Computer Security for the Everyday User

100 minutes

Materials: *Agenda of training written up, handouts, markers, butcher paper & tape, cards at the end of the training all cut up, about 40 small blank pieces of paper for activities, and pens.*

Introduction - (5min)

- *[Introduce trainers.]*
- This training will teach you how to protect your data with good security habits
- You don't have to be a computer geek to be very secure in your computer use. In fact, geeks often have *terrible* security habits
- There are other things you should think about, like the physical security of your computers, and people tricking you into giving your password. We don't cover those issues in the training, but we're happy to talk about them afterwards**.**
- We love answering questions. But since we're covering a lot of ground, take a peek at the agenda before asking to see if we're going to address your point later.
- We're passing out a handout at the end, so don't feel like you have to take notes.
- Go 'round: What do you want to get out of this training? [*Write down answers on a piece of butcher paper. We come back to this at the end of the training]*
- Our goal is give concrete skills for people to improve computer security. This info won't make your data 100% safe, but if someone wants to get at your data, they'll really have to work at it.
- *[Review the agenda for this training]*

Introduction to Computer Security - (5min)

Why is computer security important?

- [Brainstorm] Who might try to get access to your data? Why?
  - Criminals, cops, feds, teen hackers, bored co-workers, your mom, rival organizations, private companies thwarting activist work...
- We call anyone who is trying to access, use or destroy your information without your consent "adversaries."
  - This is different than "enemies." Adversaries might not have anything against you personally. In the case of random hackers, they might not even know who you are.
- Anecdote: For basically all of 2003, the Republican in Congress were able to spy on all the email traffic of the Democrats. They successfully leaked the Democrats' internal memos and foiled their strategies. This went on for about a year before it got fixed.
- We think computer security is especially important because the less access adversaries have to your data, the safer we all are from COINTELPRO tactics and criminal charges.
- The same goes for foreign governments whose policies we protest (like China) or private security hired by the people we're campaigning against
- Protecting digital information is important because it's really easy to search it for incriminating information - much faster than going through paper. Also, a few hundred million more people have access to the data on your computer (via the internet) than have access to the paper records in your house.

- A perfectly secure computer is one that is disconnected from the internet and unplugged from the power outlet. That is to say: Computer security is a compromise between usability and security.
- We think good security habits are more valuable than technical ability or software tools, so that will be the focus of this training (though we do include *some* tech stuff). There is a geek adage: "If you think technology can solve your security problems, you don't understand the technology and you don't understand the problem."

Secure Passwords - (40min)

"Size matters."

What passwords protect

- Brainstorm: What do you use passwords to protect? [Your computer login, network, access to your email, ATM card, cell phone, PDA, online banking, wifi...]
- Have you ever had a password "stolen" - or stolen someone else's? Discuss.
- Anecdote: A friend once had the password to the super privileged account for all computers in the California State University system. That's 100's of thousands of users! With that account they could eavesdrop on anyone and they did!
- Your password is usually, by far, the weakest link in your computer security. The goal is for it to not be the weakest link.

Exercise: Password 20 Questions

- A participant chooses a short, single word password (10 characters or less), writes it down, and everyone else plays 20 questions to guess it. *[Note: A trainer should look at the password and make sure it's simple enough to guess.]*
- Trainers pass out "20 Question Cards" to anybody who wants one. (see cards at end)
- "It took us a few minutes and we (almost) got the password. On average, a computer can ask far over a million questions a second."

There are programs that can do the exact same thing to discover your passwords:

- They can try every word in the dictionary in under one second.
- Then they can try dictionary words with common susbtitutions (a zero instead of the letter "o," etc.)
- Then they can try every pop culture reference, every famous movie quote, every simple combination of short words, etc
- If they know you (or can see your Facebook page), they'll try personal info (name of pet, birthday, zip code, etc.)
- If all that doesn't work, they can do a "brute force" attack: they try every combination of letters, numbers, and characters. This is what you want them to have to resort to. With current technology, if your password is long enough, it will take them so long to do this that it's effectively impossible. We'll talk more about this in a minute.
- There are always other ways of getting at your data - like stealing your computers - but cracking someone's passsword is usually the easiest way to get someone's data.

Brainstorm "What makes a good password/passphrase?" list on butcher paper

- We suggest using a "passphrase": A password between 10 to 100 characters long.
- *Do Not* use pet names, birthdays, etc
- *Do Not* use dictionary words, famous quotes, movie titles, song lyrics, etc
- *Do Not use* simple substitutions (1 for i, 0 for o, 4 for a. Example: phooey becomes ph00ey.)
- *Do* use a mix of upper and lower case, use some characters other than letters (numbers, punctuation)
- *Do* make it something you can remember. Using nonsense sounds or mnemonics helps.

- Make your passphrase about 25-40 characters if you're using English words with the tools we described above. At this length, it should take about 10-15 years to break your password (barring huge advances in technology or a very lucky computer).
- Generally, the more your passphrase looks like something a normal person could understand, the easier it is for a computer to guess it.
- If you look at your passphrase and think, "That looks pretty messed up," you're probably on the right track. The shorter it is, the more messed up it has to look.

Exercise: Making strong passphrases – 5 minutes
[In pairs or teams, participants create a strong passphrase. Participants bounce ideas off each other and come up with one passphrase per pair/team. We then come back together to share passphrases and briefly critique them. Then the group picks 1 and works together to make it better. (This may include making it more memorable.)]

Now that you have a great password:

- Don't share it with friends – they may not have your good security habits.
- Don't give it to a stranger (tech support almost never needs your actual password to do their job)
- Do use different passwords for your serious stuff (i.e, credit cards, etc) than for stuff you don't care about (i.e, NY Times online subscription)

Data Creation and Retention - (20min)

"If you don't have it, they can't take it."

Most of us keep a ton of old information on our computers that we'll probably never use, but could be used against us by our adversaries.

Subpoenas

- If the government wants your info, they'll probably give you a subpoena instead of dealing with tricky wiretapping.
- A subpoena is a court order to do something, usually to show up in court with a bunch of documents.
- Subpoenas are commonly used in criminal and civil cases.
- If you get a subpoena requesting every e-mail you've ever sent or every document you've ever written, the first thing you should do is get a lawyer to help you fight it.

- It may be tempting to destroy a bunch of information after you get the subpoena, but if you do, you can get screwed.
    - There are criminal penalties for destroying evidence. (In California, it's up to a $1000 fine and 1 year in jail; it's bad in Federal court, too.)
    - You're likely to become a suspect in the investigation, and you could even get convicted of a crime you were never involved with in the first place – just because you destroyed information that may have been related to it.
    - Like Bill Clinton discovered, it's not the crime, it's the cover up.
- However, if you destroy the data before you get a subpoena, you generally don't have anything to worry about.

Hat share!

- [Pass around pens and slips of paper.] Lots of people have private information they keep on their Desktop for no good reason – for example, how many people keep all their old emails? What are some other types of data people might keep long after it's useful to them? *[Have everyone write one category of data & put it in the hat.]*
- [While people are writing their hat shares:] Big corporations delete their old records as soon as they legally can. That way when people sue for getting hurt by their products and send them a subpoena for everything about those products, the corporations can say, 'We don't have those records anymore.' If big corporations destroy their incriminating documents, we should use the same tools to destroy corporations.
- [Now look in the hat] How hatshare data can be used against you:
    - Financial: Credit card info, donor info, QVC login, etc.: Criminals can steal it.
    - Passwords for other systems: Compromises those systems.
    - Browser Cache & Cookies: Shows what you've been doing on the internet.
    - Info about political actions: Associates you with those actions.
    - Social Security #s: Steal your identity or do background research on you.
    - Meeting Notes: Gives adversaries an idea of your situation and future plans.

Lessons:

- The only time you have total control over your information is when it's only in your head. If you don't absolutely need to put it into a computer, don't.
- If you do put it into a computer, delete it as soon as you don't need it on there anymore.
- This is about good habits, not being high-tech.
- This is useful for subpoenas *and* when the cops just come into your house and take your computer.
- Don't forget about other places your information lives – CDs? Flash drives? Old laptops? On paper? You should be thinking about data retention for all these things.

Homework: Go home and pretend you're about to get this terrible subpoena and destroy everything it's going to ask for.

E-mail - (20 min)

"Like a postcard, but less private."

E-mail exercise

- You and your friends here are planning a protest against a local ROTC recruiting office. You're going to email each other to help plan the protest.
- *[All participants get a Roleplay Card (see cards below). They write a short message, then "send mail" by trading with their neighbors. When everyone's finished, they read the email they got and pick an Internet Card (see cards) from a hat and tell everyone what happened to that email.]*
- Wrap-up: The problem with email is that you write something stupid, send it to ten people, and each of them forwards it to ten more people, and your bad email ends up on a thousand different computers of (mostly) random strangers.
- Email is insecure. This makes bad habits worse. Brainstorm bad email habits (on butcher paper) and possible/likely consequences:
    - Divisions in the movement/gossip can be used for COINTELPRO.
    - Anything illegal or semi-illegal can wind up in the Feds' hands.
    - Any stupid exaggerations made ("I'm gonna crash a plane into Chevron;s headquarters.") can make you a target of investigation.
    - Shit talking can be revealed to your adversaries, and your private language made public.

Good Email Habits:

- Don't do any of the email bad habits we came up with.
- Don't type anything into email that you don't want to hear during a trial against you or your friends 5 years from now – or read on Indymedia.
- Before hitting the send button ask yourself, "Should I really send this?"

Software/Web Stuff:

- Microsoft Outlook sucks. Don't use it. It has a number of privacy and security flaws that leave you susceptible to viruses and attacks. Try using Thunderbird or Eudora, both of which offer similar features and are free.
- A lot of people use Gmail and other free "webmail" for their email. When you sign up for them, you agree to let them save your email and use it for almost anything they want – you give up almost any expectation of privacy. And these corporations won't think twice about handing over your email to the government. If you want more secure email, try hushmail.com and ziplip.com, or webmail based in other countries. (The government can't subpoena them as easily.)

Evaluation (10 min)

- [Pass out the computer security handout]
- [Review questions people had from the Intro part of the training]
- What's one thing you learned in this training that suprised you?
- [Write down] What did people like about the training? What could we do differently?

Role Play Cards - *Use the bold-faced cards first*

You're very curious. Write a two sentence email asking another member of the group about how their green card application is going.

You're a hard core militant. Write a two sentence email about how the group needs to be more militant and use more destructive tactics.

You're very curious. Write a two sentence email asking another member if they were able to sell the heroin they had in their car.

You know some juicy gossip. Write a two sentence email about how a rival group is going to join the Republicans.

You've just broken up with someone else in this group. Write a two sentence email about what a terrible person they are. (Don't make it too personal. It's just a training.)

You are Yahoo.com. Write a two sentence spam email about a weight loss program or about joining Yahoo.

You're really pissed off by the government. Write a two sentence joke email about how you're going to crash a plane into a government building.

You've got the inside scoop. In a two sentence email, reveal to your friends that Julia Butterfly Hill is probably a cop.

You're a long-time activist. Write a two sentence email about how this action reminds you about a time when you broke the law and totally got away with it.

You're mad as hell about the ROTC. Write a fiery, in-the-moment two sentence email about how we should blow them up for a change.

20 Questions Cards

Is it a word in the dictionary?	Does it have to do with your work/activism?
Does it start with a letter in the first half of the alphabet?	Is it a noun?
Is it more than two syllables?	Did you make substitutions (like changing o's to 0's or i's to 1's)?

Internet Cards - *Use the bold-faced cards first*

Nothing happened to it.	Your mom read it.
It got posted to Indymedia.	The Hotmail.com staff read this.
The FBI read this.	Your activist friend saved this to his hard drive.
It got posted to a random listserv.	Yahoo.com saved a copy.
Your boss read it.	The FBI read this.