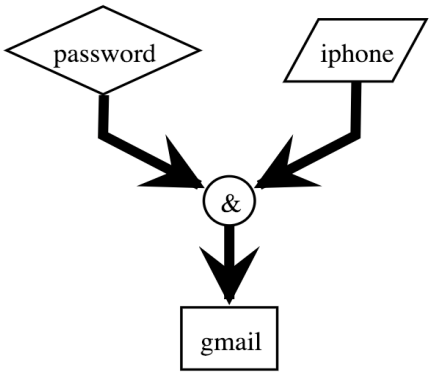


The ``things" in our digital life will be visually represented by dots. The basic control relationships between them will be represented by arrows. A single arrow from a dot A to a dot B means that anyone who has control of thing A can extend that power to also control thing B.

Sequences of these arrows form paths: a path from A to be B means that someone who controls A can, via a sequence of steps, also gain control of B.



In the cybersecurity realm, there is another kind of relationship between assets that is fairly common, but slightly more complex than the one-to-one relationship of a password that opens an email account. It arises from something called "two factor authentication." The "two factor" part of the name refers to scenarios when getting into a device or account requires control of two different resources. For instance, maybe knowing the password is not sufficient *by itself* to get into an online account. Maybe you also need a temporary access code that is texted to your phone. Or maybe a smart phone is set to unlock only if you enter the proper passcode *and* provide an accepted fingerprint. These 2-to-1 relationships, where controlling two items simultaneously can be extended to control a new item, will be visually represented like this:



The visualization here emphasizes the fact that controlling just *one* of the originating assets does not itself extend to control of the new asset. But if you control *both* originating assets, the extension is enabled.

Putting this all together, we can build a "map" of your digital universe, with paths that express all of the implied security dependencies. Mapping out this kind of structure for our devices, accounts, and relevant pieces of information gives us a single conceptual framework that we can use to address what might seem like a long and disparate list of questions. Questions like:

1. If a stranger steals my phone, will they be able to access my email?
2. If I share the password to my Netflix account with my roommate, who I also share a desktop computer with, will there be any unintended consequences?
3. If a con-artist knows my birthdate, my social security number, and the contents of my social media posts, can he or she access my online bank account? And what other assets might be at risk?
4. What benefit is there to using two-factor authentication for my work email?
5. How should I choose the security question answers for my online banking account?
6. Why is reusing passwords discouraged? Shouldn't one really good password be enough?

A question like 1. Above is relatively straightforward once we have our map of assets and the control relationships between them. We can restate this question as: if someone controls the physical asset of my phone (which is a dot in our visualization), will that imply control of my email? In other words, is there a path of steps starting from the phone dot to the email account dot? If yes, then yes! If no, then no! So this is a just a question of: can dot B be reached from dot A via a sequence of steps? In other words, is there a path from dot A to dot B?

A question like 2. above is a little more broad, but still translates to a pretty straightforward question about our map of assets: what are all of the *other* assets in the map that are reachable via paths starting from the Netflix account password? If the password is never reused, the answer is just the Netflix account itself. But if you have reused your Netflix password for other purposes, the answer might be a much larger (and more worrisome) collection of assets. While Question 1 required us to determine the existence or non-existence of one path between two specified points, Question 2 asks us to find and describe the set of all points connected to a specified starting point via paths.

Question 3. is similar to Question 2., but instead of asking for an inventory all of the assets that are reachable by paths from a single starting point, it compels us to inventory all of the assets reachable from a collection of starting points. Because of the possibility of 2-to-1 control relationships, this might include some assets that are not reachable from any *one* such starting point alone.

Question 4. is a question not about one specific map of assets and control relationships, but two maps: a version of the map *without* two factor authentication, and a version of the map *with* two factor authentication. How might we compare the two maps and make statements explaining in what ways one is "better" than the other? A natural approach is to compare the answers to questions like our questions 1., 2., and 3. above: a compromise of a single asset or set of assets in one map might snowball into a greater region of compromise on one of the maps than the other, allowing us to pinpoint a particular way in one map might represent a better security strategy than the other. But we should be cautious about judging a map too harshly. From a security perspective, the ideal map is one with no paths whatsoever! In such a digital universe, all of our assets are safe, but none of them are usable! So we must be conscious of the ever-present undercurrent of tension between security and usability. We compare two maps on security criteria not so we can definitely crown a "winner," but rather so we can make more informed and deliberate decisions about security and usability tradeoffs. If one map represents a vast improvement in security over another in many common scenarios of asset compromise, and only results in a relatively minor increase in inconvenience, it may be worth it. Whereas if a map represents a small increase in security over another and results in a prohibitive level of inconvenience, it may not be worth it.

The most important lesson here is that this isn't rocket science. You can make more informed decisions about how you set up your devices and accounts, and keep track of the implications. You can make individual choices with an understanding of how they affect the bigger picture, And you can learn the core concepts underlying security dependencies that will serve you well in evaluating new technologies and new options that aren't covered explicitly on any particular checklist.

This is just an introduction. Upcoming articles in this series will dive deeper into the details.