


Wachtwoordbeveiliging

Mei 2003

Henk Jongedijk, woensdag 27 september 2006 - 00:00:00

STAAT UW WACHTWOORD IN DEZE LIJST?

- » Uw voornaam of van familielid/vriend(in)
- » Uw achternaam of van familielid/vriend(in)
- » Geboortedatum van u of een familielid/vriend(in)
- » Nummerbord van uw auto of van familielid
- » Een woord dat op of bij uw computer staat
- » Naam van een school waar u op heeft gezeten / Naam van bedrijf waar u werkt
- » Naam van een favoriet TV-programma of film
- » Naam van een personage of acteur
- » Term uit een (computer)spelletje
- » Een woord uit een woordenboek (maakt niet uit welke taal)
- » Naam van een tijdschrift of boek
- » Een van de bovenstaande woorden, achterstevoren
- » Een van de bovenstaande woorden, met een cijfer of leesteken er voor of achter

Heeft u  of meer vragen met  JA beantwoord?... dan is uw wachtwoord z  ³ geraden!

HACKERS EN CRACKERS

Een 'hacker' is iemand die handig is in het schrijven van software en goed met computers overweg kan. Een 'hacker' heeft de mogelijkheid en kennis om systemen te kraken, maar doet dat uit principe niet. Een 'cracker' is ook erg handig, maar gebruikt deze handigheid om systemen te kraken (in te breken), mogelijk gegevens te stelen, te vernietigen of te vervalsen.

'Hacker' wordt vaak gezegd, terwijl 'cracker' wordt bedoeld.

JE MAG ALLES VAN ME WETEN, BEHALVE M'N WACHTWOORD!

Computergebruikers denken vaak dat crackers allerlei moeilijke trucs gebruiken om ergens binnen te komen. Niet waar! Het grootste deel van alle inbraken gebeurt met geraden wachtwoorden. Soms maken crackers gebruik van een programma dat alle woorden uit het woordenboek probeert. Wilt u dus veilig surfen, zorg dan dat uw wachtwoorden niet te raden zijn.

ONZINNIGE ZIN

Een eenvoudige en toch krachtige manier om een niet te raden wachtwoord te maken, is het kiezen van een onzinnige zin. Kies van elk woord uit uw zin de eerste letter, leestekens blijven staan en bepaalde woorden vervangt u door cijfers of andere tekens. Bijvoorbeeld de zin: "Ongelofelijk, betaal ik hier geld voor?" Met het bovenstaande recept, waarbij we het woord "geld" vervangen door een dollarteken, ontstaat het volgende wachtwoord: "O,bih$v?" Niemand die dat zomaar raadt, en toch is het makkelijk in te typen als u bij uzelf de zin zegt terwijl u hem intypt.

Tip:

'de appel valt niet ver van de boom' wordt wachtwoord 'dAvnvvdB'

VIJF WACHTWOORD TIPS

- » Wijzig al uw wachtwoorden regelmatig, bijvoorbeeld elke maand. Let er op dat het nieuwe wachtwoord echt verschilt van het oude, en niet bijvoorbeeld slechts op een ander cijfer eindigt.
- » Vertel nooit aan anderen wat voor manier u gebruikt om wachtwoorden te verzinnen. Onthul ook geen oude wachtwoorden. Hieruit kunnen anderen gemakkelijk afleiden wat uw huidige wachtwoord is.
- » Gebruik nooit hetzelfde wachtwoord voor verschillende systemen, zeker niet als een van die systemen een Website is. Die wachtwoorden zijn veel kwetsbaarder dan de wachtwoorden van uw inbelaccount.
- » Controleer regelmatig of u al uw wachtwoorden nog weet. Dit is de beste manier om er voor te zorgen dat u niks vergeet.
- » Probeer wachtwoorden nooit in de buurt van uw computer te bewaren. Vernietig brieven met wachtwoorden die u van uw provider krijgt, nadat u het wachtwoord hebt ingevoerd.

SHOCKING!

Experts adviseren gebruikers van het Internet om regelmatig hun wachtwoorden te veranderen voor hun eigen veiligheid. We kunnen het al een beetje op onze klompen aanvoelen, maar weinig mensen houden zich aan deze aanbevelingen. Meer dan de helft van de internettende menigte verandert zijn wachtwoord nooit. Opvallend onveilig is ook de keuze van de wachtwoorden: het meest worden namen van partners of kinderen gebruikt, maar ook het favoriete voetbalelftal of de naam van een geliefde band. Er zijn zelfs mensen die hun wachtwoord gewoon op een briefje op de computer hebben hangen. Het onderzoek waaruit deze gegevens komen is door de Britse online bank Egg gehouden onder 1000 personen:

Meest gebruikte wachtwoorden:

23% namen van kinderen

19% naam van partner

12% verjaardagen

9% naam voetbalclub

9% beroemdheden en bands

9% favoriete plaats

8% eigen naam

8% naam huisdier

Bron: Egg survey Juni 2002

WACHTWOORDSAMENSTELLERS

Op de volgende links kunt u gratis een wachtwoordsamensteller downloaden.

- » <http://blazonry.com/javascript/password.php>
- » <http://world.std.com/~reinhold/diceware.html>
- » <http://www.pctools.com/guides/password>

SLECHTE WACHTWOORDEN

Slechte wachtwoorden zijn die wachtwoorden die makkelijk te raden zijn of met enig speurwerk eenvoudig te achterhalen. Hieronder volgt een aantal voorbeelden van wachtwoorden die u uit veiligheidsoogpunt beter niet kunt gebruiken.

- » Gebruik als wachtwoord nooit hetzelfde woord als uw gebruikersnaam of een afleiding daarvan.
- » Gebruik als wachtwoord geen woorden die herleidbaar zijn tot uw gegevens als gebruiker. Gebruik dus geen eigennamen, postcodes, kentekens, namen van vrienden, vriendinnen of huisdieren. Kies ook geen woorden als 'geheim' en 'secret', 'password', 'jamai', 'gtst', 'breezer' en dergelijke.
- » Gebruik als wachtwoord nooit telefoonnummers, kentekens, pincodes en giro- of banknummers. Dit is informatie die met wat speurwerk eenvoudig te achterhalen is.
- » Gebruik als wachtwoord geen blokjes en rijtjes op het toetsenbord als 'fred' en 'qwerty'.
- » Gebruik als wachtwoord geen woorden die voorkomen in een woordenboek of in de woordenlijsten van de spellingcontrole op je computer. Deze wachtwoorden zijn namelijk eenvoudig te kraken met behulp van de zogenaamde woordenboekmethode. Dit is een methode waarbij krakers met een woordenboekprogramma op zoek gaan naar de wachtwoorden die in uw computer staan. Een wachtwoord dat per definitie slecht is, is een wachtwoord dat niet alleen bij u bekend is. Wijzig daarom direct het standaard wachtwoord dat u ontvangt als u zich ergens aanmeldt als abonnee.

GOEDE WACHTWOORDEN

Goede wachtwoorden zijn wachtwoorden die in principe niet te achterhalen zijn door mensen of door speciale kraakprogramma's. Dit zijn programma's waarmee krakers gecodeerde wachtwoorden kunnen ontcijferen. De volgende richtlijnen kunnen u helpen bij het verzinnen van een goed wachtwoord.

- » Kies voor elk programma een ander wachtwoord. Gebruik nooit hetzelfde wachtwoord voor verschillende diensten.
- » Kies een wachtwoord van minimaal 5, maximaal 8 karakters, dat bestaat uit zowel hoofdletters, kleine letters en minimaal ã © ã ©n cijfer bijvoorbeeld T3st,05.
- » Kies een wachtwoord dat u makkelijk kunt onthouden. De veiligste plaats om een wachtwoord op te slaan is in uw hoofd. Gebruik eventueel een wachtwoordsamensteller.