Hacker-Proof

written by LYDIA JEN

How to protect your data from a cyberattack.

I compartmentalize my childhood into two distinct eras: BC (Before Computers) and AD (All Digital). BC: days spent soaking in the California sun while racing my cousins to the neighborhood park to squeeze in a couple rounds of soccer before dinnertime. AD: school lunch periods spent swapping Pokémon cards, until my classmates then moved on to trading Tamagotchis. When a friend showed up at my house with a shiny new first generation iPod a few years later, I remember aggressively messing with the click wheel, fascinated at how simple it was to navigate through hundreds of songs. No longer did I need to sit by the radio to record my favorite songs. That same friend introduced me to the endless world of computer games soon after. What once sat as an empty plastic box on the living room desk, transformed into a portal with direct access to an unexplored digital paradise.

As my interest in technology grew, so did my mother's concern. As a self-employed homeowner and landlord, she never really had the time to get into computers when they were first popularized—and understandably so. At the time, although she did not fully understand how computers or technology worked, she would never fail to remind me, on an almost day-to-day basis, to avoid revealing information that might identify myself to strangers. I used to think she was silly for being so cautious, but I now realize just how relevant her intuition was.

Regardless of whether you support the growth and advancement of technology, one thing is clear: as our digital world inevitably becomes more complex, hackers will become more sophisticated. Falling into a mindset of dismissal is incredibly easy when it comes to cyber protection, and I believe this is because the internet is, inarguably, one of the biggest staples of our modern society. Throughout the years, the internet has been seamlessly integrated into our everyday lives, and in most cases, this has been a great thing. For example, let's say I was working at my local coffee shop, and I decided that I wanted to grab lunch with a couple of friends—a quick text is all it takes to solidify some plans. One of us could pull up our Yelp mobile app, plug in filters to narrow down the search engine, choose a restaurant, and then send the address to everyone without even leaving the app. It would take me just a few minutes to plug in the destination point and call a Lyft, and then I'd be on my way.

Technology has made forming and maintaining connections conveniently efficient, but hackers are the consequence to this advantage. Due to how the media portrays cyber security breaches, people think that only large corporations or celebrities are attacked. However, viruses are not picky, and anyone can be targeted. At the end of the day, data is data, no matter who it comes from. Oftentimes, only a single click or swipe is needed for a virus to latch on to your personal information.

Let's go back to that coffee shop example, where we can assume I was connected to their public wifi: one point of entry for hackers to target. Through this entry point, a hacker would have access to my messages, any accounts I use, and where I frequent as an avid Lyft user. The sour cherry on top would be if I paid for my iced green tea latte using a card reader with a skimmer. A hacker would then have a record of my credit card information, possibly resulting in the draining of my savings. Do I really think that exact chain of events will occur? The truth is, I don't; but I know that there are people out there capable of pulling it off. The possibility is what encourages me to stay alert.

As a homeowner, landlord, most likely non-millennial, who has something of financial value to lose, the information in your messages or emails is probably in much more need of privacy than the messages in my phone insisting on pizza for a lunch date. But again, data is data, regardless of what it is, or who it's from. Therefore, because it's almost impossible to comfortably separate our personal lives from the constant transforming web of the digital world, setting up precautionary measures is important. Being prepared is more effective than scrambling around to secure already breached data.

Pinpointing every single hacker out there in efforts to decrypt their unique way of stealing information is unlikely, and if it's not your specialty, doing so would be a waste of time. Fortunately, there are now multiple ways to make sure that your digital footprint will be kept private and secured. Cybersecurity insurance is available to help with the financial burden that often comes with

a data breach. Unfortunately, investing in cybersecurity is not enough to make sure that you are well covered. Yes, you'll have a financial cushion to fall back on in the event of a breach, but this type of insurance is not really geared toward avoiding risk. Instead, consider setting up some safety nets for yourself.

Let's say you're the one working at the coffee shop in the previous example. A deadline is creeping up, and details still need to be communicated to your colleagues across the city. Using a VPN, or a virtual private network, will ensure that your digital footprint is secured and private—a perfect tool for those days when you just need to have freshly brewed coffee at your service. Next up: your wallet. Rather than using the magnetic strip and potentially exposing yourself to susceptible financial harm via credit card skimmer, use the microchip. Now that you're drinking your coffee (paid for via credit card microchip), relaxed thanks to the VPN, it's time to check your email. One of your prospective tenants sent you what they titled "Signed Lease Agreement." Before you open that attachment, be sure to double check the email address to verify the identity of the sender. Also, read through the message to clarify at what exactly you are looking. If everything matches up, go ahead and save the file onto your desktop, scan it for virus and malware, and then go through with opening it—a process that our firm also implements.

Go one step further and restrict the file sharing option on your devices. You could also encrypt all your devices. Nowadays, it seems like our whole life can be accessed with a couple of clicks, so encrypting your devices will make your data unreadable to someone who manages to hack into your data. For example, we do not allow our clients to send us personal information through email here at the firm; instead, we provide them with a safer, encrypted option. When you are ready to head home after a long day of work, you can call a Lyft from your phone, but before you do that, you have to unlock it. Make sure that your pin number is unique and personalized, but avoid setting a password that has any identifying information that may be linked to you. This rule applies to every password that you set. As a child, I remember using an old, now disconnected, phone number as my password for my computer game accounts. My mom would have probably scolded me if she'd found out, but now knowing what she knows, I have since gotten a little more daring with my passwords.

And that brings me to my last bit of advice. On top of taking practical steps to secure your identity in our ever-growing technological society, the most important thing to remember is to stay informed and up to date on new technological advancements. Devices, systems, and gadgets are being developed every day, so not only is it wise to update your literal hardware, but you'll also benefit from being knowledgeable about the gadgets you own.

My generation grew up during the transitional period between the analog and digital age; because of this, I am convinced that millennials have an interesting perspective on how technology has influenced our society. On one hand, I know nothing about owning a home, running a business, or breaking into the stock market; but on the other hand, because I adapted to the concept of technology at such a young age, I have the resources to help my mom understand how she can best secure her digital assets as a homeowner, landlord, and business owner. In return, she can teach me how to save money by making my own avocado toast instead of paying $13 for it at my neighborhood coffee shop.

Lydia Jen is currently majoring in English with a concentration in Creative Writing and a minor in Philosophy at San Francisco State University. When she is not at school, she works at Shwiff, Levy & Polo as an administrative professional.