Recommending Tools

“I’ve heard that MagicCryptoEightBall keeps your pictures secure. Is that true?”

“What phone do you recommend?”

“Is Skype secure?”

“What VPN should I use?”

Participants in a digital security training often have very specific questions about what software and hardware they should use. To an attendee, a direct answer to these questions is one of the quickest and most concrete benefits of a training.

Unfortunately, a quick direct answer that is accurate and useful is very hard to give. You should resist the temptation to give an absolute yes/no answer, even though that may be frustrating for you and your audience.

Straightforward answers are rarely correct for everyone. And if they’re correct now, they might not be correct in the future.

There are ways to make a less direct response easier to give and accept, however. You can ask questions back, and seek to tailor your answer to your questioners’ threat model. And you can give humble and non-technical but realistic explanations of how you came to your answer.

The Case Against Simple Answers

Take the answer to a frequently-asked question: “What phone do you recommend?” At time of writing, if locked in a room and told we could only leave if we gave a two-word answer, the answer we would give is probably, “An iPhone.” The Android market is currently fragmented, and Android phone makers are notoriously bad at providing security updates. Apple has a clear lead in building secure hardware and a good track

record of fighting off legal attempts to obtain the personal data of iPhone users. There are no equivalently secure open hardware, open-source solutions, and even if there were, we'd want to see how such solutions performed in real-life settings.

Each of these factors could change, and may change quickly. Google could shift their focus heavily toward security, or Apple's attitude toward law enforcement access could shift. Apple's institutional culture is secretive, so we have little insight into its internal decision-making policies, or the details of its hardware and software. A publicised flaw in the design of Apple's products could make all of its protections useless in the future. An unpublicised flaw might mean that none of those protections work right now.

Further, a suggestion to buy an iPhone may be alienating and unfeasible for some learners. iPhones are notoriously expensive, and such valuable hardware may make its owner a target for theft in some communities.

Based on all of these factors and more, our "confident, direct" answer is much more like a reasonable guess than a scientific, undeniable fact. We must acknowledge all of these factors and the way they change over time, because otherwise participants will be much more reticent to update that information (or listen to another expert) when the facts underlying a straightforward suggestion change.

Answers Can Change

As hard as it is to give useful digital security advice, it's even harder when you're trying to revise outdated but direct past advice.

A good example here is the answer to the question "Is Skype secure?". There was a time when Skype was one of the more secure options for messaging and video chat. But over time, changes in infrastructure by Microsoft, the lack of a published and audited description of the Skype protocol, the known targeting of Skype by state actors, and the growth in better alternatives has changed this answer. The correct answer was never, "Yes, Skype is absolutely secure." The answer now is not quite, "Skype is always insecure!" either. It does remain better than using text messages, and—if you're being targeted by someone other than the United States and a handful of other major state actors—better than a phone call. The frustrating answer remains: it depends.

People want a direct, yes/no answer. But when (not if) conditions change, it's much harder to persuade people to follow a new recommendation if they were not told the reasons for the old one.

How To Make “It Depends” Sound Okay

In an ideal world, the best thing you could teach your attendees is not a list of absolute facts about digital security, but strong intuitions about what the right answer might be, and an ability to ask follow-up questions that can pin down that answer more accurately.

To that end, here’s a good way to structure your answer:

- **Make it personal, not technical.**
- **Explain your thinking.**
- **Give a recommendation anyway.**
- **Give the audience a place to look for deeper explanations and updates.**

Make it personal, not technical

First, make it clear that this is your opinion, not a voice from God. ”I don’t think anyone has an absolute answer for that which works under any situation, but here’s what *I* think.” “There’s not an easy answer to this question.” And of course the old favorite, “It depends.” This gives you a chance to walk the audience through your thinking, which in turn gives you a chance to explain how the advice might be incorrect, while conveying some of the intuitions you’re using.

The advantage here is that the authority to your advice comes from your explanation, not from your position. That means that if your audience gets conflicting advice from another source, they’ll look for explanations from that source, too.

Explain your thinking

The biggest intuition we use is to threat model, so it’s useful to repeat that. For example, an explanation that takes this into account could sound like:

“If I was trying to decide which phone I’d use, I’d be thinking about a number of different aspects. First of all, what’s my threat model? If I’m worried about someone who could send me malware, I might want to avoid a fancy smartphone entirely. A cheap feature phone won’t contain much information, and is hard to remotely control. If I was worried about a state actor who could control the local telephone network, I might want

something that could let me securely communicate with others, so I'd probably want a smartphone that could use Signal or WhatsApp."

Give a recommendation anyway

Most audiences won't be happy with just hand-waving. They will want some answer, even if it's couched in very general terms. If you've shown your work, and you've made it clear that this is just a personal opinion, you can give them the answer they'll use:

"My current impression is that the average iPhone is less often successfully attacked than the average Android phone."

Hopefully it goes without saying that this may not be the right advice for the reader of this article or the people you teach!

Give the audience a place to look further

You've now empowered your attendees to understand your thinking, and take away an actionable morsel of practical information. But for that information to continue to be useful, you should give them resources that let them keep that knowledge up to date.

"If there's a big security problem with iPhones, it'll be headline news, so keep an eye on tech news sites like Ars Technica or just by typing "iphone" into Google News.

If you're in regular contact with your audience, you might want to forward them any news that has caused you to change your opinion, with a note as to why.