“Are you a hacker?”

Any time someone asks me that question, I pause to reflect on what they mean. Do they want me to pirate software for them? Do they want to know if I can fix some problem for them that resides in some faceless back-end? Do they envision me in some shadowy, confined space up at all hours of the night relentlessly smashing keys in pursuit of some locked away gem of knowledge? Or do they have a genuine interest in my abilities as a problem finder/solver?

I usually respond in the affirmative and wait for the next question, but sometimes I can tell already what it will be. I definitely don’t pirate software for people (anymore), break into protected systems (anymore), and I think my home office is fairly well-lit and decently sized. The locked away gems I hunt are those that still reside in my own mind, waiting to be seized. So, if I peg someone as the type whose follow-up is likely on one of those veins, I just shrug and say “nah, not really.”

In reality, yes, of course, I am a hacker. But, it was many years before I became comfortable self-labeling as such without feeling like an impostor. When I was a pre-teen, the hacker persona I envisioned could do amazing things like break through any password-protected software on the fly, cause money to spit out of ATMs, and bring us all to the brink of nuclear war (thanks a lot, WarGames!). I could do exactly zero of these when I began my journey.

I began a typical 80s kid’s route to hackerdom by dialing up to various local BBSes and playing games, downloading piles of docs on all kinds of interesting subjects (yeah, you had to print them out if you wanted to realistically reference or share them), messaging other users, and learning about “warez” and the trading of them.

My first hack struck a blow against Corporate America. I had a Commodore 128 and a 1200 baud modem at that time (prior, my rig was the workhorse VIC-20 and its screaming 300 baud acoustic coupler). It occurred to me that the 2400 baud modem and mine were pretty much the same size, being cartridges and all. So, I purchased a brand new 2400 baud modem from a nationwide toy store chain, took it home, popped open the cartridges, and switched the guts. If I recall correctly, I had to make some small modification to (read: melted a hole in) the 2400’s case for it to fit back together. Armed with my receipt and recently swapped guts, I returned to the store where I made the purchase and approached the return counter. I was extremely paranoid that I was going to be busted. I was only 12 and had no idea how closely it would be examined. To my adrenaline-enhanced elation, I succeeded!

Soon, I began looking into disk copying software that eliminated copy protection and shoplifting games from another, more software-focused national chain. My technique was pretty good: walk in the store with a bag from another retail establishment (in the same mall, no big deal), grab two copies of the target software and hold them as one with one in front of the other, position things so that I could hold the bag open, and drop the back box in. I could crack the games and use them for currency to download other warez or, if that particular title was already cracked, I could sell a copy to my classmates for less than they would pay retail. When Pools of Radiance came out with its code wheel encryption, I had my first success using a hex editor to remove the check all on my own (shout out to Bandit’s Hideout in the 817!)

I wasn’t always breaking the law. One of my favorite hardware hacks to date was one I made when I was in junior high school. That
Christmas, I received a gift that was essentially an answering machine for your locker. It came with two whistles that you could give to friends, and the idea was that they could go to your locker (where you would hang this recorder inside), blow the whistle to activate it, and talk to the ventilation holes (where you would tape the microphone) to leave messages. For me, it had limited utility as my friend count was quite low and, of that number, none of them were really interested in my toy beyond an initial test.

I also had an old hanging door knob alarm that I had liberated from a box of old electronics my grandfather was tossing. I decided that I would see if I could somehow merge the functionality of "touch the doorknob to do X" and "blow the whistle to do Y" and I spent an evening following wires and leads from microphone to controller board of the tape recorder and weird insulated wire loop to controller board of the alarm. When I was satisfied that there was no harm in trying and thought I had a good idea of how the change should go, I cut some leads and soldered the right bits to their new places. I fully expected failure, but it worked! I was able to touch the wire and make the tape recorder turn on. I essentially had eliminated the hard limit of two users without resorting to paying for more whistles and struck another blow to Corporate America!

Eventually, retail security started tightening up and I abandoned the physical theft game. I turned back to the BBSes and piles of docs I had accumulated and started exploring the phreaking side of things. One box, two box, red box, blue box... there is no way I can get into the history of boxes in this article. Just imagine a world where payphones were plentiful (COCOTs were also fairly easy to find) and you could make free phone calls to anywhere at will if you spent a little money and some time with a sodering iron. The best part of that? Being one of very few people on your college campus that knew this stuff and making some spending money selling non-resident students the magic box that let them call back home to their parents, significant others, or anyone. Oh, and of course, giving Corporate America as many paper cuts as possible.

I think one of the most important skills for the general hacker is social engineering. Social engineering is fun. Once, my then-girlfriend and a few of her friends were looking for a place to rent when the semester was finished. She had an idea that I was a "hacker" (though I wasn’t embracing it fully at the time) and "good with phones" and asked if there was anything I could do to help make sure nobody got in touch with the person renting out this particular place. I called up Bell and posed as the mark, and was able to add remote call-forwarding to his list of services. Then, I simply forwarded his calls to an unused PBX extension on our dorm floor and waited for the girls to tell me they had it.

My college years were incredibly enlightening. Until 1991, I had never heard of the Internet. Once I learned some initial Unix commands for the school’s workstations, I began learning about how the systems on the network communicated, what services they offered, and how to chat with people all over the world. Instead of IRC, I fell hard into the MUD that was being hosted on one of the university’s Suns. I fell so hard, in fact, that my academic life suffered to the point that I was unable to continue my education. It was a depressing time. I had finally figured out that I wanted to be "in computers," likely a programmer of some kind, but I had just shot myself in the foot by dropping out of college.

To avoid the humiliation of returning to my hometown as a failure, I moved in with some roommates to save expenses and I took on temporary jobs, making pitiful hourly wages. I wanted to stay because it was 1994 and things were starting to heat up around everyday consumers and the Internet. I needed to get "in" somehow. During this period, I was still accessing my old university account to play the MUD. When we didn’t have phone service at the apartment, I would splice a neighbor’s line at the junction block while they were at work or sleeping. When the university disabled my login, I went to the lab and I found a way to
get MUD access from the dumb terminals without
needing to log in at all. It wasn’t magic, it was
CTRL-C telnet. And, if you are thinking, “Wow,
I could do some serious SMTP exploitation with
unlogged access to telnet,” you are right! I had
some fun with that, for sure. I never did anything
stupid, like a friend of mine who used his work
machine to spoof a threatening letter to President
Clinton. Seriously, he got walked out by Secret
Service agents and everything.

By this time, I had gathered various bits of
knowledge across a number of domains. I had
also made the jump in the temporary labor market
to “knows DOS” contracts. At last, a foot in the
doors! I slowly began the long slog through the
path of low-level IT/support grunt, to permanent
positions doing “level 2” support, then to
freelance work around the products I had been
supporting, to returning to Corporate Land as a
technical and sales-enablement trainer.

I came to view hacking as more of a life ethic
than an activity. I am always looking for ways
to poke at the squishy edges of things. I do it
to further my knowledge about that thing - or
how that thing, used in a manner that it wasn’t
originally intended, might help me discover more
squishy edges of another thing or things. Hacking
is not confined to the world of software or
computer hardware or phones. If you can envision
any process as a diagram or flow of individual
component pieces, you can come up with attack
vectors that can help you gain advantages or
control outcomes.

I was finally able to jump from the IT side of
technology to the creator/programmer side about
seven years ago. I had been dabbling with web
development as applications on smartphones
and it turned out I was pretty adept at it. I made
a few apps, then a little money. Then, like
before, I freelanced some work making apps for
other people. I became involved in the online
community and the IRC channel that grew around
the ecosystem. At one point, I approached the
smartphone manufacturer about a cryptic tweet
they had made regarding a position that seemed
perfect for me (minus the part about having no
professional programming experience or
computer science degree). They asked me to
describe what I thought the position would
entail. They practically plagiarized my response
when they made the official posting! I decided I
would take my chances, since I felt I was at the
pinnacle of my career path at that point. I still
had major reservations about being exposed as
a fraud, but I made it through the initial phone
screen, then another, then a face-to-face where
I had to do some of the hardest things I’ve ever
done in an interview. I was honest about the
perception I had of myself as not strictly a web
developer, but as a consummate troubleshooter
and asked questions of each of my interviewers
that let them know I was engaged and serious
about learning the things I couldn’t answer. In
short, I relied on every piece of experience I had
gained to that point and used it to hack my way
through each bit of that hiring process to land the
position.

So, yeah, I’m a hacker and I’m damned proud
of what I have accomplished. It doesn’t matter
that I’m not stealing corporate secrets from
competitors or fixing parking tickets for people.
What matters is that I know I can always approach
problems from an angle that is slightly different
than people who don’t care about the why. If you
understand the why of something, you can most
times deduce the how of subverting it. If you are
just starting your journey, don’t get discouraged
by not knowing everything (or anything!).

Keep hacking at things and, over time,
experience will improve your technique. Stay
safe, smart, and secure!

Who knows what mediocrity lurks in the hearts
of software? shadow knows... and likes to tell
everyone about it until they’re sick of listening.

HACKER PERSPECTIVE submissions have closed again.

We will be opening them again in the future so write
your submission now and have it ready to send!

Page 28