Eldar Kudinov • Michail Diakov • Vasily Yaltonsky • Dennis Fisher

# HAYATTA KALMAK DİJİTAL DÜNYADA

Dijital hayatınızı güvende tutmak için pratik tavsiyeler

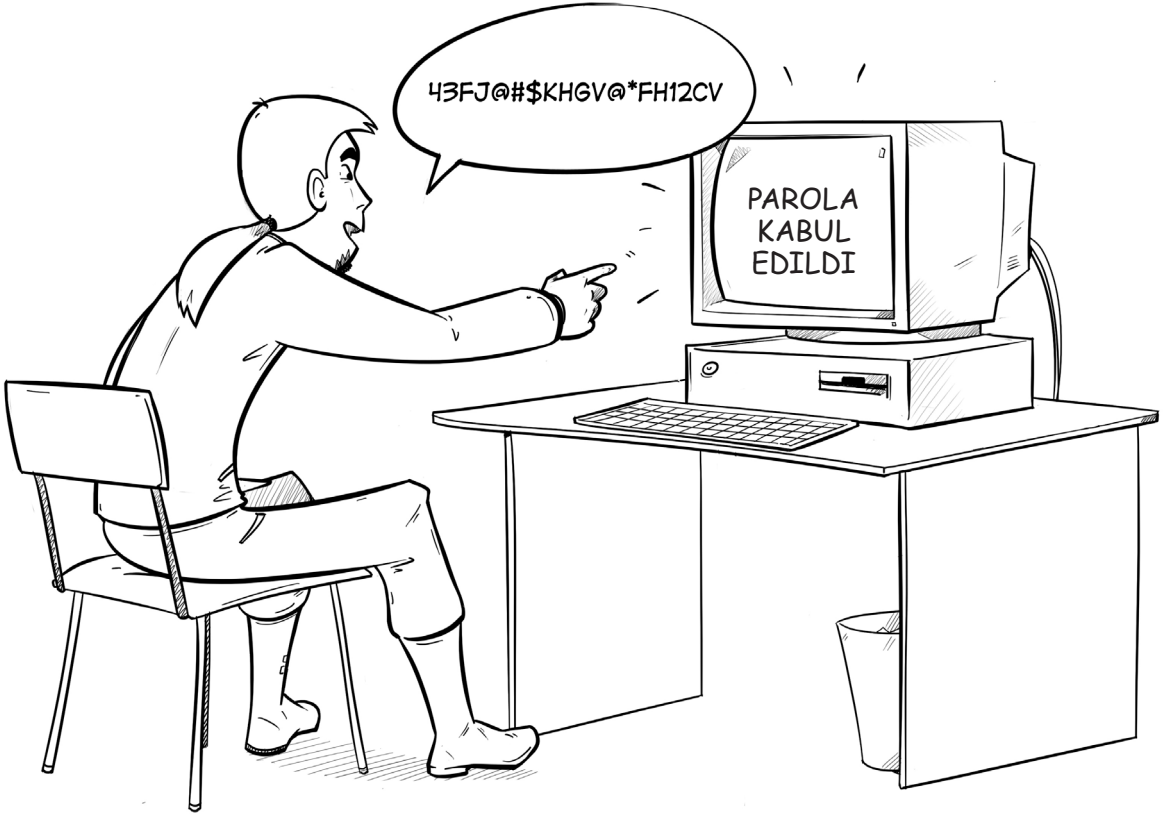
KASPERSKY lab

# GİRİŞ

Dijital çağın doğuşu beklediğimiz gibi görünmüyor. PC'ler ve cep telefonları, insanlara büyük miktarda bilgiye erişim sağlarken, bunları paylaşmak için sonsuz yeni olanaklar sunuyor; yeni teknolojimiz ve İnternet sayesinde hayatımız artık daha kolay ve daha iyi. Ancak, bu iyi şeyler kişisel bilgi hırsızlığı, kötü amaçlı yazılımlar ve Web'i kişisel oyun alanı olarak kullanan suçlular grubuyla dolu olumsuzlukları da yanında getir. İyi haber ise, bu kaos ile savaşan ve deneyim ve bilgilerini gelecek nesillerle paylaşmaya istekli insanlar var. Böylece efsanenin karanlık kısmı sona eriyor ve hikayemiz başlıyor ...

# İPUCU 1: **FAYDALI BİLGİLER**

Düşünün: bir virüs bilgisayarınıza telefon ağı yoluyla sızar, gecenin bir yarısında telefonunuzu açar ve bir füze başlatma emri gönderir. Bu bir Hollywood senaryosu ama gerçek dünyada, zararlı yazılımlar genellikle çok farklı bir şekilde çalışır ve başka amaçları vardır. Bilgisayar sistemlerinin güvenlik açığı ve kullanıcıların bilgi güvenliğinin temel ilkelerini bilmemesi, herhangi bir kötü amaçlı yazılımın başarısı için temel bileşenlerdir. İnanılmaz gelebilir, ancak bir bilgisayar korsanının bilgisayarınıza virüs bulaştırırken arka planda korkutucu bir müzik ile tuhaf bilgiler yazmasına gerek yoktur. Bunun için kötü amaçlı bir dosyanın bulunduğu bir e-posta yeterlidir. Kurban, mesajın doğruluğuna inanırsa, kötü amaçlı uygulamayı kendisi başlatacaktır. Bu nedenle, siber suçlulara karşı korunmak için tehditlerin ne olduğunu anlamanız önemlidir.




PAROLA OLUŞTURURKEN ***GERÇEKTEN*** YARATICI OLUN...

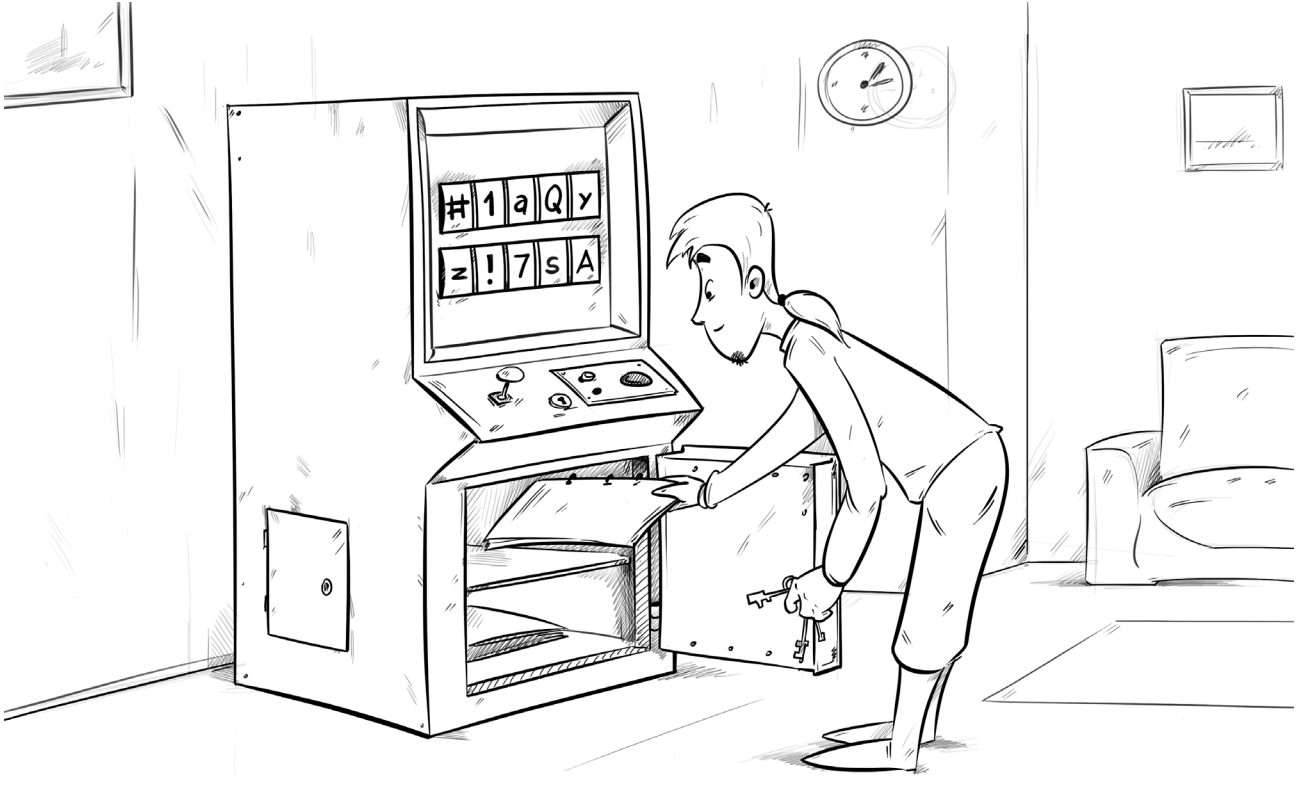
# İPUCU 2: **PAROLA GÜCÜ**

Bilgisayar korsanları, daha önce çevrimiçi olarak kullanılmış veya sızdırılmış milyonlarca parola içeren özel bir dağarcık ile çalışmalarına başlarlar. Bu gezegende, sizin gibi düşünen birçok kişi var, bu nedenle şifreniz bu listede olabilir. Ortak sözler, şarkı sözleri, film adı, kedinizin adı, doğum tarihiniz veya kolaylıkla tahmin edilebilecek veya sosyal medyada bir şifre olarak bulunabilen hiçbir bilgiyi kullanmamalısınız.

GÜÇLÜ PAROLA KIRILMAYI ZORLAŞTIRIR....
... VE ONLARI GERÇEKTEN KIRILMAZ HALE GETİRİR.

# İPUCU 3: **GÜÇLÜ BİR PAROLA**

İlişkilendirme, zor bir parola oluşturmanın en kolay yoludur. Kaydolmakta olduğunuz hizmet veya web sitesi ile ilişkili bir cümleyi yazın, yazın, birkaç sayı ve harf ekleyin. İşte bu güçlü bir paroladır. Böyle bir parolayı hatırlamak kolaydır ve yalnızca sizin için anlamlıdır.

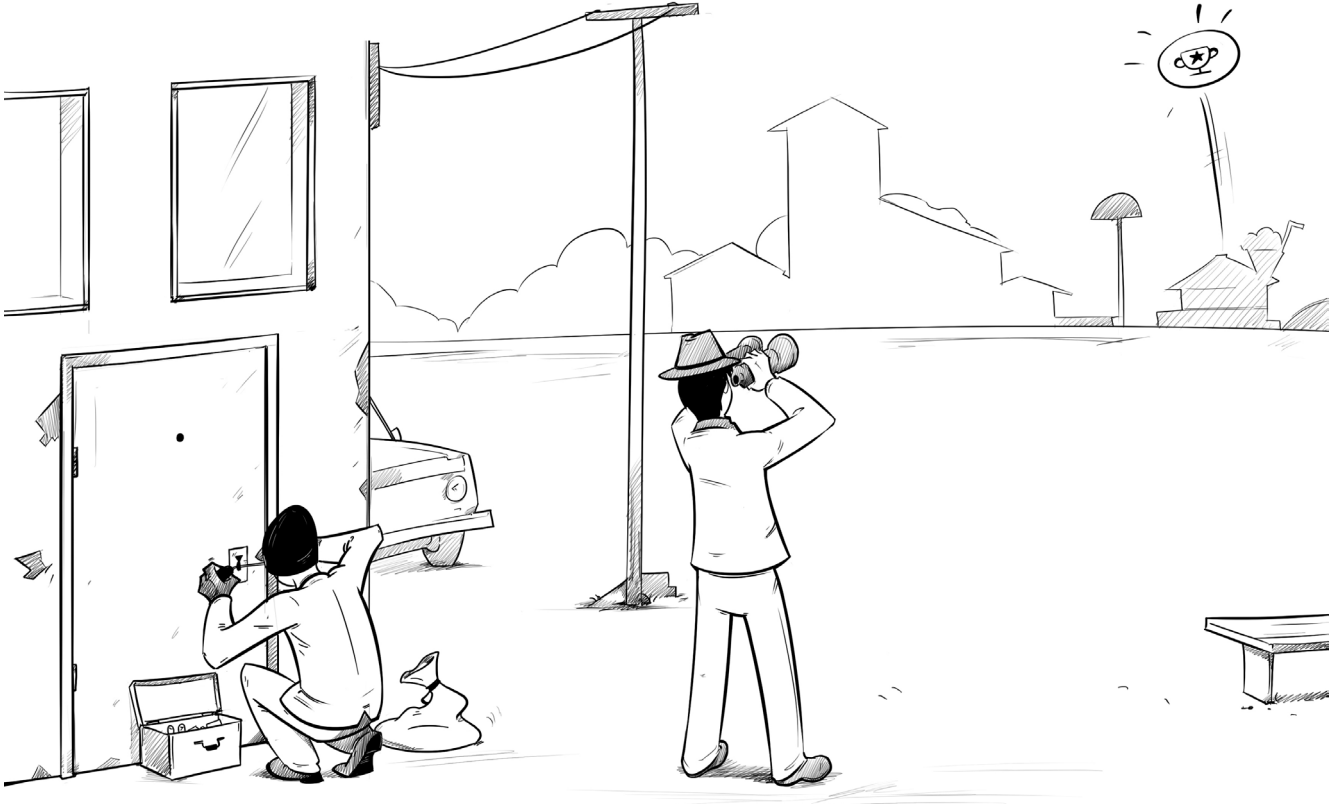



PAROLALARINIZI SAKLAMAK İÇİN PAROLA YÖNETİCİSİ KULLANIN, NOT KAĞIDI DEĞİL.

# İPUCU 4: **PAROLA SAKLAMA**

Parola ne kadar zor olursa, tahmin etmek o kadar zor olur. Parola ne kadar kolay olursa hatırlamak o kadar kolaydır. Bu yüzden hem zor hem de kolay olmalıdır ama maalesef herkes iyi bir tane bulamayabilir. Eğer İPUCU 3 sizin için uygun değilse, o zaman özel bir parola yöneticisi uygulaması kullanın. Bu uygulamalar, çevrimiçi hizmetler, sosyal medya, uygulamalar vb. için zor, benzersiz parolalar oluşturacak ve daha sonra kodlanmış veritabanına kaydedilecektir. Sana kalan tek şey, yönetici için bir ana parola oluşturmaktır. Unutmayın: parola zor olmalı, böylece kimse tahmin edememeli ama hatırlaması da kolay olmalıdır!

BİR KAFEDE YAPTIĞINIZ BİLDİRİMİN GİZLİ OLMADIĞINI BİLİYOR MUYDUNUZ?



# İPUCU 5: **SANAL CASUSLUK**

Geçmişte suçlular sizi, evinizi, kır evinizi veya arabanızı uzaktan izlerdi. Ancak artık bu durum o kadar da geçerli değil. Bugünün hırsızları, gittiğiniz yerlerde bildirim yapmayı alışkanlık haline getirdiyseniz nerede olduğunuzu ve nerede olmadığınızı öğrenmek için sosyal medyadaki haber listenize abone olabilirler. Bir dahaki sefere bildirim yaparken Swarm veya Facebook hesabınızda kaç tane gerçek ve eski arkadaşınız olduğunu göz önünde bulundurun.


KİŞİSEL EŞYALARINIZI FAZLA PAYLAŞMANIZ HIRSIZLIKLA SONUÇLANABİLİR
1200 $
340 $
2700 $

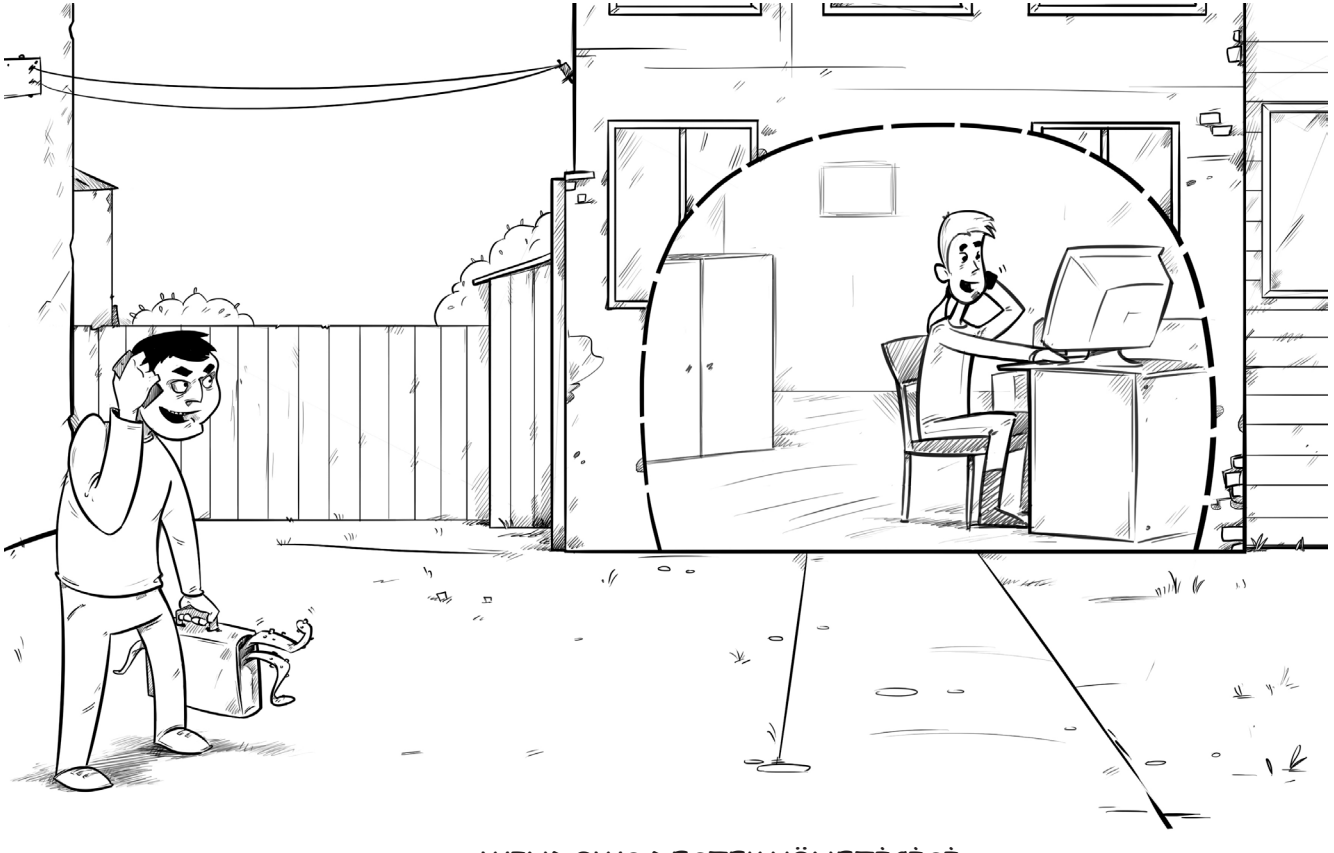
# İPUCU 6: **GÜZEL HAYAT**

Suçlular, sosyal medyayı en az bizim kadar, hatta daha da iyi kullanabilirler, çünkü bu tür beceriler onlara kazanç olarak geri dönebilir. İnternetteki lüks daire, yeni araba veya pahalı dizüstü bilgisayar fotoğraflar veya önümüzdeki hafta sevdiklerinizle birlikte tatile gideceğiniz hakkındaki bir bilgi sizi bir hedef haline getirebileceğinden, kendi güvenliğiniz için sanal hayatta daha mütevazı olmanız gerekir.

WEBCAM'İNİZİ SİZİ İZLEMEK İÇİN KULLANABİLİRLER.

# İPUCU 7: **FARKEDİLEMEYEN CASUS**

Web kameraları, arkadaşları veya yakınları uzakta yaşayan insanlar için mükemmeldir. Ancak, lütfen kameralarınızın, yasadışı yoldan özel hayatınızda olanları göstermeyeceğinden emin olun. Bilgisayar korsanları bunları farklı şekillerde kullanabilirler. Her şey hayal dünyalarına ve hikayelerine bağlı. Fotoğrafları ve videoları bir porno sitesine satabilir veya kullanıcıya şantaj yapabilirler. Böyle bir sorunla karşılaşmak istemiyorsanız, kameranıza erişimi denetleyen virüsten koruma uygulaması korumasını kullanın.



WINDOWS DESTEK YÖNETİCİSİ,
DOLANDIRICILAR ARASINDA YAYGIN KULLANILAN BİR ARAÇTIR.

# İPUCU 8: **TELEFON DOLANDIRICILIĞI**

"Merhaba, Ben Windows Teknik Destek uzmanıyım. Bilgisayarınızda çok tehlikeli bir virüs bulunuyor, "- Bu, telefonla çalışan bir dolandırıcı ile konuşmanın muhtemel bir başlangıcıdır. Şu an için her şey kolaydır: saldırgan, bilgisayara virüs bulaştığına sizi ikna eder ve ardından kesinlikle yardımcı olacak bazı işlemler yapmasını önerir. Ancak gerçek zararlı yazılım, "uzman tarafından" önerilen "eylemler" dir. Asla unutmayın: Microsoft Teknik Destek, bilgisayarınızda kaç virüs olursa olsun sizi aramayacaktır.