Using passwords

PB/INFO/026 (10/05)

Why passwords matter

Every time we use a computer, a network or an electronic service we should have to prove who we are. This is important to ensure that we are entitled to use the particular service, and to give us access to our own personal information and settings.

In many cases, ranging from e-mail to banking, these settings are our complete electronic identity. If someone can ‘borrow’ my access to the system not only can they see and alter my personal information, but they can impersonate me perfectly. A message or money transfer sent by them will be identical to one sent by me. My password is the key to my filing cabinet and also my signed letterhead and blank cheque. It is essential for anyone using a computer to choose and use passwords well.

The first rule is never tell anyone your password. If you are given an account with a password already on it, change it immediately to something only you know; never set your password to something someone tells you. If you need to share information there are always safer ways to do it. Always check before entering a password that the form or web page requesting it is the one you expect.

Managing passwords

Remembering a few passwords should be no problem but as we use more computers, networks and web sites they can get out of hand. Ideally every password should be unique, but it is possible to reduce the number to be remembered without reducing security too much. If access to different things represent the same risk, there is little loss of security if the same (or linked) passwords are used. For example if someone can log into my personal webmail account they can send forged e-mails in my name. They are unlikely to do me any more harm by logging into my other personal webmail accounts so there is little increased risk in using the same password for these.

Passwords sent over the Internet are more likely to be stolen than those that are only used on a single computer or Local Area Network. The same password should not be used for Internet and local accounts, especially as local passwords often give access to more sensitive systems or information. The password protecting the list of books I bought last month should be different from the one I use to access student records or department finances.

Time is much better spent thinking up a few good passwords, rather than memorising dozens of bad ones.

Changing passwords

Computers always seem to ask for passwords to be changed at the least convenient time. However it is important to change passwords regularly to defeat the attacker who simply tries every possible combination of characters. The factsheet 'Threats to Passwords [1]' explains how effective this can be and why good passwords are needed to protect against it. If possible, don't change your password the first time the system asks you to. Instead treat this as a prompt to spend some time thinking of a good new password. Then change your password **next** time you are asked and you will have both a better password and a better chance of remembering it. Never change your password just before a holiday or last thing on a Friday as you will have forgotten it by the time you need to use it again!

Choosing passwords

So what makes a good password? It should be memorable to you, but infeasible for anyone else to guess. Neither a person who knows your favourite food, pet, football team or anything else about you, nor a computer trying combinations of letters, numbers and dictionary words should be able to find it out.

Most textbooks recommend that passwords have at least eight characters including upper and lower case letters, numbers and punctuation symbols. This should be sufficient to protect against the computer guessing systematically, but leaves the challenge of how to remember such a keyboard soup. The best way is to start with a phrase or sentence you can remember, perhaps from a song or a poem, and then convert it to letters, numbers and characters in some easy-to-remember (which often means humorous) way.

For example, use the initial letters of 'Twinkle, twinkle little star how I wonder' with ***** (for star), **?** (for how) and **1** (for wonder - puns are memorable). This generates the effective and memorable password:

T,tl*?I1

Bruce Schneier has published an article [2] with more examples and an explanation of how passwords are most frequently attacked.

A study at Cambridge University in 1999 found that users taught this mnemonic technique produced passwords that were much more secure but no harder to remember than those chosen by untrained users. A paper describing this study can be found at: http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-500.pdf [3].

Of course any password used as an example immediately becomes a bad password, so now you will have to think up your own.

Links
[1] http://community.ja.net/library/janet-services-documentation/threats-passwords
[2] https://www.schneier.com/crypto-gram-1403.html#13
[3] http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-500.pdf