You can think back to the "aha" moments you had when you were first learning about computer science, or teachable moments where you've made something click for someone else. Were there any "big picture ideas" that gave you a helpful mental framework of how all these other tips and ideas fit together?

+ The cloud is just someone else's computer.

+ When you move or upload a file, you're making a copy of it.

+ Software updates are important because they often address known security exploits.

+ Deleted files can be recovered. If you're wiping a file, you're rewriting
over the file many times.

(Nash)
+ Things that don't fit in the visual of a "computer", like phones, are computers. Smart TV's, Cars (entertainment, navigation, and diagnostic systems) e-book readers and tablets, Home security systems, Point-of-Sale systems.

(Susan M)
+ Deleting or "emptying trash" doesn't actually delete the data!

(Nate)
Password reuse is bad because if one site has a mess up, it means that the rest of your life just got exposed.

(Shahid)
+ vicarious security

+ security is a team sport

+ one person can easily reveal sensitive information about a third party (a friend, colleague, or family member) that might inhibit their opportunity to freely express themselves in the future.

+ Shift the frame from “what do I have to hide” to “who in my network might be vulnerable"?

(Hugh)

When you send an email or other digital communication, that transfer involves the creation of dozens (hundreds?) of copies of that file on computers all over the world.

Also, my favorite big picture response to “I have nothing to hide” folks, re: NSA spying: Imagine a scenario where government agents come into your home while you sleep, and copy all of your stuff: your phone records, your correspondence, your purchase history, financial records, your reading material. They don’t harm you, or awaken you, and they leave everything as it was. But they do make copies while you’re sleeping. Is this OK with you? The answer, universally in my experience, is “hell no” followed by a little lightbulb going off over their head: “If this type of surveillance is wrong, why is the digital collection of everything outside our homes OK?”

(Danny)
Who is running what on your computer/device: operating system managed by Apple/Google/Microsoft, browser controlled by Google/Mozilla, apps controlled by whoever created them.

When you're talking to your friends privately on Facebook/Twitter, Facebook/Twitter gets to see all those messages: that they're in the middle of every conversation.

Data takes can take ten hops or more through strangers' computers to get from one place to another online.

Cheap, simple tech can be easier to protect than expensive new tech.

Pen and paper can be safer than tech.

There's value in using the same systems as everyone else.

Learning to think about where the weakest link is in your security, and concentrating on that.

(Freddy M)
"What is the Internet" is a good one.

Twitter responses:

Jillian York:
“This probably only works for communities already versed in the concept, but that digital security is about harm reduction.”

Jeremy Tribby:
“Threat modeling is figuring how much armor you should wear.”

Fred Jennings:
“It seems obvious, but at trainings I've done for non-technical folks, the biggest "aha" tends to be the idea of security as an environment/system rather than a single magic-bullet product.”

Dan Bateyko:
To the dreaded "I have nothing to hide" canard: It's not just your privacy that you're protecting—it's the privacy of everyone you talk to.”

Rachel Weidinger:
“The idea that we have to make (and) evolve our own security was huge for me. Nobody is going to do it for me. DIY is only option for now.”

Yarthur?:
“Encryption isn’t a lock with a key; it’s a puzzle with a solution.”

Florencia Herra-Vega:
Your data flows through literal wires, or is screamed across rooms in the case of wifi, and people can eavesdrop on that.
Not everyone’s security goals are the same — for example, ephemerality might be essential to some but unexpected and damaging to others.

Franz von Weizsäcker

Email is like a postcard

Google and facebook are the world's two biggest advertising companies - they sell your data and eyeballs.

There are different types of security: State security versus IT-security.

An insecure phone network benefits both criminals and law enforcers.

Framings that we may want to cover:

What is a computer?

How does the Internet work?

What is malware?

What is a vulnerability? What do security researchers do?

What is an update?

What is encryption?

How do downloads work? How are files executed? What might this look like?

What is a browser? What is a browser extension?

How do you think critically about security news? How do you teach to think in a nuanced way about security to a beginner? What might security skepticism look like, and how can we teach it?