

Tahmin Edilmesi Zor Bilgisayar ?ifresi Olu?turmak

Bilgi güvenli?inin en önemli araçlar?ndan birisi de, kritik bilgilere eri?imi kontrol altında tutan ?ifrelerdir. Ancak, ?ifrelerin çözülmesini sa?layan ?ifre k?r?c? programlar? elde etmek, internette yap?lacak k?sa bir arama sonucunda i?ten bile de?il. ?ifre güvenli?i konusunda kullan?c?lar?n dikkatsiz davranmas?, ?ifre k?r?c?lar?n i?ini oldukça kolayla?tır?yor. Yap?lan ara?tırmalar en yayg?n olarak kullan?lan ?ifrelerin 123456, qwerty, 987654321 gibi klavye üzerinde kolayl?kla bulunabilecek ?ekilde olu?turuldu?unu göstermektedir.

Bir çok ki?inin ise, ?ifrelerini küçük ka??tlara yazarak çal??ma masalar?na, bilgisayar ekran?n?n kenar?na yap??t?rd?klar? veya kalemlik içine koyduklar? da bilinmektedir.

Ancak, ?ifre güvenli?ine önem vererek, harflardan ve say?lardan karma??k ?ifreler olu?turmaya çal??anlar?n dahi ?ifrelerini kolayca hatırlamak için tahmin edilmesi kolay kelime ve rakam serileri kulland?klar? bilinmektedir. Hatta ?ifre kullanarak girilen web siteleri, ?ifre olu?turma a?amas?nda kullan?c?y? etkili ?ifre olu?turmak konusunda zorlamaktadır.

?ifre güvenli?ine kar?? en büyük tehdidi ise, yaz?l?m dünyas?ndaki geli?melerin sonucu ortaya ç?kan ?ifre k?r?c? programlardır. Bu programlar ?sözlük sald?r?s?? yöntemiyle bir kaç saniyede, bir kaç yüzbin deneme yaparak ?ifre k?rabilmektedir.

?ifre k?rma giri?imlerine kar?? alınacak en basit tedbirler,

- uzun ve karma??k ?ifreler olu?turmak,
- ?ifreleri kimseyle payla?mamak,
- kendi kontrolünüzde olmayan bilgisayarlarda ?ifre kullanmamak,
- ?ifreleri ka??t, bilgisayar, cep telefonu gibi eri?imi kolay yerlerde muhafaza etmemek,

Tahmin edilmesi zor ?ifreleri nas?l olu?turabiliriz?

Tahmin edilmesi zor ?ifreler, hem uzunluk olarak, hem de içerdi?i karakterler aç?s?ndan benzersiz olanlardır. Ancak, karma??k ?ifre olu?turmak isterken, kendi ?ifremizi unutmak riski de mevcuttur.

A?a??daki bölümde, bu konuda bir yöntem önerisini örnek çal??ma içerisinde bulabilirsiniz. (www.csoonline.com dan faydalan?lm??t?r). Bu yöntemle belirledi?iniz ?ifrelerinizin gücünü a?a??daki linkte test edebilirsiniz.

<https://www.microsoft.com/protect/fraud/passwords/checker.aspx>

Ad?m-1; en az 5 kelimedenden olu?an bir cümle seçin. Bu cümle; bir ?ark?n?n veya ?iirin ilk cümlesi veya nakarat bölümü, bir ata sözü veya sevdi?iniz bir kitab?n ba?l??ı olabilir. Bu çal??mada seçece?imiz cümle; ?biz hergece heybelide mehtaba ç?kard?k? olsun. Yap?lacak ilk i?lem, bu cümleden belirli harfleri sistematik olarak ay?klamaktır. Biz de bu cümledeki her kelimenin ilk ve son harfini Türkçe karakterlere yer vermeden ay?rarak bir harf öbe?i olu?turuyoruz.

bzhehemack

Ad?m-2; ?de bu yeni harf öbe?inin harflerini çe?itli rakam ve ?ekillerle de?itirerek, baz?lar?n? büyük harf yaparak de?itiriyoruz. Örnek olarak;

- z harfini 2
- hehe harflerini ayn? harfleri tekrar etmemek için Hex2 (he çarp? 2)
- m harfini M
- a harfini @
- k harfini 1 olarak de?itiriyoruz ve harf öbe?imiz.

b2Hex2M@c1 haline geliyor.

Yukarıda verdi?imiz linkteki ?ifre güvenli?i test program?n? kullanarak, ?ifremizin güvenli?ini test etti?imizde hala orta seviyede güvenlik sa?lad??n? görebiliriz.

Ad?m-3; ?de ?ifre aday?m?z olan harf öbe?inin 10 basama??n? 14 basama?a ç?karmak için ilaveler yap?yoruz. Bunun için ak?lda kalmas? kolay rakamlar ekleyebiliriz. Örnek olarak, e?inizin veya çocu?unuzun ya?ad??n?z yerden farklı olan do?um yerinin il

trafik kodu, bir rakam? benzer bir harfle de?itirerek eklenebilir. Örnek; il ad? Ankara ise, 06?y? o6 olarak ba? tarafa ekleyelim. Son tarafa ise, Ankara?n?n sessiz harfleri olan nkr eklenebilir.

o6b2Hex2M@c1nkr

Yukar?da ç?kan karakter öbe?ini yukar?daki linkte test etti?imizde ?ifremizin ?kuvvetli? oldu?u görülmektedir. Ancak hâlâ ?ifremizin güvenli?inin tam oldu?u söylenemez.

Ad?m-4;de ?ifre aday?m?z olan harf öbe?ini çe?itli ihtiyaçlar için çe?itlendiriyoruz. Örnek olarak, ?irket bilgisayar?ndaki mail hesab?n?z için kullanaca??n?z ?ifreye ?sirket?, gmail hesab?n?z için kullanaca??n?z ?ifreye ?goo?, yahoo için ?hoo? gibi ilaveler yap?l?r ve a?a??daki ?ifre elde edilir. Test sonucunda ?ifre güvenli?inin ?en iyi? düzeye geldi?i görülecektir. (test için kulland??n?z ?ifre aday?n?n bir kaç harfini de?i?tirmenizde fayda varJ)

o6b2Hex2M@c1nkr goo

Ad?m-5; Peki, bu karma??k ?ifreyi nas?l hat?rlayaca??z. Tabii ki, bunu bir ka??da aç?k aç?k yazarak de?il. Bu ad?mda yapaca??m?z i?lerin yar?s?nda haf?zam?za i? dü?mektedir.

- biz hergece heybelide mehtaba ç?kard?k cümlesini bir ka??da birinci sat?r olarak yaz?n
- yapt??n?z ilk de?i?iklikleri akl?n?zda tutun
- ikinci sat?ra 06 Ankara, gmail için yaz?n.
- Bu kelimelerin de?i?ik hallerini nereye ekledi?inizi de akl?n?zda tutun.
- ?ifre de?i?ikliklerini her zaman ayn? ?ekilde yap?n.
- Her ?eye ra?men ?ifrenizi 30 günde bir de?i?tirin.

Di?er aç?klamalar

Olu?turulan bu ?ifrenin sözlük sald?r?lar?na kar?? direnme gücü çok yüksektir. ?ifre k?r?c? 72?nin 18?nci kuvveti kadar olas?l??? denemek zorundadır. Bu say? 34 basamaklıdır ve saniyede bir milyon deneme yapan bir ?ifre k?r?c?n?n dahi bu ?ifreyi çözmek için aylarca çal??aca?? ortadadır.

En fazla bir kaç yanl?? ?ifre giri?ine müsaade edilen sistemlerde bu yöntemin kullan?lmas? gerekli de?ildir.

Otomatik ?ifre hat?rlat?c?lar? kullanmay?n, bilgisayar?n?z ba?kas?n?n eline geçerse tüm ?ifreleriniz elde edilir.

?ifre kurtarma sorular? için kaydetti?iniz cevaplar?n da tahmini zor olmalıdır. Örnek olarak ?ilk ö?retmeninizin ad? ne? sorusuna kar??l?k do?ru cevab? kaydetmek zorunda de?ilsiniz, ilk ev telefon numaran?z? veya okul numaran?z? kaydedebilirsiniz.