Computer Security for the Everyday User

Intro

Almost all of us use computers in our political work. So it's amazing that so few of us have good computer security habits. This handout and our Computer Security training will give you the basics you need to protect your data from anyone who's trying to go after it.

Computer security is important because it's really easy to search digital information for anything incriminating – 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 you house. We think computer security is especially important because the less access the cops & feds have to your data, the safer we all are from COINTELPRO[1] tactics and criminal charges.

This handout covers some basics of computer security[2]. It explains the best first steps to protecting your data. Good computer security is based on having good habits – especially around passphrases, data creation and destruction, encryption, and email. You don't have to be a computer geek (in fact, computer geeks often have terrible computer security), and you don't need the most expensive hardware and software.

A perfectly secure computer is one that is unplugged from the internet and unplugged from the power outlet – it's unusable. That is to say, **real computer security is a compromise between usability and security**. It's more important to have good security and use it (and know your weaknesses) than to have amazingly great security that's too much of a bother to actually use.

Secure Passphrases

"Size matters"

Passwords are your first and only line of defense for a lot of your information. You use them to access your e-mail, your network, check your voicemail, use the ATM, etc. A passphrase is just a password that's two or more words long.

The Basics

There are many programs that can crack passwords. In a matter of minutes, they can try every word in the dictionary, every word using common character substitutions (like '3mma g0ldman'), every band name, famous quote, and pop culture reference. Also,

1 An FBI program aimed at attacking dissident political organizations in the US (http://en.wikipedia.org/wiki/Cointelpro)

2 Caveats:

a) Technology changes quickly, so assume that the specifics in this handout are suspect after January 1, 2005.

b) Security is actually a very complicated subject. If you're going to have comprehensive security, your defenses depend on who your enemies are and how they're likely to attack you.

c) Physical security is another important security issue, and is outside the scope of this handout

anyone with access to your trash will probably try your pet's name, your favorite sports team, your daughter's birthday, etc.

And if *that* doesn't work, it's still possible to use brute force and try every possible combination of letters, numbers, and symbols. This is what you want them to have to resort to. The idea is to make your password good enough so they'll have to use brute force, and that your password will be long enough that a brute force attack will be take years to succeed.

Looking at it that way, it's easy figure out what makes a good passphrase. Some tips:

- **Do Not** use pet names, birthdays, etc
- **Do Not** use dictionary words, famous quotes, movie titles, song lyrics, etc
- **Do Not** think that simple substitutions will help (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 good and long. (See below)
- **Do** make it something you can remember. Using nonsense syllables or mnemonics helps.
- **Do** make the password as random as possible. You can increase randomness by:
  - mixing upper/lowercase;
  - putting weird characters in the middle of words;
  - not starting with a capital or end with punctuation.

As a rule of thumb, if you look at your passphrase and think "that looks pretty fucked up," you're on the right track.

Good examples

Roostaz dinna l&y no 13 &ggz.

- 29 characters
- & substitutes for 'a' once and 'e' once

,rUnning,jUmping !fAlling!

- easy to remember
- mixed up punctuation and capitals
- not a sentence

/7NYLe.60]iAx=L,4~

- nice and random
- (probably a little hard to memorize)

Bad examples

Big Brother is watching. (we actually used this!)

- only 24 characters
- common, obvious quote

H3y, d0n't g3t c@ught, d00dz!

- uses simple, obvious (to computer geeks) letter substitution

11/30/99

- way too short
- no letters, and just one symbol (the slash)
- obvious date to some people

Passphrase Length and Randomness

Random means you choose a character in an unpredictable manner, like by throwing dice (Here's an example that we made with dice: /7NYLe.60]iAx=L,4~) A shorter random string is as hard to break as a longer, less random string.

Make your passphrase about 18 characters if they are randomly chosen, 25-40 if you're using words with the tips we described above[3]. In either case it should take existing computers more than 149 trillion years to break using brute force! (The universe is currently only 15 billion years old.) With advances in technology, computers will eventually catch up, but you should have 10-15 years before folks can break your password. Generally, the more your passphrase looks like a something a normal person could understand, the easier it is for a computer to guess it.

Striking a Balance

Like we said, security is a compromise. The longer and more random your password is, the better it is, BUT the harder it is to remember and use. If you know you have a bad memory, use a longer passphrase that looks more like English; if your memory is good and you hate typing, use a shorter more random one. One solution is to come up with a nonsense sentence that's easy for you to remember, but impossible for anyone else to guess. Also check out www.diceware.com - it's a great website that helps you generate strong, memorable passwords.

The security of your passphrase is not absolute. It's relative to the strength of other people's passwords. (If someone wants to steal credit card numbers and doesn't care whose, then your password just has to be better than other people's.) It's relative to the amount of resources the bad guys have. (A shorter password is good against your kid brother but a longer password will be needed to survive the attempts by the Feds.) It's relative to the other pieces of your computer. (If your password is long enough and strong enough, people will find it easier to go after a bug in the software, or to call your friends to try to get the info, or to break in and steal your hard drive.) Ideally, you want your password NOT to be the weak link. It usually is.

Now that you have a great password, don't share it with others – they may not have your good security habits – and don't give it to a stranger (the person claiming to be tech support, working for your bank, or whatever). Also, don't use the same passphrase for everything. Specifically, don't use the same password for things that aren't important (on-line newspapers, etc.) that you use for things that are important (anything with your credit card, email, etc.) Often, if someone discovers one of you passwords, they will try to use to get into every password-protected service you use. Obviously, the more sensitive the data, the better your passphrase should be.

Data Creation and Destruction

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

Think about some information you have in digital form – saved email, documents, pirated mp3's, etc. – you don't want other people to know about. Take a second.

3 Some e-mail providers and older software only let you choose passwords up to 8 characters long. In those cases, it's even more important to use the other tips and to be aware of that weakness.

Because we create and save that kind of information almost every day.

Gerri Guerrilla has been doing a lot of organizing against animal cruelty. Recently, a local animal testing facility was bombed, and Gerri got a subpoena – (a legal order from a judge) – to hand over every email she's ever gotten about protesting, and every document she's ever written or received about animal rights. The prosecutor plans to send a grand jury subpoena to every person who sent Gerri any mildly "suspicious" emails and force them to testify before a grand jury. And if Gerri's computer has any documents on it that are too radical, she's going to be declared a suspect in the bombing.

So what can Gerri do? She can risk destroying any information she has, but if she gets caught, it's a serious crime – up to 1 year and $1,000 in California state court, or 1 year (plus a significant sentence enhancement) if she's in Federal court. In fact, the destruction of evidence alone might get Gerri convicted of a crime she wasn't even involved in. As Bill Clinton discovered, it's not the crime, it's the cover up.

Digital information is more dangerous than paper in part because it's so easy to search through. In the above example, Gerri's not a suspect – yet. But the police and courts want to harass her. So they'll probably just get her email and search through them for keywords like: bomb, fire, "fuck shit up," etc. Then they'll quickly compile a list of every e-mail address she's sent to or received from and search for names of individuals who they're already suspicious of.

There are actually a few steps Gerri can take after getting the subpoena – the first of which is to get a lawyer to fight it (narrowing the scope of what she has to turn over, etc). But Gerri and her contacts would be a lot better off if Gerri had erased all her old email she didn't absolutely need.

Here are a couple of rules of thumb around data creation and destruction:

1. **Don't write it down if you don't have to**. This is especially true around anything borderline illegal. Ditto for shit-talking people – the government was enormously successful in breaking up movements in the past by playing on existing divisions in the activist community.
2. **Delete it as soon as you possibly can**. We all have some sensitive information on our computers. The key is to delete it as soon as possible – like right after the action, conference, or meeting. If you can't articulate a reason for keeping something the slightest bit edgy, you should probably delete it[4].

   Big corporations delete old emails, memos and documents as soon as they legally can. That way, when people sue them and subpoena them for documents, they can say there aren't any. If big corporations do this to enrich themselves at our expense, we should do it to destroy big corporations.

3. **If you have to keep it, encrypt it.**

Once again, this is about good habits, not high tech. These habits will help protect you

4 Other sensitive info: credit card info, donor losts, passwords for other systems, etc. Don't forget backups, CDs, floppies, paper, and anywhere else this info might live.

in the case of police raids or 'sneak & peek' warrants, also.

Bonus!

Pretend you're about to be served with a terrible subpoena, and delete everything it's going to ask for.

Email

"Like a postcard, but less private."

Here's the problem with e-mail: You write something stupid, you send it to 10 friends, they forward it to 1000 more people, and now what you wrote (or parts of it, or stuff forged to look like yours) lives on 1000 different computers, as well as on the hotmail.com (or whatever service you use) computers. Also, while it's bouncing around the internet, anyone with the knowhow can read it, copy it, scan it for key words, etc.

This section will help you reduce the risk in using email. Here's a partial list of things you should always avoid in your email:

- 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 skin that fur company CEO and see how he likes it!") can make you a target of investigation.

Basically, don't type anything into email that you don't want to see on Indymedia or hear during a trial against you 5 years from now. Before hitting the send button ask yourself, "Should I really send this?" Also, like we said in the Data Creation and Destruction section, don't hang on to old emails, especially if they violate the tips above. I know you really need those 718 emails from 1999, but it might be time to do a little spring cleaning.

One more thing: Microsoft Outlook sucks. Do not use it. It contains a number of privacy and security flaws that leave you susceptible to viruses and hacking attacks. It is configured by default to open attachments and run things you don't want to run. Try using Thunderbird Mail (mozilla.org) or Eudora (eudora.com), both of which offer similar features and are free.

Computer Security

"If you think technology can solve your security problems, you don't understand the technology and you don't understand the problem."

There's a billion or so people with access to the internet, all of whom could potentially access your information. However, having good habits about passphrases, data creation and destruction, encryption, and email, you'll be ahead of 99% of people out there. Just by reading this you know more about computer security than most police officers and prosecutors.