Managing Your Digital Life: Beyond Social Media

Overview: Computers, mobiles, digital files, pictures, notes, cloud, social media…. The information about us is everywhere. How do you know what's going on, and how can you best take control of your digital life? Find out now!

Student Skill Level: Basic – this is for everyone!

Requirements:

- A desire to learn!

Objectives:

- The student will be able to:
  - Understand the scope of information available to people
    - See examples of technology today, and how much they "know" about us – Google in particular
    - What do our browsers say about us online?
  - Understand the impact of computer devices on all humans – especially younger generations
  - See examples of tomorrow's technology
  - Understand the implications of these changes on themselves and others

Image courtesy of khunaspix at FreeDigitalPhotos.net

Scope of Available Information

There is a ton of information available on the Internet. Some we give out ourselves, some we do not. What's the deal, anyways? Well, Dave Lewis (2017) from CSO Online Magazine (CSO stands for Chief Security Officer – Information Security) states: "Governments the world over are moving to **strip privacy from their citizens under the guise of security**. One was the battle cry was to protect the children which has given way, in most respects, to the fight against terrorism. That logic has the appearance of being sound for people who are afraid will be less likely to argue.

I personally have always loathed the argument that you have nothing to fear if you have nothing to hide. Personally I say nuts to that. …Now, with **reports that the US government will be asking travelers to provide their social media accounts at border crossings** it really sank in that it is time to say something about this trend."

Google and Other Search Engines Track You

Wendy Boswell from Lifewire (2017) has some very interesting points. If you are signed in to a device, like your Android phone, tracking is more in-depth. But, even if you're not signed in, search engines track us all, big time. **If you are signed into your Google account, they see:**

"**What** you are **searching** for
How you are searching
Your **search patterns**
What **ads** you're interested in
What you click on
What **images** you view
What **videos** you watch"

Does Google Track My Search History Even if I'm Not Signed In?

Every single time we log onto the Internet, we leave traces of our identity via **IP addresses** ("An IP address provides an identity to a networked device. Similar to a **home or business address supplying that specific physical location with an identifiable address, devices on a network** are differentiated from one another through IP addresses" Fisher, 2018), **MAC addresses**, (this is an identifier "used by Ethernet to identify a unique network card inside a device. Think of the **IP address as the road name and MAC as the door number of a house**" – Wikipedia, 2018) and other unique identifiers. In addition, most **web browsers, sites, and applications require the user** to opt in to the utilization of **cookies** – simple software that basically make our web browsing experience more enjoyable, personalized, and efficient.

If you're not logged into Google, there is still a wide variety of information that you're making available to Google simply by being online. That includes:

- **Where you are in the world** geographically
- Your **IP address**
- Information about the Google services you use and how you might be using them based on **your activity patterns**
- What **ads** you might click on
- What **device** you are using
- **Server information**
- Identifying information gleaned from your use of partner services.

This information is used for **targeted ad placement** and search relevancy. It's also made available to **people who own sites that are tracking data** via Google's statistics tool, Google Analytics; they won't necessarily be able to drill down and see from what neighborhood you're accessing their site, but other identifying information (device, browser, time of day, approximate geo, time on site, what content is being accessed) will be available. (Boswell, 2017.)

"What are Examples of Information That Google Collects?

Information that users give to Google, including personal information such as name, email address, phone number, credit card, and photo
Information gleaned from use of Google services, including usage data, personal preferences, emails, photos, videos, browsing history, map searches, spreadsheet and documents, etc.
Information from the device you are using to access Google and Google services, including hardware model, mobile network information (yes, this includes your phone number), even what operating system you might be using
Server log information collated from when users are actively using Google services, including search queries, phone information (time and date of calls, types of calls, forwarding numbers, etc.), **IP addresses, cookies** that are uniquely linked to your web browser or Google account, and device activity information (crashes, what settings are on your hardware, language, etc.)
Location information about where you are in the world, including your city, state, neighborhood, and approximate address
Peripheral services and apps can also provide what is called a "unique application number" that provides more identifying information to Google when queried
Search history, including personal information found in Google services such as YouTube, Google Maps, and Google Images
User interactions with other sites and services are also tracked, especially when the user interacts with ads." (Boswell, 2017).

There are several lists of search engines that do not track users. Top on these lists is **DuckDuckGo**.

Also mentioned frequently are the following (from USA Today and NordVPN)

Ecosia.com

Startpage.com

SearchEncrypt.com offers better default privacy than the more popular DuckDuckGo.

Yippy.com (automatically filters all adult content for kids)

Swisscows.com

If you are signed into your devices, there are a number of other, **private messaging apps that you might use. Private messaging (like text messages) are one of the most confidential ways to communicate today, on any computer device.**

“Adrian Mahieu, security expert and CEO of Cortex Insight said this: Installation of **Signal** is at an all-time high with month on month increase in users. More users installing **Telegram** and **Wickr**. (**Signal** is a private messaging app for Apple and Android. It’s geared towards privacy and security rather than cute emoji stickers. In fact, so good are its security measures that even Edward Snowden recommends it… Anything you send or receive is encrypted, which makes it very hard for anyone who intercepts the data to work out what's being said unless they are the specified recipient. What's more, Signal doesn't store any user data, so governments and other agencies can't request it, and it can't leak out.” “**Telegram** is a messaging service combining the speed of WhatsApp with Snapchat’s ephemerality and advanced new security measures.” – see Hamburger, 2014. “The **Wickr** instant messaging app allows users to exchange end-to-end encrypted and content-expiring messages, including photos, videos, and file attachments. The software is available for the iOS, Android, Mac, Windows, and Linux operating systems.” – see Wikipedia, 2017)

On top of that, **[Signal’s] code is open source, which means anyone can look at how the app is written**—that doesn't mean hackers can break Signal's encryption (which is virtually uncrackable), but it does mean **security experts and users can check that Signal is maintaining the high privacy standards** that it says it is.

Just about every **security researcher that's taken a look at Signal has given it a big thumbs up** from a data privacy and security standpoint, and its underlying technologies are now used in a lot of other apps too. The FBI and CIA might not like it, but right now Signal is about as good as it gets for "going dark" on your phone.

Border search & seize of electronic device worries are at an all-time high - good/bad travel advice is all over social media with respect to this. (US borders **extend up to 150 miles inland – we are “at the border” here.**

One very interesting thing is happening though: These technical tools are now being used by Millenials as a matter of course - they as an age group care more about their privacy than many."

Impact of Devices on Children, Teens, and Young Adults (Older ones, too!)

Tracking begins with your Browser

Have you noticed the creepy advertisements that pop up on web sites you have visited, even only once? How in the world did it know? Well, tracking you begins with any browser you use to surf the Internet.

Please go to www.webkay.robinlinus.com

Scary, right? I know I was surprised!

Unfortunately, EVERY WEB BROWSER tracks its users. How much? Well, David Nield (2017) wrote an excellent piece on this. He points out the following: "Unless protect yourself, **as soon as you open up an internet browser, you begin to leave digital footprints behind you that the sites you visit can use to track your activities and recognize who you are**. We're not talking about some crazy government data mining operation. This is **totally legal, above board tracking** done by the sites and services you use every day. **Data collected includes your current location, which links you're clicking on, whether you're on desktop or mobile.** And that's just the beginning."

"The information leak starts with your browser, which reports various bits of basic data to the sites you visit by default. As soon as you appear online, for instance, you start reporting an **IP address, your particular entry point to the internet**, which can be used to approximate your location.

Your **browser also reports its name**, so sites know whether you're a Chrome devotee or a Firefox user, as well as information about the **computer system** it's running on, including your desktop or mobile OS, the **CPU** and **GPU** models, the **display resolution**, and **even the current battery level** if you're using a laptop, tablet, or phone."

https://panopticlick.eff.org/

https://clickclickclick.click/#245e0be49c167c3e18d99961e40a463c

"Sites can also choose to monitor your inputs much more closely**. To see some of this tracking in action, head to Click, which will report your mouse movements, mouse clicks, and other browser actions back to you.**

These nuggets of data are just the first that help sites identify who you are. Your browser revealing that you're running Microsoft Edge from somewhere in New York doesn't tell a website much about you, but **it can be combined with other data points to pick you out from a crowd.**

Open up the **Panopticlick** test from the Electronic Frontier Foundation, and you can learn more about how **your browser can broadcast a unique fingerprint to the web**—your very own specific mix of browser software, hardware, default language, even the fonts you have installed—which can identify you even without any other information. In other words, it's unlikely that anyone else is using your special combination of monitor color depth, screen size, combination of browser plugins, and so on. **Even if you haven't typed in a single personally identifiable piece of information, a website can make a good guess about whether you're the same guy who swung by last Tuesday**, and can market you some **relevant advertising accordingly**. Browser-reported data is just the beginning. The next layer is the data sites can gather for themselves."

“Most **sites are very keen to find out as much about you as possible**, whether to personalize their services to you or to target you with advertising. To help log this data, they’ll usually drop what’s called a **cookie** on your system when you turn up for the first time—these cookies are little files that act as markers to identify you.

Like breadcrumbs in a forest, they tell a site that you’ve been there before. They can also hold little bits of data: **A cookie might save you the trouble of having to pick a particular city every time you visit a weather website**, because the site knows what you picked last time; a **cookie can also store items in your shopping basket** so they’re still waiting for you when you come back days later.

Browser security protocol dictates that sites can only access their own cookies—a fairly essential safety measure—but you also have what are called **third-party cookies**, which aren’t associated with a particular site but **get injected across multiple pages through ad networks and other tracking technologies.**

It’s these cookies that result in you seeing ads for fishing gear for a whole week just because you opened up a fishing website a couple of times, and it’s these cookies that Apple is fighting hard against in the latest version of its Safari web browser, much to the chagrin of advertisers.

Fundamentally, this is all being used to recognize who you are and better target advertising. Data from website visits, searches, cookies, and your browser is put together with some educated guesswork to try to figure out the ads you’re going to be most interested in seeing.”

“What’s more, a recent study from Princeton University found that **cross-site trackers embedded in 482 of the top 50,000 sites on the web were recording virtually all of their users’ browser activity** for analysis. These recordings are ostensibly for the purpose of website management and optimization; but while **sensitive information is supposedly redacted** from them, it’s another case of users having to put their trust, and their data, into the hands of third-party companies.

And another group of firms are adding to this pile of data: **Our internet service providers, which can now make money by selling your browsing history**, letting advertisers know where you’ve been and what you’re interested in. **None of this data works in isolation**, with marketing firms trading details and combining details to put together a very detailed profile. And it gets even more detailed...”

“So far, so much information, but we haven’t yet talked about the data you’re giving up voluntarily: The searches you run while signed into Google, the venues you check into while using Facebook, the date of birth details you give to Twitter, and so on.

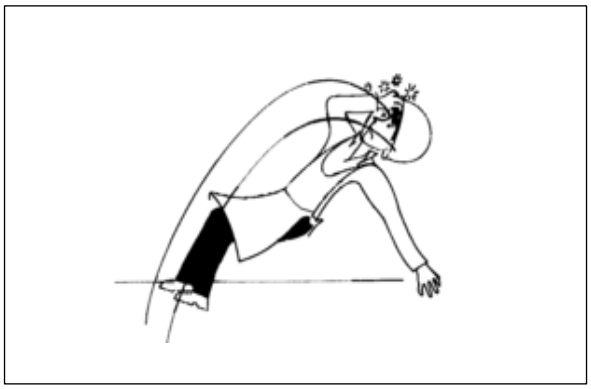
Sites have their own privacy policies about how this data can be used—usually to target you with advertising, and maybe to improve the actual products and services at the same time—and the **usual**

deal you make is to put up with this data collection if you want to use the services in question. Add all of this personal information together with the data that's already been harvested from your online sessions, and the **biggest operators like Google and Facebook can easily know you better than you know yourself.**

Last year **Google amended its privacy policy** so that data from its DoubleClick ad network could be merged with the other data it knows about you—like your name and your favorite YouTube channels—to **build up a very comprehensive picture of you and your tastes**. Not every company has the reach of Google or Facebook, but data can be easily bought and sold between firms specializing in this kind of profiling.

On **Facebook alone you could well be revealing who your closest friends are, the places you like to visit most, how often you order pizza**, and the top bands living or dead that you'd want to put in your dream gig line-up."

"DATA COLLECTION AT ITS CORE IS NOT MALICIOUS. Websites need data to make their products better and to sell you the advertisements that keep them afloat. That said, you should be conscious about what you give up and to whom. For more on that, see our companion guide on how to avoid tracking as you browse the web."



Some simple steps to help you

Again, Mr. Nield does a great summary of some simple steps you might take to help protect your online privacy. "Starting with data reported to sites by your browser, a plugin or extension is probably your best bet for stopping data from leaking out. **Try NoScript Security Suite for Firefox or ScriptSafe for Chrome, which prevent active items on websites from running when you don't want them to**. Other good options include the Electronic Frontier Foundation's Privacy Badger, which blocks third-party tracking cookies while allowing useful, like those that record ones to continue operating, and Disconnect, which offers free add-ons that work in a similar way. We also like **Ghostery, a privacy extension available for Chrome, Firefox, Opera, and Microsoft Edge**. Like Privacy Badger and Disconnect, it stops cross-site, third-party trackers from running, and you can actually see a list of trackers on each site and choose to block or allow them as needed."

There are built-in browser options that you may use to help avoid tracking. "For more cookie settings beyond the extensions we've mentioned, head into your browser's settings page. **One of the settings will refer to Do Not Track, an agreed-upon protocol that automatically asks sites to not run any scripts designed to track your behavior.** It sounds like a perfect solution in theory, but there's no legal obligation for websites to honor the request, and many will just ignore it. … Opening up an **incognito or private window can help**. In these cases **cookies are only kept for the current browsing session**, so as soon as you close down the incognito window, they get erased from your system. From the perspective of the browser, it's as if you were never online at all.

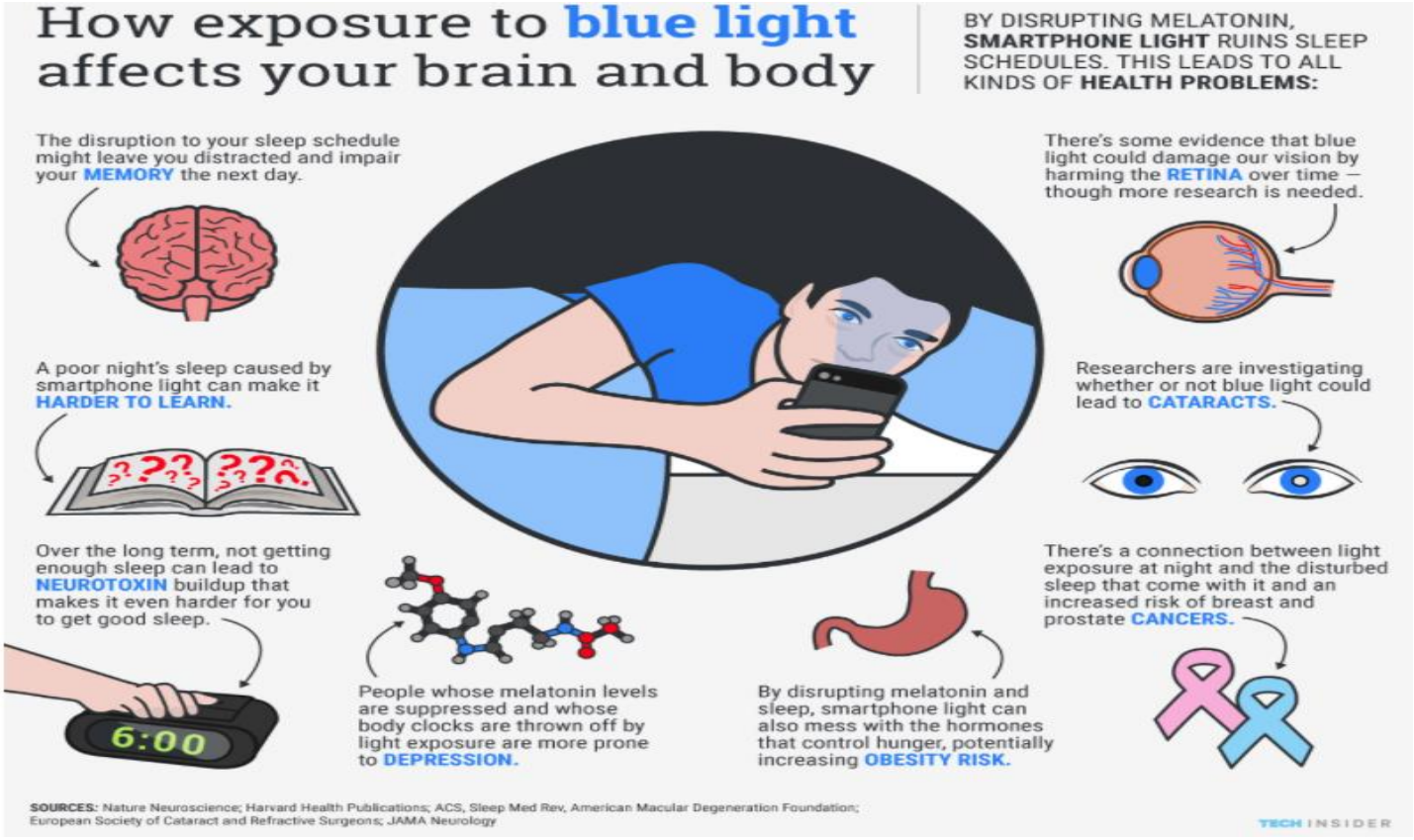
On the other hand, incognito mode doesn't stop websites and ISPs from knowing you're online. You're still broadcasting your IP address, for example. And, of course, if you log into Facebook (or anywhere else) all the usual rules about tracking and data collection still apply. It's best to think about incognito mode as hiding your browsing activity on your local device rather than adding any extra anonymity to your online travels."

Impact of Devices

I looked around online (I see the irony here) and found a well-written paper by an unknown student from California State University at Northridge - CSUN. I pulled some of the references here from that paper, and want to give proper credit, so I put these in my reference list at the end of this handout.

"Smartphone screens emit **bright blue light** so you can see them even at the sunniest times of day.

But at night, your brain gets confused by that light, as it mimics the brightness of the sun. This causes the **brain to stop producing melatonin, a hormone that gives your body the "time to sleep" cues.** Because of this, **smartphone light can disrupt your sleep cycle**, making it harder to fall and stay asleep — and potentially causing serious health problems along the way" (Loria, 2015).



A big concept is called the **“continuous, partial” attention span**. This term refers to the way anyone might pay partial “simultaneous attention to a number of sources of incoming information, but at a superficial level. The term was coined by Linda Stone in 1998. Author Steven Berlin Johnson describes this as a kind of multitasking: "It usually involves **skimming the surface of the incoming data, picking out the relevant details, and moving on to the next stream. You're paying attention, but only partially.** That lets you cast a wider net, but it also runs the risk of keeping you from really studying the fish" (Wikipedia, 2018).

I see this All. The. Time.

I’m glad there’s a name for this phenomenon.

“Continuous partial attention can **hamper your relationship-building efforts** - not only on a **personal level**, but also on a professional level. When attending a function of any type, it is becoming **increasingly common to find people who remain connected to their social networks** (beyond uploading a photo or tweet about the event) with mobile devices during the meeting…. We have probably all experienced being in conversation with someone at a networking function and getting pinged during the conversation. **When we take our attention off what is happening in front of our nose to take a look at what is happening on our phone, we lose the connection with the person we’re speaking with. We will not remember this part of the conversation well, if at all.** And we will send a subtle message to this person that he or she does not matter as much as the various pings coming in on our mobile device do” (Misner, 2014).

“It’s like having one foot in cyberspace and one foot in “meatspace” all the time. It’s not that easy to do, and occasionally you stumble trying to accomplish both. [Linda] Stone goes on to say, “Continuous partial attention is an **always-on, anywhere, anytime, anyplace behavior that involves an artificial sense of constant crisis.** We are always in high alert when we’re in constant partial attention.” Stone calls attention “the most powerful tool of the human spirit.” She says you can enhance it through things like exercise and meditation, or you can “diffuse it through technologies such as email and Blackberries.”

Whether you call it autopilot or continuous partial attention, I’m not sure living this way is all it’s cracked up to be. Life is not best lived in “an artificial sense of constant crisis.”” (Jantz, 2018).

Tomorrow's Technology

First, a little history. Much of the newest innovations will depend on some sort of 5G access.

"The "G" in 5G stands for "generation." **Wireless phone technology technically started with 1G**, and in the early 1990s, and it expanded to **2G** when companies first started enabling people to send **text messages** between two cellular devices.

Eventually the world moved on to **3G**, which gave people the ability **to make phone calls, send text messages, and browse the internet**. **4G enhanced many of the capabilities** that were made possible with the third generation of wireless. People could browse the web, send text messages, and make phone calls—and they could even download and upload large video files without any issues.

Then companies added **LTE, short for "long term evolution,"** to 4G connectivity. LTE became the fastest and most consistent variety of 4G compared to competing technologies like WiMax. The difference between WiMax and LTE is similar to the difference between Blu-Ray and HD DVDs: Both technologies achieved similar outcomes, but it was important to create a standard for everyone to use. LTE did just that, and it made 4G technology even faster.

5G will build on the foundation created by 4G LTE. It's going to allow people send texts, make calls, and browse the web as always—and it will dramatically increase the speed at which data is transferred across the network. 5G will make it easier for people to download and upload Ultra HD and 3D video. It will also make room for the thousands of internet-connected devices entering our everyday world. Just **imagine upgrading your data connection from a garden hose to a fire hose**. The difference will be noticeable" (Nunez, 2016).

"There are already huge consortiums of major global telecoms working to create worldwide standards around 5G. Although most of those standards haven't been solidified, experts expect it to be backwards compatible (with 4G and 3G) in addition to having some interoperability across the world.

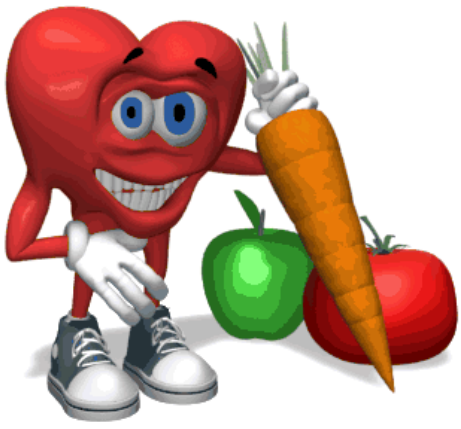
In their most basic form, cell phones are basically two-way radios…. **Typically when a new mobile wireless technology comes along (like 5G), it's assigned a higher radio frequency**. For instance, 4G occupied the frequency bands up to 20 MHz. In the case of 5G, it will likely sit on the frequency band up to 6GHz. The reason **new wireless technologies occupy higher frequencies is because they typically aren't in use and move information at a much faster speed. The problem is that higher frequency signals don't travel as far** as lower frequencies, so **multiple input and output antennas (MIMOs)** will probably be used to boost signals anywhere 5G is offered" (Nunez, 2016).

“Even in a world accustomed to breathtaking technological disruption, the news that **GM will launch a car without a steering wheel or pedals next year comes as a shock. This significantly modified Chevy Bolt shows that the future is fast approaching** — a future of driverless cars and autonomous vehicles instead of the human-operated vehicles that we have known for over a century.

Welcome to the age of the truly driverless car: GM's latest self-driving vehicle is a modified Chevy Bolt without a steering wheel or pedals. GENERAL MOTORS

What will replace the steering wheel, pedals, and driver controls is, quite simply, communications technology. The vehicle will be communicating constantly — within itself, with other vehicles, with small cell technology that will be deployed ubiquitously, and eventually with the overall infrastructure of our roads including traffic lights, bridges, and street signs (check out this preview). This continuous communication from, to, and within the vehicle will be what keeps it operating safely. Lose it, and the vehicle stops.

Expect to see more of these types of announcements. This kind of communications technology also powers smart cities, telehealth, and other innovations — in essence, recreating the world around us” (Keenan, 2018).



“Consider telehealth. The 5G revolution will offer new opportunities in remote diagnostics, wearables that can transmit data constantly to doctors and other healthcare providers, and remote surgery, too. For an illustration of what 5G can do, consider an example from Taiwan: the “Citizen Telecare Service System” helps the elderly through remote monitoring and assistance in managing chronic diseases, including risk assessment and rapid response to health crises. 5G will make this happen more quickly and reliably and with greater functionality” (Keenan, 2018).

What Can You Do to Manage and Protect Yourself?

Seth Rosenblatt, a contributor to the C-Net web site, wrote a very interesting article. In it, he states: "You may not feel like the flotsam and jetsam that make up the facts of your life are important, but increasingly companies are using that dry data to make your every online step as indelible as if written in blood. Here's how to take back your digital dignity…. The Internet companies that power your online life know that data equals money, and they're becoming bolder about using that data to track you. If they get their way, your every online step would be not only irrevocable, but traceable back to you. Fortunately, there are some positive steps you can take to reclaim your online history for yourself."

"If you're concerned about privacy and people making connections between your birthday, your address, and your Social Security number, you owe it to yourself to perform at least one Web search for your name and see what comes up. You might be unpleasantly surprised."

Example: search familytreenow.com
Example: Facebook: Settings > Ads > Your Information > Your Categories

You might "Paint over the bad with good…. [If there is negative content about you on the Internet]…, you can create new, fresh, positive content to counteract it. The idea is that the Positive You will bury the Negative You. You can also use social-networking sites to bury bad news. From About.Me to Flickr to Twitter, social networks tend to rank highly in search results. By creating and maintaining accounts that use your real name, you can elevate the social networking results for your name and, ideally, drop the results you want to bury onto the second page of results. Since studies show that second-page results are viewed significantly less often than first-page, this could be a successful burying strategy."

Watch out for your personal information. Courtney Baker compiled an excellent list of information we all should safeguard – to the best of our abilities. Here they are:

#16 – Your Hobbies, Club Memberships, or Employer

This might seem like an unusual place to start this countdown, however many aspiring thieves begin their hunt here. This information is insanely easy to obtain, as we rarely protect these details. Once they've obtained this information, thieves will either leverage it to pretext (impersonate you) or in various phishing scams (impersonating the club, organization, or even employer). The basic idea is people are much more likely to respond to e-mail and telephone scams when they appear to be from groups they belong to.

#15 – Where You Hold Financial Accounts

Again, the value here lies in the ability for thieves to leverage this information when pretexting or phishing. Thieves will study how major banking and financial institutions contact their customers, in order to make their scams appear more genuine. In general, be wary of ANY e-mail that asks you to provide additional information, even if it looks authentic.

#14 – Your Telephone Number

In general, most of us are weary about giving out our phone number based on fear from getting telemarketing or fundraising calls of some sort. While it happens far less frequently, identity thieves aren't afraid to tap into this medium, as well.

#13 – Your E-mail Address

Like your telephone number, your e-mail address is most valuable as a medium for phishing scams. E-mails are easier to automate, can be made to look ultra-authentic, and have a higher rate of success than phone or snail-mail. E-mails addresses also carry a little extra weight, as various online accounts allow you to use them as a username.

#12 – Your Physical Address (including previous ones)

While used more rarely these days as a medium for phishing, the threat of receiving "bait" in the mail is still very real. These attempts can range from phony bills, sweepstakes scams, or change-in-service notifications with bogus customer service telephone numbers. In addition to phishing, **thieves can use your address to initiate a "change-of-address," effectively rerouting all your mail (and the additional information within) for at least a couple days.**

#11 – The Expiration Date or Confirmation Code of Your Plastic

While obviously not as valuable as the actual account numbers themselves, these two items are the most common form of security when using your plastic. These can either be picked up by more advance skimmers *(a special device attached to common places where you swipe your card)* or as the target of a phishing scam. It should go without saying that if someone can piece together your account numbers with one or both of these items, you're in for some major damage control.

#10 – Where You Were Born

This information is much more valuable than it may first appear. It's yet another piece of information that can be used when impersonating you and/or verifying "your" identity with various institutions. In addition, thieves can use this to find public records, request birth certificates, and locate relatives. Knowing just someone's full name along with the city, county, state, or even nation of birth can open up a portal to the more valuable information later.

#9 – Your Mother's Maiden Name

Ah, the default piece of information used to verify so many accounts. Luckily, this has been so popular for so long that many organizations are shying away from even offering it as a verification option. Despite this trend, a vast majority of them still DO accept it. My suggestion? With so many other options available for verification, why use this one? If you have a choice, utilize a more random and difficult-to-guess verification question/method.

#8 – Your Banking PINs

Your Personal Identification Numbers or PINs act as mini-passwords (most 4-6 numbers in length) to your financial accounts. Unfortunately, many people use anniversaries, birthdays, or other easily guess personal information. Even worse, they store their PINs in their wallet!

#7 – Your Passport Number

A passport number in conjunction with an illegal database can result in a wealth of information for thieves. Passport numbers can yield full names, date of birth, place of birth, and of course nationality. (FYI, as of 2018, there are 9 states that do not comply with official documentation required for DOMESTIC FLIGHTS IN THE US. They are: Kentucky, Maine, Minnesota, Missouri, Montana, Oklahoma, Pennsylvania, South Carolina, and Washington. If you live in these states, a passport is REQUIRED ID.)

#6 – Your Driver's License Number

Your driver's license number is much like your passport number, but because it is more common and contains more information it is actually much more valuable. Amongst the information that can be illegally obtained through you DLN is your full name, date of birth, address, and basic personal appearance data (height, weight, eye & hair color). If physically stolen they are easier to alter successfully than passports and will usually result in less scrutiny.

#5 – Your Online Passwords (including usernames)

With everything moving online these days, your online usernames and passwords are becoming more and more valuable. It should be blatantly obvious that if a thief got his/her hands on your financial institutions log-in information, you'd be toast. You can do a lot with online banking these days. Let's even assume that they only get your e-mail password or even just a social media account. Unfortunately, I'd be scared to admit what other information would be attainable if my e-mail was compromised. Bottom line… be careful what information you send through e-mail.

#4 – Your Actual Account Numbers

In terms of stealing from your current accounts (opposed to using your info to open new accounts), your actual account numbers are the primary target of thieves. The most common accounts are checking, savings, credit cards, and debit cards, but don't rule out protecting your investment and retirement accounts.

#3 – Your Full Name (including aliases)

While this may seem too basic to include on the list (especially this low), it's value is so immense that it can't be neglected. "Name as it appears on card" is one of the most common security checks for online credit purchases. In addition, it's clearly essential when generating/opening new fraudulent accounts. While a name like Adam Baker isn't going to cause any problems, names like Robert, Richard, and Elizabeth can result in many different aliases. Finding your full birth name and common aliases is the base for everything else!

#2 – Your Date of Birth

Again, another bread-and-butter piece of personal information. But, like your full name, it's value lies in the fact that it's used in the creation of nearly every account. It's also one of the most common and easily-used pieces of information to verify existing accounts. Along with the one before it and after it, this comprised what I like to call the "Big 3″ of your identity (at least to the government/corporate worlds).

#1 – Your Social Security Number

Ah, the golden ticket. So obvious, you probably guessed it from the get-go. Unfortunately, this magical number is used by nearly every government and financial institution as the **primary** form of identity. It out ranks even your name, which can vary from institution to institution depending on minor details. While it may be a sad situation that your entire life can be summed up with a number… it can. It's our system and this is your only key. Protect it!

Baker, C. (2016). Top 16 Pieces of Your Information Identity Thieves Crave. Retrieved from Man vs. Debt Web Site: http://manvsdebt.com/top-16-pieces-of-your-information-identity-thieves-crave/.

Boswell, W. (2017). Does Google Spy on Me? Here's How to Protect Yourself. Retrieved from Lifewire Web Site: https://www.lifewire.com/stop-google-from-tracking-your-searches-4123866.

Computers and Their Impact. (No Date). Retrieved from CSUN Web Site: http://www.csun.edu/~lic42878/computers.html.

Fisher, T. (2018). What is an IP Address? Retrieved from Lifewire Web Site: https://www.lifewire.com/what-is-an-ip-address-2625920.

Hamburger, E. (2014). Why Telegram has become the hottest messaging app in the world. Retrieved from The Verge Web Site: https://www.theverge.com/2014/2/25/5445864/telegram-messenger-hottest-app-in-the-world.

Jantz, G. (2018). Are You Living in Continuous Partial Attention? Retrieved from Families.com Web Site: https://www.families.com/blog/are-you-living-in-constant-partial-attention.

Keenan, K. (2018). Driverless cars and other emerging technologies require a future filled with 5G. Retrieved from The Hill Web Site: http://thehill.com/opinion/technology/370343-driverless-cars-and-other-emerging-technologies-require-a-future-filled.

Komando, K. (2020). 6 Google search alternatives that respect your privacy. Retrieved from USA Today Web Site: https://www.usatoday.com/story/tech/columnist/komando/2020/11/21/6-internet-search-engines-respect-your-privacy/6306467002/.

Lewis, D. (2017). Privacy Issues in 2017. Retrieved from CSO from IDG: CSO Online Web Site: https://www.csoonline.com/article/3176766/security/privacy-issues-in-2017.html.

Loria, K. and Gould, S. (2015). How Smartphone light affects your brain and body. Retrieved from Business Insider Web Site: http://www.businessinsider.com/how-smartphone-light-affects-your-brain-and-body-2015-9.

Misner, I. (2014). The Danger of Continuous Partial Attention. Retrieved from Entrepreneur Web Site: https://www.entrepreneur.com/article/240254.

Nakutavičiūtė, J. (2022). The best private search engines for secure browsing. Retrieved from NordVPN Blog Post Site: https://nordvpn.com/blog/private-search-engines/.

Nield, D. (2017). Here's all the data collected from you as you browse the web. Retrieved from Gizmodo Web Site: https://fieldguide.gizmodo.com/heres-all-the-data-collected-from-you-as-you-browse-the-1820779304.

Nield, D. (2017). How to avoid getting tracked as you browse the Web. Retrieved from Gizmodo Web Site: https://fieldguide.gizmodo.com/how-to-avoid-getting-tracked-as-you-browse-the-web-1821008719.

Nunez, M. (2016). What is 5G and how will it make my life better? Retrieved from Gizmodo Web Site: https://gizmodo.com/what-is-5g-and-how-will-it-make-my-life-better-1760847799.

Rosenblatt, S. (2012). How To Delete Yourself From the Internet. Retrieved from Cnet Web Site: https://www.cnet.com/how-to/how-to-delete-yourself-from-the-internet/.

Wikipedia. (2018). Continuous Partial Attention. Retrieved from Wikipedia Web Site: https://en.wikipedia.org/wiki/Continuous_partial_attention.

Wikipedia. (2018). MAC Address. Retrieved from Wikipedia Web Site: https://simple.wikipedia.org/wiki/MAC_address.

Wikipedia. (2017). Wickr. Retrieved from Wikipedia Web Site: https://en.wikipedia.org/wiki/Wickr.

Edited 2023

Computer Training Program is provided by:

NIOGA Library System
Knowledge Within Reach

NIOGA LIBRARY SYSTEM
6575 Wheeler Road - Lockport, NY 14094
Phone - (716) 434-6167 Fax - (716) 434-8231