8 steps to a strong password

Useful tips for your online protection

PASSWORD

pA5SW0RD

A;7;3oLSgkM'%3

epoxy hippo double bread listen neuron plaza

1 Word character alternatives do not work

Due to the growing sophistication of attacks, replacing letters with numbers or special characters does not work if the original word mirrors an existing dictionary word. Attackers expect character alternatives and can predict their usage.

2 Passphrase instead of password

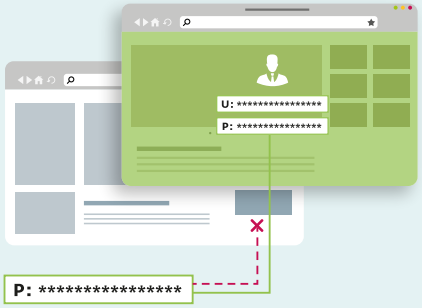
A passphrase is a multi-word password that is specific and has meaning. This "hidden sense" makes the passphrase easier to remember for its creator. It is much harder to memorize passwords containing a long string of letters (lower/upper case), numbers and characters than a meaningful passphrase.

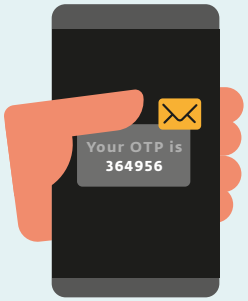
3 Imagine all the people living life in peace...

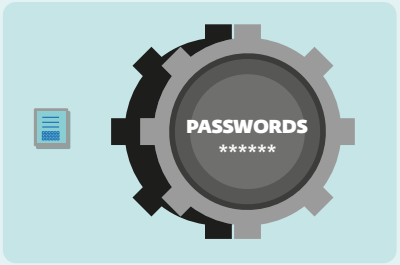
A few words of caution about passphrases. Although this 8-word phrase looks like an unbeatable passphrase, the opposite is true. Famous quotes and well-known phrases or lyrics are highly predictable. Cybercriminals exploit databases of popular phrases, so it is not so difficult to crack your multi-word password. Change the order of words randomly. It will make your passphrase more secure.

4 Beware of a dictionary attack

A dictionary attack is a method of hacking your password by systematically entering similar terms from various dictionaries. To prevent attackers cracking your password by this method, we suggest you use at least a 7-word passphrase with words in random order.







5 More is better

Why a 7 word passphrase? Because password strength is measured in information entropy. Malware algorithms scan according to combinatorics (mathematics of counting). But each bit of entropy doubles the number of guesses required. For example, a 7 word passphrase equals about 90.5 bits of entropy, which would take approximately 27 million years to decode at one trillion guesses per second*. In comparison, a 5 word passphrase would take only 6 months.

6 One passphrase for one site

The basic rule is do not use the same passwords or passphrases for several different accounts. Attackers can take control of the remote servers, which makes them able to steal your passphrase as soon you log in, regardless of how strong or unique your passphrase is.

7 2-Factor Authentication

2FA is always a good way to deter attackers. It adds an extra layer of security—and this solution is massively supported by the password database services, if you opt for one.

8 Use a password vault

Keep your passwords in a secure digital location. The passport vault/manager software encrypts the password storage so you use a single password or passphrase for accessing different passwords. Keep your strongest passphrase as the master passphrase for a service like this and that's the only one you need to memorize.

*E. Snowden claims that NSA is able to perform about one trillion guesses per second.

ESET ENJOY SAFER TECHNOLOGY®