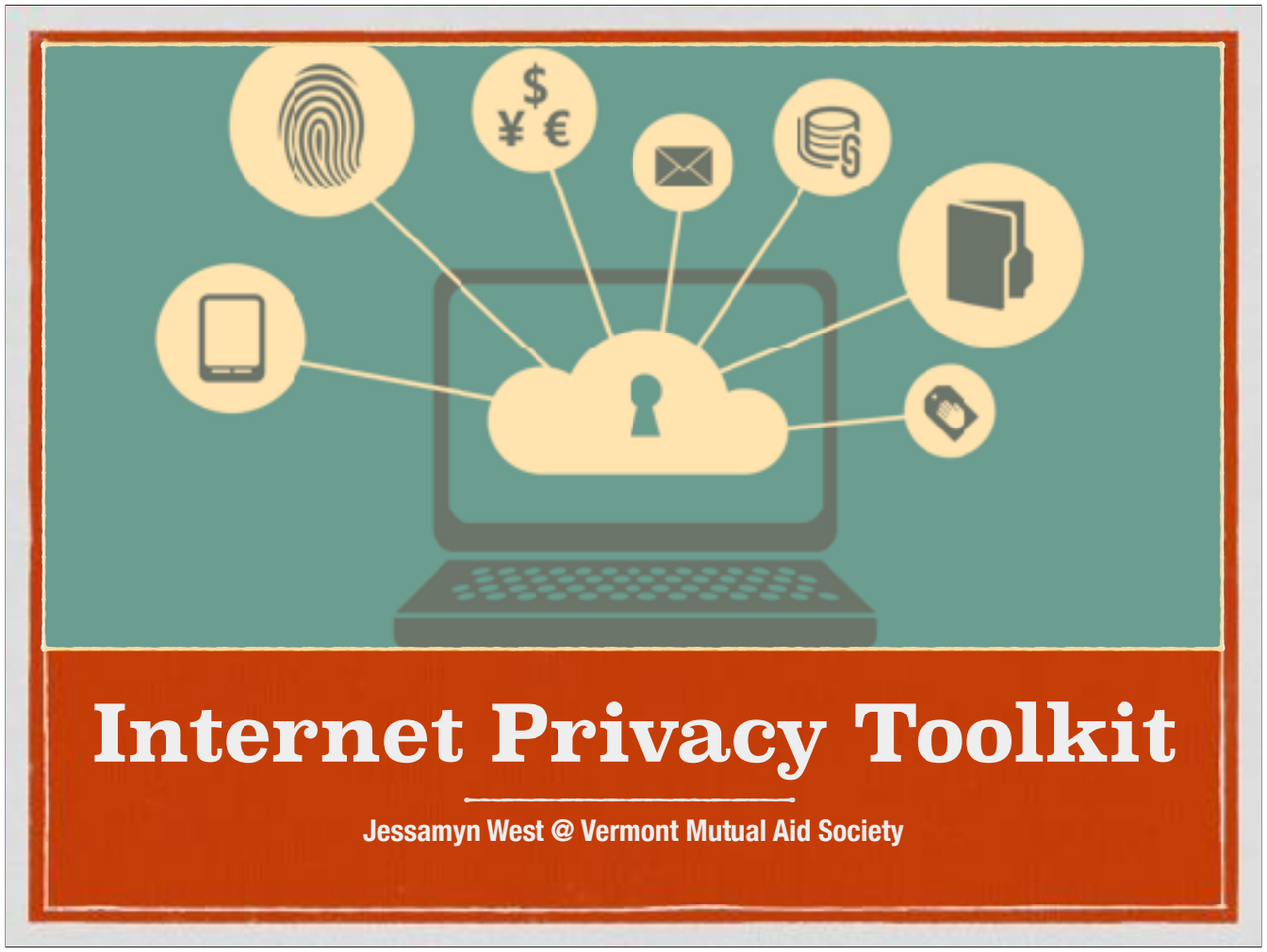
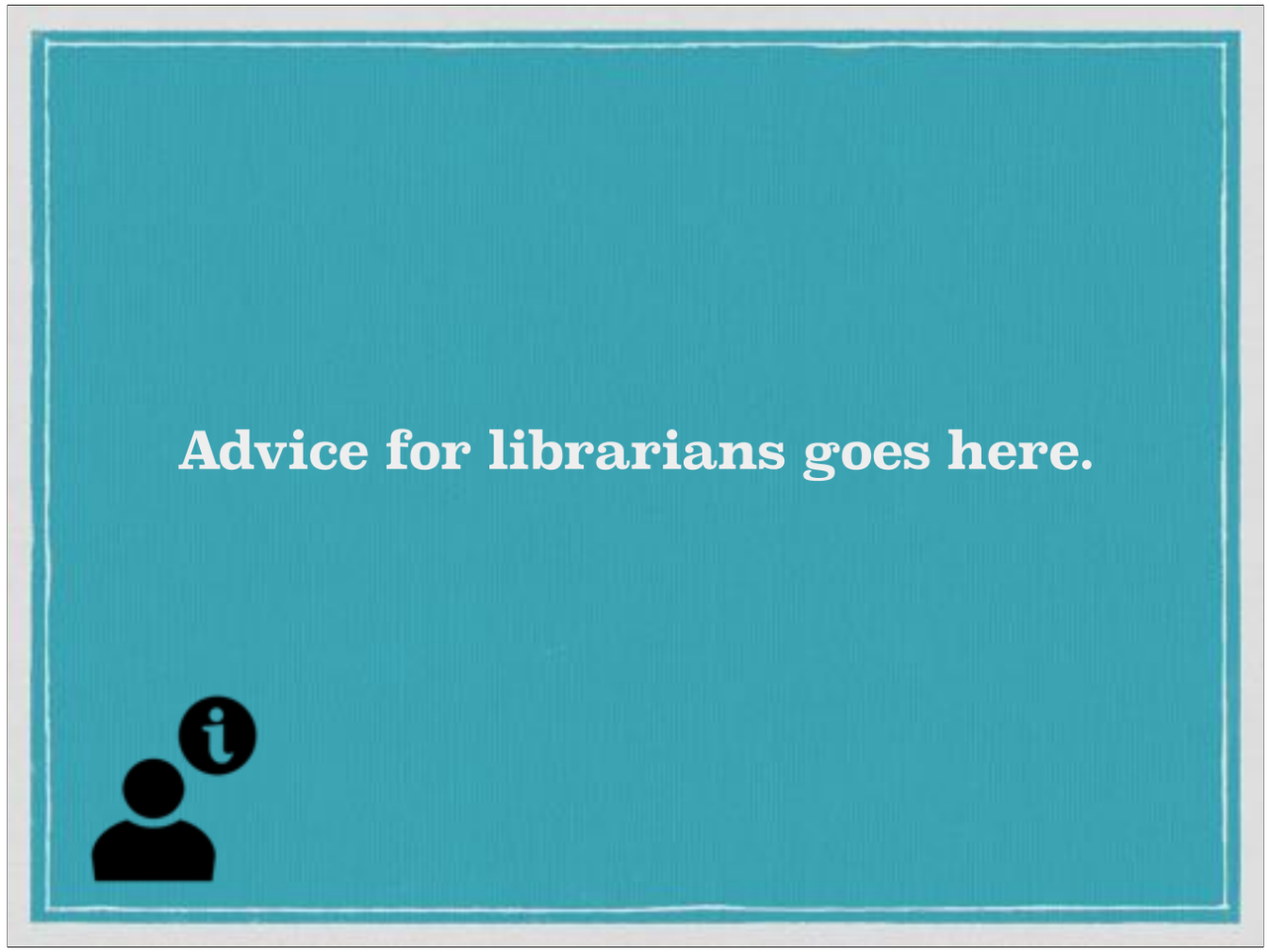
Hi and thanks for having me. I'm going to talk about some of the things we've seen and things we have to think about in 2021 with privacy, particularly digital privacy, specifically as it relates to libraries. I'm going to do this using a format I use to give basic privacy talks at small libraries in Vermont, so its sort of a talk within a talk. Links to more information about every resource I mention is at this address. There is also a printable shareable Google doc on that page.



This is what my privacy toolkit looks like. Basic slides with a lot of backgrounder information for people (usually in the form of a print handout). Things people can think about. The goal is not to get them all 100% private by the end of the day, but to give them the information they need to make the choices that are RIGHT FOR THEM and their personal environment.



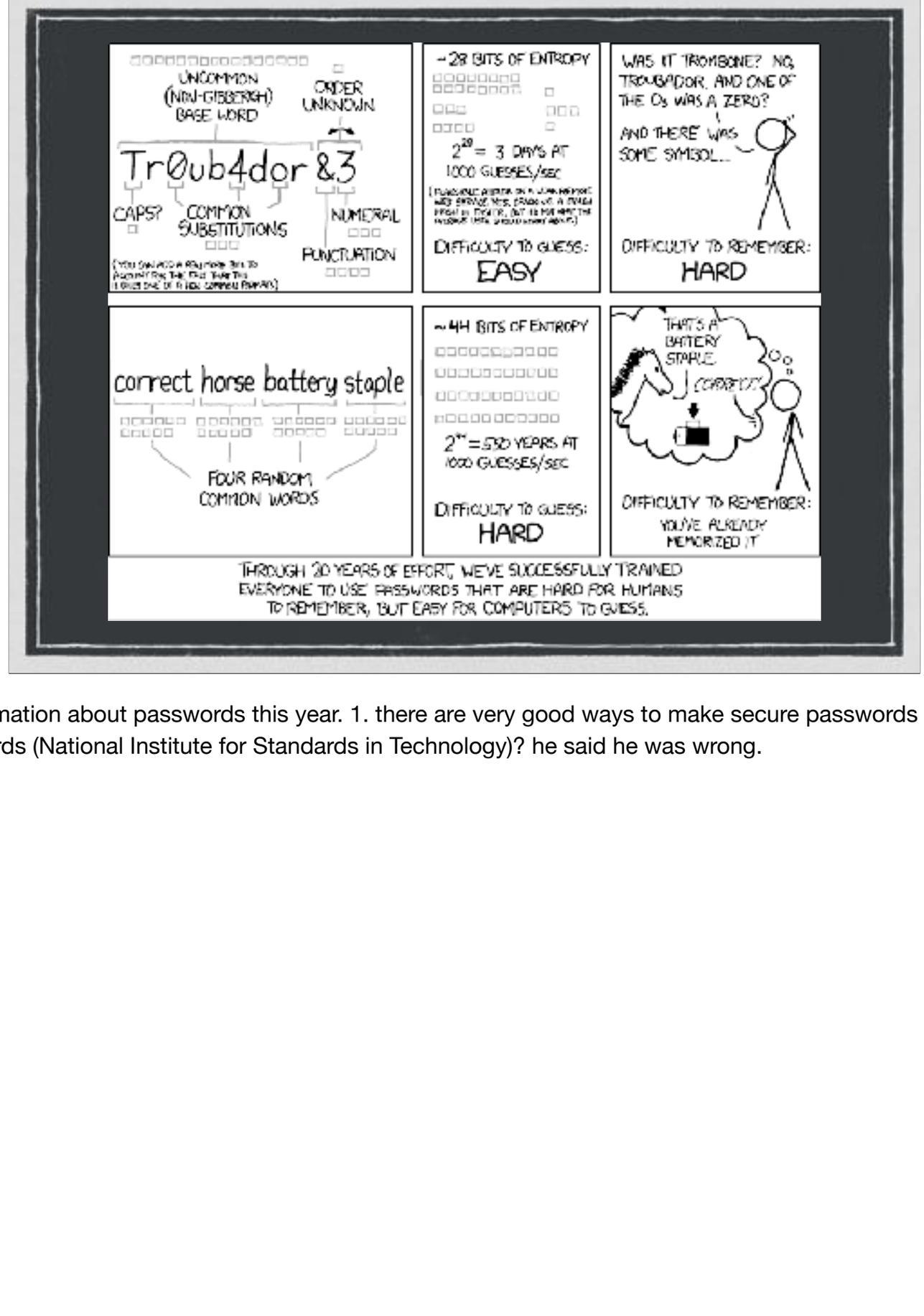
As I go, I'll add notes for librarians who may be thinking about giving similar talks about these topics. You can also grab the slides without the librarian notes.

This is the format I use to cover this stuff. The big deal is, as always, we don't have all the answers. So giving people places to go for more information—preferably to things *in your collection* as well as to things online—is a crucial part of this. I've seen libraries do great hands-on privacy workshops, helping people get their email or facebook accounts more secure, for example.

I said five steps but I mean five and one to think about. In the "info sec" world you always start here. How secure do I HAVE to be? Because there's really no such thing as perfect privacy especially in the internet age. So we need to make reasonable choices. What choices you make depend on who you are. So I ask people to think about this and I ask you to. Keeping patron information secure is our legal AND ethical obligation, but not everyone needs to be held to this standard. (aside, being a kid, fearing kidnappers)

Help people assess and maybe talk about the fact that this is different for everyone. It's also great to put in a pitch for the library's privacy policies and state alws helping patrons keep their library information secure.

Passwords are supposed to, or were originally supposed to, be memorable. But not too memorable. Our current best practices about passwords includes the long-complicated one number, one letter, one special character blablabla. But you know what? That wasn't practical. It made people choose one password and never change it. Or rotate two or three. Or increment them with the year's date. Or other less-secure things. And I know this goes against the grain but I say WRITE THEM DOWN. People get nervous about this, but for the average person at home this is safer than one password you never change. If you work in a library, consider a password manager app. Many are quite good.



There are two important pieces of information about passwords this year. 1. there are very good ways to make secure passwords that are also memorable. 2. that guy who made us make all the bad passwords (National Institute for Standards in Technology)? he said he was wrong.

Why to not reuse passwords (too much)

"Here's what I do."

Refer back to threat models

The best techniques are ones people will actually use.

2. internet traffic

Private browsing vs. Public wifi.

Online banking/medical stuff.

Look for HTTPS.

Advanced: VPN or TOR.

Our users don't always know the difference between different types of security. So there's being private in your browsing and being private over your networks. (explain) There's also being more secure about stuff that is more important… I saw a great talk at WLA about TOR (browser and network) and the best part of it was that it was given by a woman who was an older reference librarian at Marquette. People paid more attention to her because she was like them so her advice resonated more clearly.

The biggest deal people will encounter is browsers starting to "call out" pages that don't have https:// especially ones that have data entry areas. Know what it means, know how to look for it. The good news is that many companies are starting to offer this with their web hosting. The bad news is that some aren't And we should be asking for it.

Offer secure browsing & browser choices

Secure your own networks

Keep browsers clean and safe

So keep track of the https

3. listening& recording devices

If it's not online, it can't spy on you.

Anything that listens for your voice is actively paying attention.

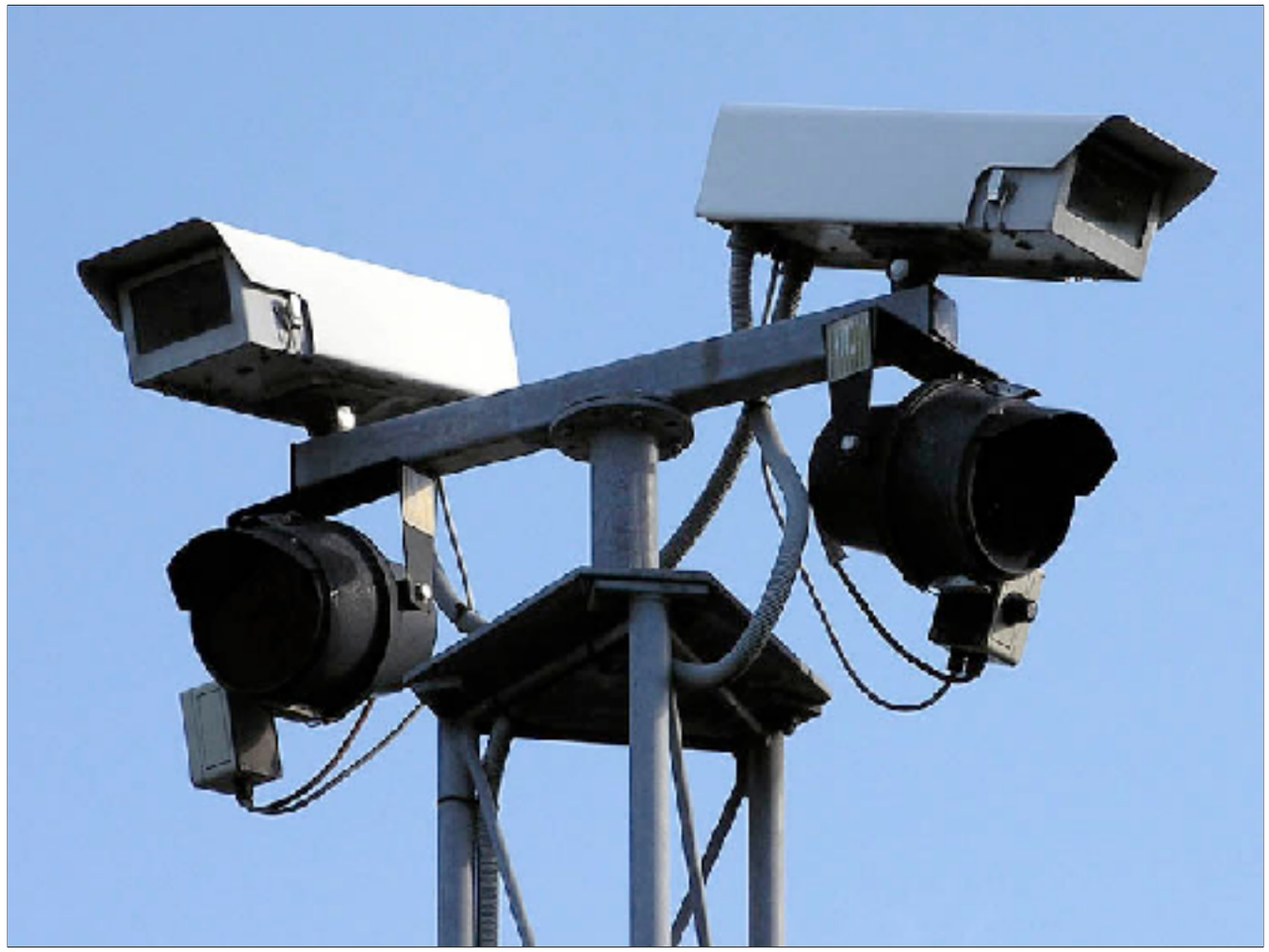
Siri, Alexa, Google, your tv…

There's a lot of talk about the Internet of Things and many people have these smart devices but aren't really sure how they work, how much they listen to, or what is done with that information. It's helpful to be able to answer questions, especially basic ones. Sometimes this puts people's minds at ease, sometimes it just tells them what to be mindful about.

"Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition"

- Samsung

Samsung warns users about this with their Smart TVs.



Many larger libraries have cameras as part of their security system. I was at a library in Massachusetts recently and saw this. And started a conversation with people about whether these signs are agreeing or conflicting.


THIS
LIBRARY
IS A
SAFE SPACE
FOR ALL
NOTICE
VIDED SURVEILLANCE
IN USE ON
THESE PREMISES

Cameras have privacy as well as safety implications.

Be mindful of your internet of things acquisitions.

Informed consent as much as possible, help users make choices that work for them.

4. tracking

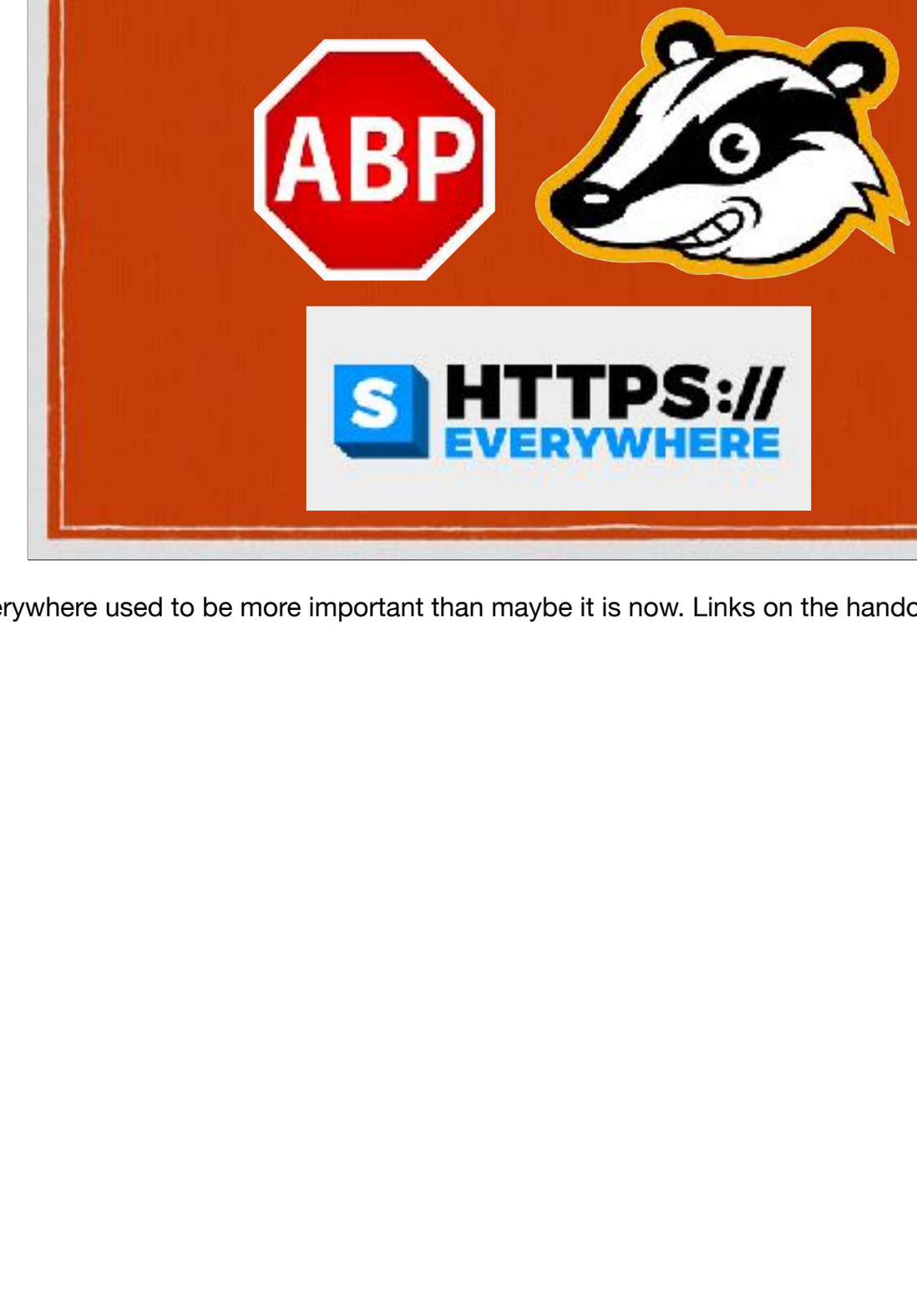
Review your browser settings.

Browser plug-ins are simpler to use than you think.

Don't keep all your eggs in the Google basket. Or any basket.

Ever since the General Data Protection Regulation went in to effect, people visiting sites that serve Europe or an international audience are having to make affirmative acceptance of site cookies, but do people know what they are yet? (my story about my eBags purchase). And do they know what choices they really have? The biggest deal here is explaining to people that their browser environment is adjustable and that there are privacy-forward plug-ins that they can use that do not require more skills than clicking. I do a live demo of this in the talks just to drive this home,. Try it yourself if you haven't used Ad Block Plus or something similar before.

Tools are easier than they were



Here are a few basic ones. HTTPS everywhere used to be more important than maybe it is now. Links on the handout.

Software is malleable

Facebook, Instagram and Twitter are all tools that can be adjusted either using their own internal settings (i.e. choose who can reply to your images on Instagram, keep Nazis out of your Twitter) or add-on tools like FB Purity (alas, not for mobile)

If people do Only One Thing. You can change all your browser's search engines to this one. Nearly the same as what Google wold be if it weren't relying on personal information you probably didn't give it to give you results. I still hop oevr to google for social results and when I'm looking for CC images but that is mostly it.

The biggest part is to know that there are answers. EILI5 can be a good search term if you're learning, it means "Explain it like I am five"

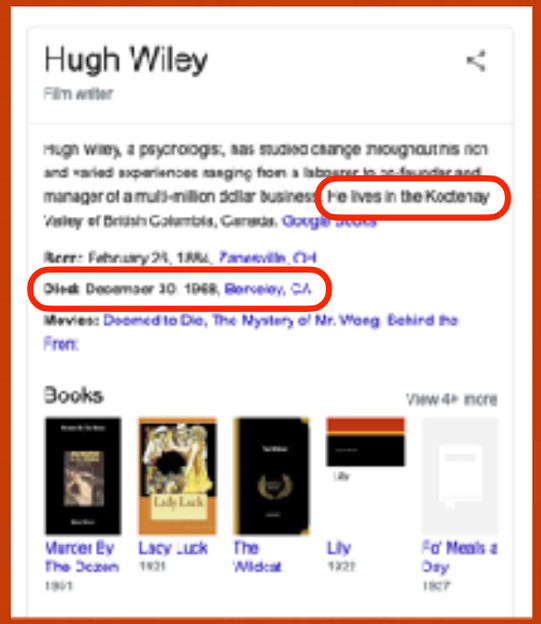
5. trust but verify

Not so much "fake news" as "Where does this news come from?"

Don't click on mystery email links.
Don't call numbers you see in pop-ups.

Know how to see where a link goes.

Advanced: tell your friends, report what's wrong.



How much do you know about cybersecurity?

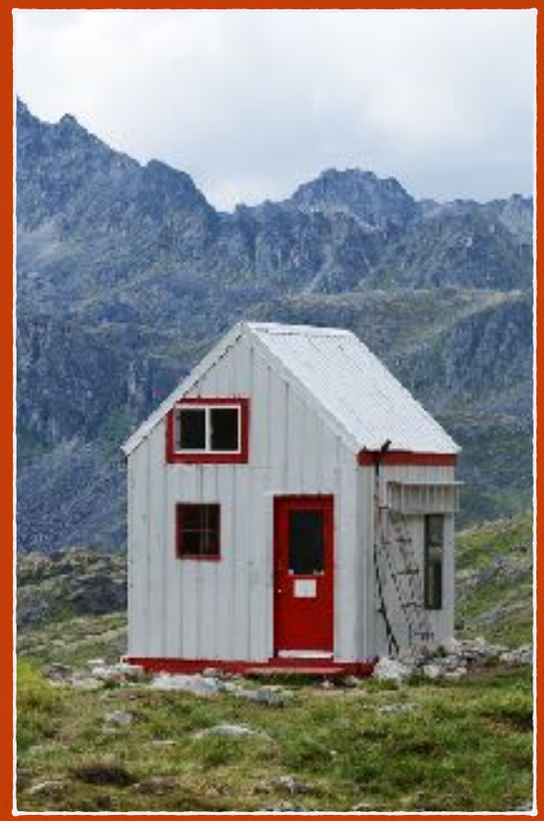
Test your knowledge on cybersecurity topics and terms by taking our 10-question quiz. Then see how you did in comparison with a nationally representative group of 1,055 randomly selected adult internet users surveyed online between June 17 and June 27, 2016. The survey was conducted by the GfK Group using KnowledgePanel.

When you finish, you will be able to compare your scores with the average American and see explanations for the terms and topics in each question. The analysis of the findings from the poll can be found in the full report, "What the Public Knows About Cybersecurity."

Learn to live with imperfect privacy.

But don't let that stop you from trying to do better.

Help people feel good about making informed privacy choices.



Your confidence helps

Places they can learn more

"You're on the right track"

Get your reality checked @ your library

Librarians can help you or refer you to people who can help.

jessamyn@gmail.com

librarian.net/talks/privacy

KIMBALL FREE PUBLIC LIBRARY—RANDOLPH.