



Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

ARALIK 2019

Telefonum Çalınırsa

GÜZEL BİR GÜNDE bir arkadaşınızla buluşmak üzere evden çıktınız. İki ayrı toplu taşıma aracıyla Karaköy'e vardınız. Arkadaşınızla denize nazır bir kafede çay içip sohbet etmek için buluştunuz ve fark ettiniz ki **telefonunuz yok.**

Düştü mü, çalındı mı, nerede, hiçbir fikriniz yok Bu durumda en kötüsünü, yani çalındığını düşünüp bazı önlemler almakta fayda var. Bu durumda en kötüsünü, yani çalındığını düşünüp bazı önlemler almanızda fayda var. Örneğin popüler bir seçim olduğu için bir Android 8.0 telefon kullandığınızı düşünelim. Önlemler temelde ikiye ayrılıyor:

- 1) Telefonunuzu kaybetmeden önce yapmanız gerekenler
- 2) Telefonunuzu kaybettikten sonra yapmanız gerekenler

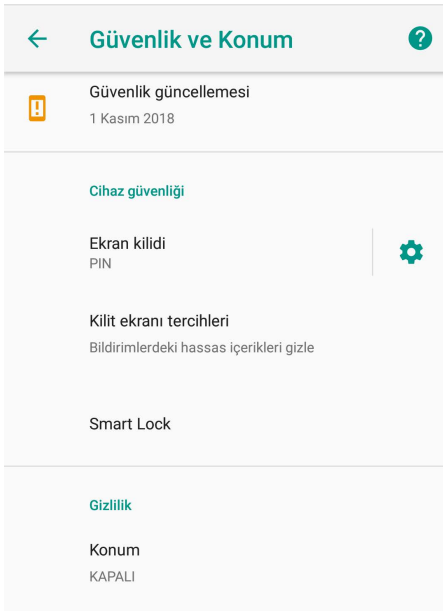
Telefonunuzu kaybetmeden önce yapmanız gerekenler:

- » Her şeyden önce telefonunuzun mutlaka bir ekran kilidi olmalı. Bunun için çeşitli alternatifler söz konusu; telefonunuzun ekranı parmak izi ile açılıyor olabilir ya da 4 ya da daha fazla sayıdan ya da karakterden oluşan bir şifresi bulunabilir; ya da ekranda çizeceğiniz bir şekille açılabilir. Bunlar arasında benim en sakıncalı bulduğum ekran üzerine çizilen şekildir çünkü bu telefonunuzu

telefonunuzu çalma niyetiyle sizi gözlemleyen biri tarafından çok kolayca öğrenilebilir. Benim önerim 6 ya da 8 haneli bir sayısal şifre kullanmanız. Eğer bu bile size çok zor geliyorsa, her ne kadar sanıldandan daha az güvenli olsa da parmak izi okuyuculu bir telefon almanızı öneririm. Şifreli ekran kilidi, telefonunuzu her kullanmak istediğinizde girmeniz gereken bir şey olduğu için biraz can sıkıcı olabilir ama inanın bana, birilerinin telefonunuza şifresiz ulaşması sonucu yaşayacağınız can sıkıntılarınıyla karşılaştırıldığında bir hiçtir. Eğer sadece bir tek önlem alacaksanız bunu uygulayın.

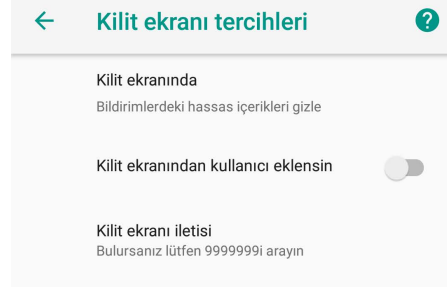
» Cihazımı Bul:

Bu özellik sayesinde cihazınızın nerde olduğunu (eğer kapatılmamışsa) bulmanız mümkün. Çalınmanın söz konusu olmadığı durumlarda sizi birçok zahmetten kurtaran son derece faydalı bir özellik. Ne var ki çalındıysa, muhtemelen telefon kapatılacağı için pek bir işe yaramıyor. Ayrıca işe yaraması için devamlı konumunuzun açık olması da gerekmektedir.



» Kilit Ekranı İletisi:

Yine telefonunuzu kaybettiğiniz durumda, bulan birilerinin size ulaşabilmesi için Kilit Ekranı Tercihleri altında Kilit Ekranı İletisini "Bulursanız lütfen xxxxxx'i arayın" gibi bir yazıya çevirirseniz, telefonunuzu bulma ihtimaliniz artar (kendi telefonunuzu yazmayın, çünkü onu kaybettiniz!)

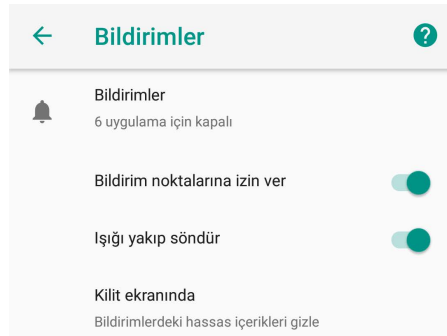


» Hesaplarınızın Güvenliği:

Genellikle uzmanlar hesapların güvenliği için, gerekli olan hemen her yerde çift faktörlü güvenlik (bir şifre + sms vs.) kullanılmasını öneriyor. Diğer konularda bunu yapmaya üşeniyor olsanız da banka hesapları ve benzeri kritik hesaplarda üşenmemenizi öneririm.

» Bildirilerin Güvenliği:

Yukarıda bahsettiğim kritik mesajların (banka sms'lerinin ya da uygulamalardan gelen ikincil şifrelerin) telefonun kilitli halinde görünmesini istemezsiniz. Zira bu durumda telefonunuzu ele geçiren biri telefonunuzu açmadan bile bu ikincil şifrelere ulaşabilir. Bunun için Ayarlarda, Uygulamalar ve Bildirimler ekranı altındaki Bildirimler menüsünde "Kilit Ekranında Bildirimlerdeki Hassas İçerikleri Gizle"yi seçmeniz gerekmektedir.



Telefonunuzu kaybettikten sonra yapmanız gerekenler:

Bir telefonun kaybı durumunda dört kritik bilgi başkalarının eline geçebilir ve bunlar başta sizin ve tanıdıklarınızın dolandırılması olmak üzere birçok kötü niyetli amaçla kullanılabilir:

- » **E-postalarınız:** Yıllardır silmediğiniz e-postalarınızın içinde, bir yere yolladığınız resmi belge fotokopileri (nüfus kağıdı, pasaport vs.) bulunabilir.

- » **Uygulama hesapları:** Başta bankacılık ve e-ticaret uygulamaları olmak üzere, şifrenizin kayıtlı olduğu uygulamalarda sizin adınıza ticari işlemler yapılabilir ya da o telefondaki e-postanız üzerinden şifreler resetlenebilir.
- » **Anında mesajlaşma ve e-posta uygulamaları:** Bunlar üzerinden tanıdıklarınızla sizmiş gibi bağlantı kurulabilir, para ya da yardım istenebilir.
- » **Fotoğraflarınız:** Belge fotoğrafları dolandırıcılık gibi kötü amaçlarla kullanılabilir. Tabii telefonu kaybettiğinizde maddi zararın yanı sıra, bir daha gelmeyecek yedeklenmemiş fotoğraflarınızın kaybolacağını da unutmayın.

Eğer sim şifreniz yoksa, sizin adınıza yapılacak konuşmaların (büyük maliyetli yurt dışı konuşmalarının ya da tanıdığınız birilerini dolandırmaya yönelik konuşmaların) engellenmesi için telefonu kaybettiğinizde sim kartını iptal ettirmenizde fayda var. Benim ekran kilidim var diye güvenmeyin; başka telefona takıp kullanabilirler. Burada değinilmesi gereken küçük bir ayrıntı da, yeni sim kartı çıkarıldığında, olası dolandırıcılıkları engellemek için bankaların bir süre SMS doğrulama hizmetini durdurmasıdır, başka bir deyişle bir iki gün banka işlemi yapamayabilirsiniz.

Telefonunuz gasp edildiyse ya da çalındığından eminseniz, bir karakola uğrayıp tutanak tutturmanız gerekir. Telefon şirket telefonuyla ya da sigortalı bir telefonsa, sizden tutanak talep edilecektir.

Bir tanıdığınızın telefon ya da bilgisayarından Google hesabınıza girip, kaybettiğiniz telefondaki Google oturumunu kapatmanız da iyi olur. Böylece, bir şekilde telefonunuzu açmayı başarsalar bile başta sizin e-postalarınız olmak üzere telefondaki kritik bilgilere ulaşamayacaklardır.

Uzun sözün kısası, telefonunuzu kaybetmek her ne kadar tatsız bir süreç olsa da, yukarıda belirttiğim bazı basit önlemleri aldığınız takdirde telefonun maddi değeri ve kaybolan yedeklenmemiş fotoğraflarınız dışında hayatınız pek etkilenmeyecektir.

YAZAR HAKKINDA

KIVILCIM HİNDİSTAN yaklaşık olarak 25 yıldır telekom, e-ticaret ve yazılım firmalarında Bilgi Teknolojileri ve Güvenlik alanlarında çalışmaktadır. Ayrıca Fazlamesai.net'in de kurucularındandır.



[linkedin.com/in/kivilcimhindistan/](https://www.linkedin.com/in/kivilcimhindistan/)
twitter.com/kivil

YASAL UYARI

Bu dokümanın tüm hakları Lostar Bilgi Güvenliği A.Ş.'ye aittir ve Creative Commons BY-NC-ND 4.0 (Attribution-NonCommercial-NoDerivatives 4.0 International - (CC BY-NC-ND 4.0) lisansı altında dağıtılır. Herhangi bir değişiklik yapmadan kaynak gösterilerek dağıtılabilir. Ticari olarak kullanılamaz.