

# PICKING AND PROTECTING PASSWORDS

University of Miami Ethics Programs

## WHY WORRY ABOUT PASSWORDS?

- **Your personal computer** – A compromised password can allow unauthorized access to the computer system you use, and to all the files you keep on it.
- **Shared computer systems** – Unauthorized access to a shared system can compromise security for you and everyone else who uses it.
- **Computer networks** – Unauthorized access to a single system can compromise an entire network, including every computer attached to it.

A person who has access to your password has your computer identity. They can do “bad things” with the access gained, like delete or alter files; and all the bad things may appear to have been done by you. Password compromises can also lead to identity theft in the broader sense – putting at risk both your finances and financial reputation.

## SUGGESTIONS FOR PICKING PASSWORDS

Passwords are compromised – or “cracked” – in a variety of ways. One is to try all the words in the dictionary – called, predictably enough, a “dictionary attack.” A dictionary attack would take a human a long time, but it can be an easy task for another computer. A computer could also just try all possible sequences of letters and numbers – called a “brute force” attack. Some systems lock your computer account after a large number of unsuccessful password attempts. It might just be you having a bad typing moment; but it could also be a dictionary or brute force attack.

Cracking doesn’t require a high-tech assault. If passwords are obvious enough, they can simply be guessed by someone who knows things about you – like your birthday, your spouse’s name, your favorite sports team, etc. There’s also the “shoulder surfing” attack – someone watching you while you type your password. And, of course, don’t forget about the easiest attack of all – someone finding the password you’ve written down and conveniently left in plain sight next to the computer.

A “strong” password is one that is hard to crack. Here’s how to create one:

- **More is better.** Use more than the minimum number of characters. The more characters you use, the more resistant the password will be to brute-force computer attacks and human guessing.
- **Mixed is better.** Use different types of characters mixed together – upper-case letters, lower-case letters and numbers. Mix in symbols too – non-alphanumeric characters like `*&^%_ $#@` – as permitted by the computer system (e.g., “mEye@me” not “miami”).
- **Real words are bad.** Don’t use words that are in the dictionary without adding other letters, numbers or characters to the word, to prevent a dictionary attack (e.g., “floreeDuh” not “florida”). And we mean in any dictionary. Password crackers are multi-lingual.

- **“Personal” words are bad too.** Don’t use passwords that refer to things that are easily guessed, such as a spouse’s, S.O.’s, child’s or pet’s name. Fragments of your social security number, address or telephone number are also bad choices. (You know that everyone knows these, right?)
- **Phrases can help your memory.** Using letters based on a familiar phrase or your favorite activities can help create a strong password – easy for you to remember but still hard for others to guess. For example,

“Icra\_BT” = I can resist anything but temptation

“ilsoBB\_otw” = I like sailing on Biscayne Bay on the weekend

- **Change is good.** Don’t keep the same password forever. Some computer systems will force you to pick a new password on a regular basis. Even if you’re not forced, it’s a good idea. If you have any reason to believe a password has been compromised, change it immediately – and report it!
- **Variety is good.** Don’t use the same password for all the systems you access. You don’t have one key for your home, car, office, etc., do you?

## SUGGESTIONS FOR PROTECTING PASSWORDS

So, now you have picked a very good password. Better yet, you have picked very good, but different, passwords for each system you use. And you are changing those passwords regularly. Now you must protect what you’ve created from discovery by others, and figure out how to remember it yourself.

- **Writing down passwords** – Let’s be clear: the best security comes from never writing down your password anywhere. But, for many of us, the choice is between writing good passwords down or using a bad (weak) passwords. If you’re going to keep a password “cheat sheet,” here are the ways to do it with greater safety:

Keep your password cheat sheet hidden and secure. In particular, don’t leave it near the computer itself. You wouldn’t leave your car key taped to the door of the car, would you? Or your house key taped to the front door?

Just in case the paper is found, don’t make write “user-IDs and passwords” on it, or something equally informative like the computer systems’ names. Ideally, a person who finds the cheat sheet should not realize what they’ve found.

For example, you can disguise the password information as something else – perhaps as a fake entry in your planner or PDA, with the passwords disguised as parts of addresses or telephone numbers.

If you think your cheat sheet has been compromised, change your passwords ASAP.

- **Saving passwords** – Many computer systems and web pages allow you to save your user ID and password, so you don't need to type it (or remember it) each time. This is a very, very bad idea. Anyone who gains access to your computer will have access to all the passwords. Just say no. However, password management software or password management in USB or card tokens can be very helpful *and* very safe if used properly.
- **Shoulder surfing** – Watch out for people watching you while you type in your password. Aside from the security implications, it's generally rude to peer over the shoulder of someone who is working on a computer, unless you've been specifically invited to do so.
- **Lending passwords** – Don't "lend" your password except in emergencies, and then only to someone you know for a reason that makes sense. Be sure it's an actual emergency, not just to save a little time or inconvenience. Change the password immediately post-emergency!
- **Unattended systems** – Leaving a computer unattended while you are logged in is the same as giving away your password. Don't do it. Log off or lock your system, even if you plan to be away only briefly. Some systems will log you off or lock you out after a period of inactivity (then password re-entry is required), but don't rely solely on this protection.
- **All passwords are not created equal** – Consider the security level you need to achieve. For example, a password for a single sign-on system that provides access to many computers probably needs to be very strong and changed regularly. A password for a single web site membership may need less strength (at least if no credit card numbers are involved).

► *Questions and comments about this document are welcome. Send email to [ethics@miami.edu](mailto:ethics@miami.edu).*