

Frank's Monthly Tech Tip

October Edition

These tips are based on questions I often receive and/or address issues I feel you may be interested in, such as security and productivity.

Is Your Password Safe?

Do you use the same password for multiple sites? Is your password a name or a word that can be found in the dictionary? Maybe you've thought, "I don't care who accesses this account... I have nothing important on here," so...

Why create strong passwords?

Pretend I'm a criminal (*pretend*)... I cracked your password.

Now I can...

- **Change your password.**
- **Access *shared* sensitive information on a network.** If your account is part of a group, their data has also been compromised.
- **Conduct illegal activity using that account.** Don't take it personally. I just prefer not to conduct illegal activity on my own account.
- **Possibly access login information** for your other, more important, accounts. I can view registration e-mails or have password reminders sent to that e-mail account if you used it to register for other accounts.

What else can I do to increase my safety?

- **Change your password periodically**
Viruses and spyware may find or intercept your login information. You can't always tell if your login information has been compromised, so change your passwords every few months.
- **Use different passwords for different sites**
If a password on one account is compromised, your other accounts won't be automatically compromised.

- **You can write down hints**

Write a sufficient hint, not the password. Keep them somewhere safe, like your wallet or a safe. A Post-It note on your monitor may seem like a fortress of security, but research indicates it's deceptively easy to access.

What's a strong password?

Your password may not be as strong as you think. Widely available “brute force” password cracking tools make rapid attempts at guessing your password, often from “dictionaries” of default passwords, common passwords, English words and phrases, and literally every combination of characters depending on how patient the intruder is.

To increase your password strength...

1. **Increase the length.** Shoot for at least 8 characters.
2. **Increase the variety of characters** by mixing letters, numbers and symbols.
3. **Increase the apparent randomness.** Do not use words, names, or anything directly associated with you or the username (birthday, address).
4. **Make it something you'll remember.** Passwords are intended to keep *others* from accessing your resources.

This information and the work involved in changing the way you handle your passwords may seem overwhelming. It may not be necessary to take all these measures, but please give the issue some thought and be aware the easiest targets are the complacent ones.

Additional Reading

- **How to Create a Strong Password**

<http://www.econsultant.com/articles/how-to-create-a-strong-password.html>

Concise directions for creating strong, easy-to-remember passwords

- **Common and Bad Passwords**

<http://geodsoft.com/howto/password/common.htm>

This is the top result for “common passwords” in Google. Is your password on this list?