AKILLI TELEFON GÜVENLİĞİ (ANDROID)

1. Telefonunuzda PIN ayarlayın ve şifreleyin.
Telefonunuzun kaybolması veya çalınması durumlarında, telefonunuzun izinsiz kullanımını önlemek için, telefonunuzun ana ekranına Kişisel Kimlik Numarası -şifre/PIN- ayarlaması yapın. Mümkün oldukça e-posta, bankacılık, kişisel siteler gibi sitelerin her biri için farklı bir şifre kullanın.

2. Akıllı telefonunuzun güvenlik ayarlarını değiştirmeyin.
Güvenlik ayarları üzerinde değişiklik yapmamanız tavsiye edilir. Telefonunuzun fabrika ayarlarının ve işletim sisteminin ayarlarının değiştirilmesi (jailbreak, rooting) gibi işlemler, akıllı telefonunuzu siber saldırılara karşı daha duyarlı yaparken, işletmeciniz ve akıllı telefonunuz tarafından sunulan güvenlik özelliklerini zayıflatmaktadır.

3. Akıllı telefonunuzu yedekleyin ve veri güvenliğini sağlayın.
Telefonunuzda saklamış olduğunuz bütün verileri (rehber öğeleri, belgeler, fotoğraflar vb.) yedeklemeniz tavsiye edilir. Söz konusu bu veriler kişisel bilgisayarınızda, harici depolama aygıtlarında veya bulut ortamında saklanabilir. Böylelikle kayıp, çalıntı durumlarında rahatlıkla telefonunuzdaki verileri geri yüklemek mümkün olabileceği gibi aksi durumda söz konusu veriler kaybedilme, çalınma veya silinme riskleriyle karşı karşıyadır.

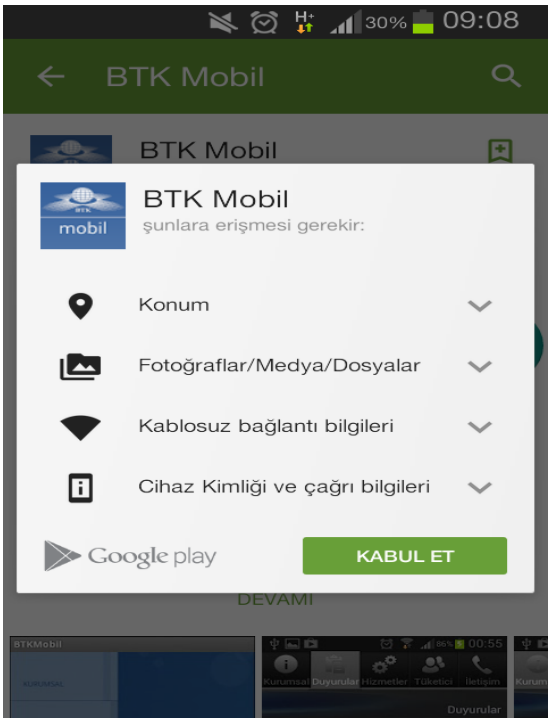
4. Yalnızca güvenilir kaynaklardan gelen uygulamaları yükleyin.
Bir uygulamayı indirmeden önce, uygulamanın yasal ve güvenilir olduğundan emin olmak için araştırma yapın. Akıllı telefonlarınıza indireceğiniz uygulamaları, işletim sisteminizin resmi uygulama ortamından edinmeniz önemle tavsiye edilir.

- Android: Google Play

Uygulamanın yasal olduğundan emin olmak için; yorumlara göz atmak, uygulama ortamının meşruiyetini araştırmak ve uygulama sponsorlarının resmi web sitesinde yer alan bağlantılar ile uygulama ortamlarındaki bağlantıları karşılaştırarak tutarlılığı sağlamak gibi yöntemleri deneyebilirsiniz. Güvenilmeyen kaynaklardan gelen uygulamalar; bilgi çalan, virüs yükleyen ve telefonunuzun içeriğine zarar veren istenmeyen yazılımları içerebilir.

5. Uygulamayı kabul etmeden önce uygulamaların kişisel bilgilerinize erişim yetkisi hakkında daha dikkatli olun.

Uygulamaların, akıllı telefonlarınızda bulunan kişisel bilgilerinize erişme yetkisi konusunda dikkatli olmanız tavsiye edilir. Aksi halde indireceğiniz uygulama ile kişisel bilgileriniz (örneğin konum veriniz) üzerinde işlem yapılmasına izin vermiş olabilirsiniz. Ayrıca yüklemeden önce her uygulama için gizlilik ayarlarını kontrol ettiğinizden emin olun.



6. Akıllı telefonunuza uzaktan erişim ile silmeyi etkinleştiren güvenlik uygulamalarını yükleyin.

Akıllı telefonlarda, uygulama olarak edinilebilecek veya varsayılan olarak yaygın olarak kullanılan önemli bir güvenlik özelliği; telefonun GPS'i kapalı olsa bile, telefonunuzda depolanan tüm verilere uzaktan erişebilmeye ve söz konusu verileri silebilmeye imkân sağlamasıdır. Bu durumda telefonunuzu kaybettiğinizde, telefonunuz sessiz olsa bile bazı uygulamalar yüksek sesli bir alarmı aktif edebilir. Bu uygulamalar aynı zamanda telefonunuzu kaybettiğinizde daha kolay bulabilmenize yardımcı olabilir.

7. Akıllı telefonunuzun yazılım güncellemelerini yapmayı unutmayın.

Otomatik güncellemeleri etkinleştirerek, telefonunuzun işletim sistemini güncel tutmalısınız veya servis sağlayıcınızdan, işletim sistemi sağlayıcınızdan, cihaz üreticisinden ve uygulama sağlayıcınızdan gelen güncellemeleri kabul etmelisiniz. İşletim sisteminizi güncel tutarak, siber tehditlere maruz kalma riskinizi azaltabilirsiniz.

8. Açık Wi-Fi ağlarına bağlanırken dikkatli olun.

Eğer halka açık bir Wi-Fi ağı kullanıyorsanız, telefonunuz siber suçluların kolay hedefi olabilir. Özellikle kişisel veya hassas bilgilerinize erişirken, söz konusu riske maruz kalma ihtimalini azaltmak için; halka açık ağ kullanımını kısıtlamalı ve onun yerine güvenebileceğiniz bir operatöre ait güvenli Wi-Fi veya kablosuz mobil bağlantı kullanmalısınız.

9. Eski telefonunuzu vermeden veya satmadan önce kişisel verilerinizi silin.

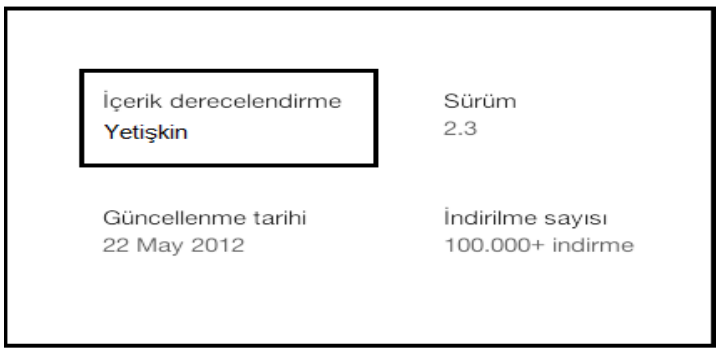
Telefonunuzu satmak istemeniz durumunda, akıllı telefonunuzda kişisel verileriniz olabileceğini unutmayın. Gizliliğinizi korumak için, verileri tamamen silin veya telefonunuzu fabrika ayarlarına sıfırlayın. Aksi takdirde akıllı telefonunuzdaki verilere rızanız haricinde erişilebileceği gibi kişisel verilerinizin istenilmeyen kullanımı söz konusu olabilecektir.

Aynı zamanda sıfırlama işleminin; telefonunuzda yer alan uygulamalar, mesajlar, arama geçmişi, müzik, fotoğraf gibi içeriklerin silinmesini de kapsadığını unutmayınız.

10. Çalınan akıllı telefonu bildirin.

Telefonunuzun çalınması veya kaybolması durumunda, hattınızı kapatmak için işletmenize başvurun. Telefonunuzun ülkemizde kullanımını engellemek için durumu BTK'ya bildirebilirsiniz. Konuya ilişkin ayrıntılı bilgiye buradan ulaşabilirsiniz.

11. İçerik Derecelendirmelerini Göz Önünde Bulundurun.



Tanınmış bazı uygulama mağazalarındaki uygulamalar aynı zamanda içerik derecelendirmeleri de sunmaktadır. Derecelendirmeler, bir uygulamanın çocuklar için uygun olup olmadığı noktasında size yardımcı olabilmektedir.

Genel olarak derecelendirmeler aynı zamanda uygulamanın içeriğine ve temasına (şiddet, argo/saldıgan dil, cinsel içerik, uyuşturucu vb…) ilişkin fikir verebilmektedir.

Her uygulama mağazasının kendine göre içerik puanlama yönteminin olabileceğini unutmayınız.

12. Telefonunuza Cüzdanınız Gibi Davranın

Genel olarak derecelendirmeler aynı zamanda uygulamanın içeriğine ve temasına (şiddet, argo/saldıgan dil, cinsel içerik, uyuşturucu vb…) ilişkin fikir verebilmektedir.

Her uygulama mağazasının kendine göre içerik puanlama yönteminin olabileceğini unutmayınız.

Parasal işlemlerin yönetilmesinde akıllı telefonların kullanımı giderek yaygınlaşmaktadır. Mobil bankacılık uygulamalarının, çeşitli avantajları bulunduğu gibi, bazı risklerinin olduğu da unutulmamalıdır.

Bu noktada, bankacılık uygulamasında oturum kapatmak (logging out), yalnızca resmi uygulama mağazalarından uygulama indirmek, telefonunuzun fabrika ayarlarını değiştirmemek ve telefonunuza şifre/parola koymak gibi temel bazı önemli hususlar göz önünde bulundurulmalıdır.

13. Maliyetlerin Farkında Olun, Özellikle Uluslararası Dolaşım (Roaming) Konusunda

Uygulamalar, sizin mobil veri kullanım limitinizden daha fazla veri kullanımına neden olabilmekte olup, bu durum yüksek faturalarla karşılaşmanıza yol açabilecektir. Pek çok mobil işletmecinin sunmuş olduğu çevrim içi araçlar veya uygulamalar veri kullanımınızı kolayca yönetmenize yardımcı olmaktadır.

Bunun yanında, bu uygulamaların yurtdışında kullanımı yüksek faturalara neden olabilmektedir. Fatura şokları ile karşılaşmamanız için yurtdışı dolaşımlarınızda (roaming) telefonunuzun veri akışını kapalı tutunuz.

Yurtdışı telefon kullanımlarınızda fatura şokları ile karşılaşmamanız için dikkat edilecek hususlara buradan erişebilirsiniz.

14. Ebeveynlerin Uygulama İçi Satın Alımlara Dikkat Etmesi Gerekmektedir.

Pek çok ücretli/ücretsiz uygulama, ilave hizmetler/ekstralar için ayrıca ücret talep edebilmektedir. Bu yöntem ile yapılan satın alımlara uygulama içi satın alımlar denilmektedir. Örneğin, bir oyun uygulamasında ileri seviyelere geçilmesi veya oyun hızının arttırılması için ilave ücret verilmesi bu kapsama girmektedir.

Bu noktada, çocuklar ebeveynlerin rızası dışında, söz konusu oyunlar veya uygulamaları kullanarak uygulama içi satın alımlar yapabilmekte olup, bu durum yüksek faturalara neden olmaktadır. Bu noktaya ebeveynlerin özellikle dikkat etmesi gerekmektedir.

Ayrıca, uygulama mağazasında sunulan bazı araçlar da istenmeyen uygulama içi satın alımların kontrol edilmesine yardımcı olabilmektedir. Örneğin, bazı araçlar, her indirme ve satın alma için şifre girilmesine imkan verebilmektedir.