

Password Security

The Plain English Guide to Password Security gives you advice that will help you to choose a password that will be safer and more secure than the one you are probably using now. 1.1 Why do you need good password security? The criminal activities of hackers is frequently documented in the news, but do you know much about them and importantly, do you do anything to protect yourself from them? Hackers will use several methods to get into your network and files. The three common approaches can be categorized as: brute force, dictionary attacks and social engineering. Brute force as the name suggests is perhaps the least sophisticated. It is also the most time-consuming method. The hacker uses a program that will try in all possible combinations of keyboard characters to guess your password. The more complex and longer your password, the longer the program will take to determine the correct combination. Experts suggest that a password which is eight characters in length and utilizes lower and upper-case letters, numbers and keyboard characters can't be cracked for two years. The best recommendation we can make with regards to passwords is to have a random password using lower, upper-case letter, numbers and characters, this will virtually eliminate this form of attack as a risk.

The second method is described as the 'custom dictionary' attack. Similar to the brute force approach, instead of running through combinations this style of attack uses a dictionary filled with combinations such as 8888 or abcd1234. Simple passwords like 'myname', 'password5566' or 'myfavpet' can be easily listed and therefore guessed. Again the lesson here is to have a random type password.

The most effective way to gain access to a person's password is by a method known as social engineering. This is the practice of someone with criminal intent soliciting the password directly from the user. People often divulge their passwords to co-workers and strangers without giving it a second thought.

The main weakness of giving out password information is that many people use a simple password on every account: Google, eBay, online banking, Amazon etc. Once the hacker has obtained one password then they can attempt to hack multiple accounts owned by that person.

So what can be done to protect and improve password security? To read the complete briefing please click on the image of the briefing above. 1.2 How to avoid a bad password

1.3 Creating a strong password

1.4 Change your passwords regularly

1.5 Recommended software Managing all these passwords takes a lot of effort. You may want to consider a program that can manage your passwords for you. We recommend the following 3 products:

Wouldn't it be great if you could remember just ONE password that gave you access to ALL your web accounts without compromising security? Wouldn't it also be great if you could bring up a menu of your web accounts and simply logon to any of them with a mouse click? This type of functionality is called Single Sign-On (SSO) and this is exactly what AccountLogon allows you to do. You do NOT need to change your individual website passwords, AccountLogon will remember them and fill them in for you! You will NEVER have to type another password again, therefore reducing the risk of your passwords being stolen by keyboard loggers and malicious viruses! Strong encryption (3 times the strength of Internet banking) and many other security features will protect your details from Identity Theft. Account logon Roboform My Security Vault