Erasing Your Online Identity

Now that we've cleared up our local identities, it's time to move over to the internet. So far, everything leading up to this point has been pretty straightforward and simple to do. This is going to be the first lesson where many of you are going to find your limits. Erasing your online identity is a very tough thing for us to do, many of your accounts you've most likely owned for a good part of your life, and some of them you may use everyday. So yes, this is the true beginning of a clean slate. **** Hold phone to ear **** *Let's start with a wake-up call.*

Promotional Spot

The first thing I want you to do is *login to your main email, and search 'sign up' in the search bar to get an unofficial a list of emails services you've signed up for. You should also search 'verify' as well. It might shock you to see how many services have your personal information,* if one of these services experiences a breach, most of your other accounts will also be exposed assuming you supply similar (or even the same) information. The sheer amount of services we mindlessly sign up for is pretty insane.

Next, if you have a Google account, go to *Google's 'My Activity' page, and browse through all of the information collected by Google.* This can be very unsettling, for me it was the recordings of every time I said OK Google that freaked me out.

Next, let's go to our good friend *Google.com. I want you to type in your email address, that's it. It's not uncommon to find random websites where people post your email with the password to get into your account right there from the search engine.* This comes from hacks or leaks, and this is how a lot of people are able to get into unprotected accounts. *You can also search your full name, phone number, and other personal details to see if your info is out there.*

After that, go to *'have I been pwned' and type in your email address to see if any of your information has been leaked from data breaches.* More than likely you're going to find some stuff you don't want to see. If there's nothing, then congrats, you haven't suffered a leak with that email.

Lastly, go to *pipl.com and type your name here to see if your personal profile is available for anybody to view.* A lot of you will have a profile here. There's also *anywho.com, which has a reverse phone lookup I recommend you try out.* These are just a few of the dozens of people-searching websites out there.
After doing all of that, my hope is that you at least see the potential risks in blatantly signing up for services with your personal information. Now you might

be asking how your information gets on these websites. *Well, a lot of it comes from online services you sign up for who sell your data. Post offices and other agencies could also be responsible, and we'll cover that in section 6.* The goal is to configure your browsing habits so this is unlikely to ever happen again, which we will cover later in the course. But for now, let's work on removing what's already online.

Remember that search you did within your email? For every service you signed up for that you no longer need, go to that *service's website, login, and find a place to delete your account. Before you delete the account, I'd recommend faking any personal information since we don't know if services are actually deleting your data from their servers, and this could one day be breached and released publicly.* Now yes, faking personal information is totally legal as long as you're not using it for fraud or illegal activities. *You can fake information by changing the email to a randomly generated one on tempmail.org, changing your phone number to one on freephonenum.com, changing your password to something random that you'll never remember again, and removing any other personally identifiable information about you.* Some services are stubborn and won't allow you to delete an account. First, try searching on *Google the service's name followed by 'delete account." A lot of times you'll find instructions there.* If there is, in fact, no way to delete an account, which does happen, just falsify your information, email, and password and never touch the account again. *Deseat.me offers a convenient service that scans your emails for any accounts you opened*, which is really nice! But keep in mind you are handing over all of your information to another company, so I would not recommend going this route if possible. If you're trying to delete an email account, I would recommend deleting all your emails and flooding the email account with mail bombers to spam the inbox with random information to help clear out any of your personal data.

Another good resource to spark your memory for rogue accounts is *justdeleteme.xyz, which has a list of different services that may help you remember. I also like using this as a resource before creating accounts to see how difficult it is to delete it down the road.* If something is too difficult to delete, I won't open the account.

Now, I know how difficult it is to entirely delete some accounts. So what if you aren't comfortable deleting a service you still want to keep? First, if it's something you use consistently, make sure you're utilizing privacy settings and giving the least amount of personal information possible. If you aren't deleting the service because you have some form of data on there you don't want deleted, like maybe a cloud storage service, see if you can move that data and **** hold external HDD **** store it locally (with proper security) so you can finally delete that account and still keep your data.

This entire process can be quick for some of you, but a majority will likely have to spend days, or even weeks working on this since you may have countless services accumulated over the years. Trust me, it'll feel good and worth it once you're done!

Next up is Google's *'My Activity' page, Go to "Delete Activity By", select "All Time" and "All Products", Then go to 'activity controls' and turn everything off to stop this stop this data collection.* If you're looking to go to the next level, I'd advise deleting Google altogether! This is very tough to do, but for those of you who really value privacy, this is a necessary step; *I put together a video breaking down the entire journey.* As for alternatives for individual Google services, these will all be discussed throughout the course, like safe messaging platforms, cloud storage, emails, etc...

Moving on...If you found anything exposing your real emails, passwords, or any other information about you in a Google search or 'have I been pwned', then you've got a problem. You must immediately change your passwords on these accounts, immediately! Don't forget about your other accounts which may use the same password. Alternatively, you can shut these accounts down altogether, which is what I'd recommend. As for exposed personal information, this is going to depend on whether or not you have the ability to remove it. If you do, then simply remove the identifiable information from the service and wait for Google to update its search engine. If you can't change or remove it, then contact the owner or writer of the page to see what they can do about it.

Exposed pictures are a bit easier to track though! You can find them by *dragging an image into google images to do a reverse image lookup, and find where that picture is posted on the internet. Another website, which does the exact same thing with slightly different results is Tineye.* If you do find something on a site you have control of, simply login and remove the image yourself. If you don't have control of the website, there are a couple options: 1) Contact the site's support team and tell them you don't give permission to have that image on their website. They will typically honor this; if they don't, the second option is to file a DMCA request by *following the instructions in the link found in the course sources.* This should be a last priority though since it dives into legal waters, and it could get you into trouble if you're misrepresenting the request.

Let's discuss your favorite topic: Social media. The obvious goal is to delete it altogether to dramatically improve your privacy, but I know a lot of you may not want to take that route. No matter what, *avoid using your full name if possible, make sure your accounts are private, enable as many privacy settings as possible, and avoid entering any information that isn't needed.* Facebook doesn't

need to know your address or birthday, so why give it to them? Bonus points if your public profile picture doesn't include your full face, so strangers don't know what you look like without adding you as a friend. I'd also recommend you go on a friend/follower purge where you remove everybody you don't actually know from your account, to avoid rogue snoops in your life. Once again, I'd advise removing it altogether, *not only is there some severe privacy invasion going on,* but it *has been shown to negatively impact your mental health--just something to think about.*

The very last thing you need to take care of is the people-searching websites. How do you remove your information on these sites? Sadly, you're going to have to reach out to all of these companies individually, and request them to remove your information. It's very tedious and every site has a different removal process. *ComputerWorld wrote an excellent guide going through people-searching websites, and how to remove your data on all of the major pages. This other website also has a guide which lays out the manual process, and they offer a service you can purchase to do it for you, although I would recommend going manual.*

Okay! At this point, you should hopefully have removed a good chunk of the services you don't use anymore, falsified any information for the ones that don't need your information, and only kept your actual information on as few services as possible. This is your clean slate!

Now, there's no other place to say this in the course, so I'm saying it here. You don't need to *register for services like Lifelock.* **** Throw all of these things over your shoulder **** You're wasting your money, time, and giving up information to a company that doesn't need to have it. Everything we've gone through in this lesson accomplishes the same thing as Lifelock, and this entire course will teach you how to protect yourself so you won't need to worry about identity theft and other invasions of your privacy. Not to mention...*Lifelock is partnered with Equifax, who suffered one of the largest leaks in American history.* Not only did Equifax suffer from this leak, but they profited from it through services like Lifelock. URGHH

Queue Outro Promos

That's going to wrap up erasing your online identity. It's very difficult to cover everything in one lesson, but that covered JUST about everything. The rest will come later when we retouch on this subject more in-depth. Hopefully if you followed a lot of these steps, you'll get the feeling of digital control, maybe for the

first time in your life! And this is just the beginning! I hope you enjoyed this lesson and thank you for watching.