

Passphrase Fundamentals



1 Een goede passphrase bestaat uit minimaal vijf woorden

Een passphrase is veiliger dan een wachtwoord. Wanneer één karakter aan een wachtwoord wordt toegevoegd is het namelijk meteen vele malen lastiger te kraken. Hoofdletters en vreemde karakters, zoals een ? of een &, zijn niet noodzakelijk maar wel aan te raden. Ze maken de passphrase nog veiliger.

2 Bedenk zelf een passphrase

Gebruik geen bekende uitspraken, gezegden of spreuken. Er bestaan lijsten waar deze uitspraken op voorkomen waardoor dergelijke passphrases snel gekraakt kunnen worden. Gebruik geen persoonlijke informatie. Denk hierbij aan een lijfspreuk of motto dat op je profiel van Facebook staat en zo door iedereen te vinden of te raden is.

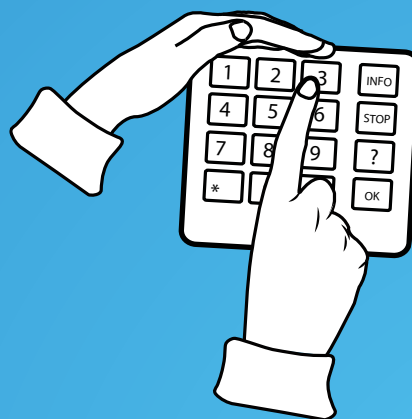


3 Gebruik voor ieder account een andere passphrase

Veel mensen gebruiken hetzelfde wachtwoord voor verschillende online diensten en accounts. Als het wachtwoord achterhaald wordt kan er met dit wachtwoord ook bij alle andere online diensten worden ingelogd. Om dit te voorkomen gebruik je voor ieder account een andere passphrase.

4 Deel een passphrase nooit met anderen

Tot slot, een passphrase is persoonlijk, net als een pincode. Deel een passphrase nooit met anderen. Voer daarom ook nooit wachtwoorden in op andermans of openbare computer. De computer kan de ingevoerde gegevens opslaan of besmet zijn met malware, waardoor er alsnog gemakkelijk toegang tot het online account verkregen kan worden.



Passphrase Fundamentals



1 A strong passphrase consists of at least five words

Since longer passwords are stronger, a passphrase is the preferred option. More characters exponentially increase the password strength, the longer the better. Capitals and special characters like a “?” or an “&” are not necessary but are recommended. They increase the passphrase strength even more.

2 Create your own passphrase

Never use well-known sayings, slogans or other quotations. Password cracking tools use lists with well-known sayings and therefore have a better chance of cracking your passphrase. Also never use personal slogans or mottos you use on Facebook since they will be very easy to guess.



3 Use different passphrases for different accounts

Using the same password for all your online accounts is like having one key that unlocks every door you will ever use. If hackers manage to steal a password database from one website they can use your password to compromise all your other online accounts. To prevent this always use different passphrases for different accounts.

4 Never share your passphrase

Last but not least: a passphrase is personal, just like a pin code. Never share your passphrase. Also, never enter your passphrase on a public computer. Someone might have installed a key logger that records your keystrokes, or the computer might be infected with malware. In both cases your account will be compromised.

