# Change your passwords

## Change your passwords | Tech Tips Podcast by PcCG

[Subscribe via Itunes](#) [1] | [Subscribe via RSS](#) [1]

We recently had an email account hacked. It wasn't because there was a security flaw in our system, or because we were a victim of phishing. It was because another third party website got hacked, which we used the same username/password combination. The hackers got the information from this other website, and used it to get into our email. Fortunately it was an old outdated account and so no damage was done. The moral of the story is, if it can happen to us, it can happen to you!

It's becoming more frequent to get a letter in the mail notifying you that some database has been hacked that contains some information about you. These hacked databases can have any sort of information stored including usernames and passwords. If you use the same username/password for the website/database that was hacked as you do for other items, you can be at risk.

Let's look at an example.

Tom has an account at Sears.com. His username is tom@myfakeemail.com and his password is A42i$#io. It's a good strong password, one that is unlikely to ever be guessed. Tom uses this information to log into the Sears website. Tom however uses the same username and password to log into his email. He wants to keep things simple, and so he uses the same username and password so that he doesn't need multiple passwords.

Sadly, jerks on the internet spend their time trying to hack and steal databases that are filled with information and improperly managed. A properly secure database would still be encrypted and unusable to the attackers – but not all databases are setup with the level of care and concern for security as they should be.

This information is even sold on some websites! You can subscribe to a website, and simply plug in the information you want regarding hacked passwords. Here is an example: https://www.leakedsource.com/main/ [2] -- I post the link not to give publicity, but so that you can check to see if your user accounts turn up any results. Even if it doesn't – it's still a good idea to manage your passwords wisely.

Follow these couple steps and you'll be well on your way to a safer internet.

**Password Policy / Guide**

We need something that balances security with practicality. It's best practice to have a unique password for every website you visit. Using tools such as LastPass can help with that! But most people are not willing to do that. Here are our recommendations as a compromise.

Have 4 levels of passwords.

1. **Level 1 Email Addresses**
2. **Level 2 Financial institutions**
3. **Level 3 Social Networking sites**
4. **Level 4 Everything else (Sears.com, Amazon etc).**

With each level you have at least 1 unique password. The password you use in Level 1 should not be used in any other levels.

Now this part is critical – Change your passwords every so often!! I know, I know it's a pain! We don't enjoy doing it either; and you can imagine as a computer company, we have a LOT of passwords to manage. Never the less, your password may have been hacked and hackers just haven't gotten around to using it yet. Changing them at least once a year (preferably every 6 months) can minimize some of that risk.

Use a strong password [3]. It's really not that hard to do! Trust me!! Using a simple password like your dog's name 123 won't fly.

For other security related tips check out...

- Protect yourself from Cyber-Threats [4]
- eHarmony and LinkedIn passwords compromised [5]
- Hijacking Email – Phishing for Information [6]
- Create Strong Passwords [3]
- More Security Alerts! [7]



Tech Tips [8]
Tech Tips Articles [9]
Tech Tips Podcasts [10]

https://www.pccomputerguy.com/Email-Hijacking-Phishing-for-data [7]
https://www.pccomputerguy.com/Tech-Tips-Podcast-More-Security-Alerts [8]
https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [9]
https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Articles [10]
https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Podcasts