Devising Passwords against Hacking

TEAM CLAWS

It is absurdly easy to get hacked. All it takes is clicking on one malicious link or attachment. Hackers are busy every day, trying to steal your personal data. Companies' computer systems are attacked every day by hackers looking for passwords to sell on auction. Hackers regularly exploit tools like John the Ripper, a free password-cracking program, that use lists of commonly used passwords from breached sites and can test millions of passwords per second. This has serious implications for both national and personal security.

Getting hacked is perhaps unavoidable but we can make the job of hackers much more difficult by following a few simple rules. Two things are essential to enable better computer security. First, avoid suspicious links, even from friends, and second, manage your passwords better. As good password hygiene takes effort, here are some tips that could help delay if not totally obviate the inevitable.

Forget the Dictionary. The worst passwords are dictionary words or a small number of insertions or changes to words that are in the dictionary. Hackers will often test passwords from a dictionary or those aggregated from breaches. If your password is not in that set, hackers will typically move on.

Never use the same Password Twice. People tend to use the same password across multiple sites, a fact hackers regularly exploit. While cracking into someone's professional profile on LinkedIn might not have dire consequences, hackers will use that password to crack into, say, someone's e-mail, bank, or brokerage account where more valuable financial and personal data is stored.

Use Long Passwords. The longer your password, the longer it will take to crack. A password should ideally be 14 characters or more in length if you want to make it uncrackable by an attacker in less than 24 hours. Because longer passwords tend to be harder to remember, consider a passphrase, such as a favourite quote, song lyric, or poem, and string together only the first letter of each word in the sentence. A password such as trissmitp25824 could simply be a combination of your IC number and the phrase, 'the rain in Spain stays mainly in the plain'. Easy to remember but hard to break. Use birthdays and anniversaries to remember numbers either in the six digit or in the eight digit format. 21031972 would thus represent 21 March 1972 and when used with a phrase could be ideal as a password.

Use Long Passwords. The longer your password, the longer it will take to crack. A password should ideally be 14 characters or more in length if you want to make it uncrackable by an attacker in less than 24 hours.

Use Random Numbers. For sensitive accounts, randomly hit on the keys in the keyboard, intermittently hitting the Shift key, and copy the result into a text file. Keep a paper printout in a safe place. Store this on an encrypted, password-protected USB drive.

Store your Passwords Securely. Do not store your passwords in your in-box or on your desktop. If malware infects your computer, they will all be stolen. Passwords could be stored on a password file on an encrypted USB drive. You must memorise the password for this drive. Then copy and paste those passwords into accounts so that, in the event an attacker installs keystroke logging software on his computer, they cannot record the keystrokes to his password. You could also use password hints and not the actual password in a piece of paper which you carry with you. That way, your most sensitive information is off the internet completely.

Care in using a Password Manager. Password-protection software lets you store all your usernames and passwords in one place. Some programs will even create strong passwords for you and automatically log you in to sites as long as you provide one master password. LastPass, SplashData and AgileBits offer password management software for Windows, Macs and mobile devices. However, there are serious risks here. Hackers have demonstrated how easily the cryptography used by many popular mobile password managers could be cracked. Also, if someone steals your computer, then you have lost your passwords too.

You are your e-mail address and your password. Please treat anything you type as a public record.

Ignore Security Questions. There is a limited set of answers to questions like “What is your favourite colour?” and most answers to questions like “What middle school did you attend?” that can be found on the Internet. Hackers use that information to reset your password and take control of your account. A better approach would be to enter a password hint that has nothing to do with the question itself. For example, if the security question asks for the name of the hospital in which you were born, your answer might be your favourite song lyric.

Use Different Browsers. Use different Web browsers for different activities. Pick one browser for ‘promiscuous’ browsing: online forums, news sites, blogs—anything you don’t consider important. However, when you’re online banking or checking e-mail, fire up a secondary Web browser, then shut it down. That way, if your browser catches an infection when you accidentally stumble on an X-rated site, your bank account is not necessarily compromised. As for which browser to use for which activities, a study in 2011 by Accuvant Labs of Web browsers — including Mozilla Firefox, Google Chrome and Microsoft Internet Explorer — found that Chrome was the least susceptible to attacks.

Share Cautiously. You are your e-mail address and your password. Please treat anything you type as a public record.

And finally, at some point, you will get hacked — it’s only a matter of time. If that’s unacceptable to you, don’t put it online.Happy browsing.