Computer security for the everyday user

v2.0
6/19/04

Materials: Hat, Handouts, Markers, Butcher paper & tape, 20 Questions cards, Email roleplay cards, Internet cards, about 40 small blank pieces of paper for emails and hatshare, pens

Intro to the training (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 to worry about, like physical security of your computers, and people tricking you into giving your password. We don't talk about those 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.
- Go 'round: what do you want to get out of this training? [Write down answers on a piece of butcher paper.]
- 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.
- Agenda Review on butcher paper

Introduction to Computer Security (5min)

Why is computer security important?

- Brainstorm who is trying to gain access to your info and why. [Criminals, cops, feds, joyriders, bored co-workers, your mom, rival orgs, private companies thwarting activist work, etc.]
- Anecdote: For basically all of 2003, the Republicans in DC 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, MSLC, think computer security is especially important because the less access the cops & feds have to your data, the safer we all are from COINTELPRO tactics and criminal charges. [if necessary, define COINTELPRO: An FBI program aimed at attacking dissident political organizations in the US in the '60s and 70's]
- 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 unplugged 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? [Login to your computer, login to your network, access to your email, atm card, online porn subscription, etc.]
- 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.

Define passphrase: A passphrase is basically a really long password (on the order of 10-100 characters).

Password 20 Qs

- 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)
- "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 every dictionary word with common susbtitutions (a "0" instead of an "o," etc.)
- Then they can try every pop culture reference, every quote, every simple combination of short words, etc
- If they know you (or can look through your trash), 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 the 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 breaking someone's passsword is usually the easiest way to get someone's data.

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

- *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 syllables or mnemonics helps.

- Make it 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 a something a normal person could understand, the easier it is for a computer to guess it. So if
- you look at your passphrase and think, "That looks pretty messed up," you're on the right track. The shorter it is, the more messed up it has to look.

Exercise

- [In pairs or teams, participants brainstorm 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 cops or in court.

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.
- If you get a subpoena requesting every e-mail you've ever sent and every document you've 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 (roughly speaking, penalties in California State court are up to $1000 fine and 1 year in jail , and in Federal court, it's much more complicated than that, but it ain't good.)
    - 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.
- However, if you destroy the data before you get a subpoena, you don't have anything to worry about.

Hat share!

- [Pass around pens and slips of paper.] Lots of people have information that should be private and keep it around for no good reason – for example, how many people keep all their old emails? What else? [Have everyone write one category & 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 old incriminating documents, we should use the same tools to destroy corporations."
- How hatshare data can be used against you:
    - Financial info - credit card info, your donors, qvc, etc. : criminals can steal it
    - Passwords for other systems : compromises those systems
    - Browser cache and cookies : shows where you have been on the internet
    - Info about political actions : associates you with those actions

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 possible.
- This is about good habits, not being high-tech.
- This applies for subpoenas *and* where the cops just come into your house and take your computer. .
- Don't forget about other places your information lives – CD-ROMs? Backups? On paper? You should be thinking about security 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) . 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 stupis exaggerations made ("I'm gonna crash a plane into the FTAA building in Miami.") can make you a traget of investigation.
    - Shit talking can be revealed to the wrong people, and private language made public.

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 5 years from now, or read on Indymedia.
- Before hitting the send button ask yourself, "Should I really send this?"

Tech

- Microsoft Outlook sucks. Do not use it. It contains a number of privacy and security flaws that leave you susceptible to viruses and attacks. It is configured by default to open attachments and run things you don't want to run. Try using Mozilla Mail or Eudora, both of which offer similar features and are free.
- A lot of people use Hotmail and other free "webmail" for their email. These are big corporations that won't think twice about handing over your email to the government. If you want more secure email, try hushmail.com and ziplip.com, as well as webmail based in other countries. (The gov't can't subpoena them as easily.)

Evaluation (10 min)

- Give out handouts
- Get pluses and deltas
- Review questions people had from the Intro part of the training
- Ask people for one thing they learned in this training that suprised them.

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 the Ruckus Society is going to join the Sierra Club.

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 Bush administration. Write a two sentence joke email about how you're going to crash a plane into a 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 reminds you about another time you totally broke the law and 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.