



DİJİTAL AYAK İZİ NEDİR?

Sosyal medya platformları, uygulamalar, web siteleri, video kanalları ve bunun gibi teknolojik ağlar, gündelik yaşamla ayrılmaz bir bağ içerisinde. Alışverişten eğitime, kültür sanat etkinliklerinden bankacılığa kadar birçok işlemimizde interneti kullanıyoruz.

Tüm bu işlemlerin arkasında ise bir geçmiş bırakıyoruz: Dijital izler.

Dijital ayak izi; İnternette olan her kullanıcının, online ortamda bıraktığı izlere denir.

Sosyal medya platformlarında yapılan **gezintiler**,

Online alışveriş esnasında e-ticaret siteleriyle paylaşılan veriler,

Bir uygulama indirirken verilen izinler,

Mail trafiği,

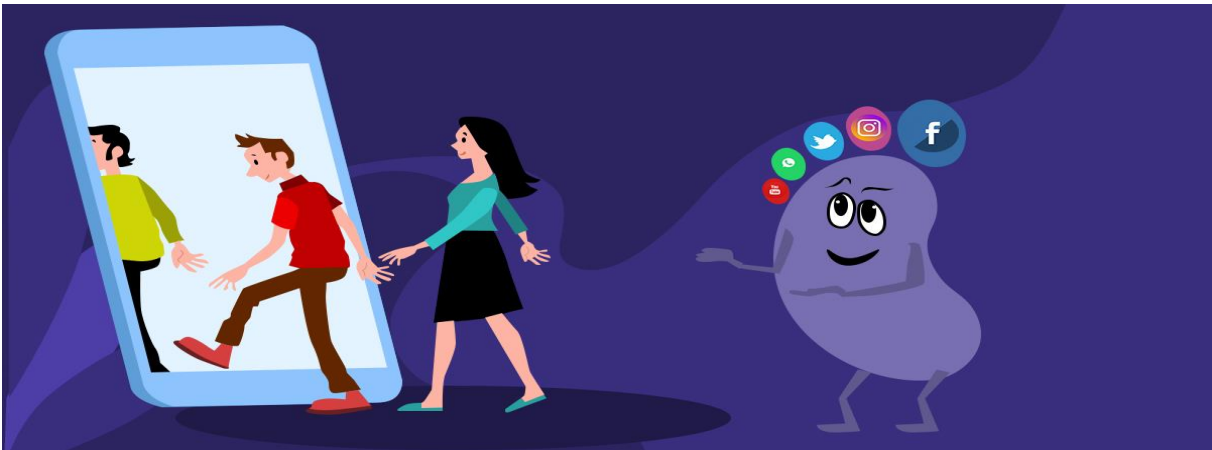
Google aramaları bile dijital ayak izine dahildir.

Aktif ve pasif olarak iki türe ayrılır.

Pasif dijital ayak izi, istenmeden bırakılan verilere deniyor; arama motorları tarafından kaydedilen arama geçmişleri buna örnek olarak gösterilebilir.

Aktif dijital ayak izleri ise blog, sosyal medya paylaşımları, uygulama tercihleri gibi bilinçli olarak verilen izinlerle oluşan veri geçmişini tanımlıyor.

Dijital ayak izleri eğer bilinçsiz bir şekilde karşı tarafa bırakılırsa, kötü niyetli yazılımlar veya şahıslar tarafından ele geçirilebilir.



Dijital ayak izimiz nasıl kullanılır?

Reklamlar: İnternet gezintimiz sırasında kaydedilen veriler, aktif olarak bulunduğumuz her dijital platformda istenen/istenmeyen reklam olarak geri bize dönebilir. Her ne kadar bunları engellemek mümkün olsa da reklamlardan yüzde yüz kaçabildiğimiz bir sistem henüz yok.

Kimlik bilgileri: E-ticaret, site üyeliği gibi veri onayının gerektiği platformlardaki kimlik bilgilerimiz aktif dijital ayak izleri olarak kayıt altına alınır. Bu kimlik bilgileri kötü niyetli şahısların eline geçtiğinde çeşitli siber suçlar için kullanılabilir. Bu nedenle sitelere üyelik sırasında verdiğimiz izinlere ekstra dikkat etmemiz gerekiyor. Benzer şekilde herhangi bir uygulamayı telefonumuza indirdiğimizde nelere erişim izni verdiğimizize (konum, telefon rehberi,

SMS okuma izni, çağrıyı yönlendirme izni vb.) dikkat etmeliyiz. Bu izinlerin pek çoğunu reddederek bilgilerimizi paylaşmamayı tercih edebiliriz. Veya herhangi bir uygulama indirirken (şimdilik iOS için geçerli) gizlilik ayarlarından 'Uygulama Beni Takip Etmesin' seçeneğini seçebiliriz.

Kişisel fotoğraf ve videolar: Sosyal medya platformlarında paylaştığımız fotoğraflar ve videolar veri arşivlerinde tutulur. Bu medyalar bir şekilde üçüncü taraflar tarafından görüntülenirse, görsellerimizin kullanıldığı birçok anonim hesap ortaya çıkabilir veya daha da kötüsü adımıza sahte paylaşımlar yapılabilir.

Özel sohbetler: Dijital ortamlarda ve özellikle yüksek güvenliği olmayan mecralarda yaptığımız sohbetler de dijital ayak izi olarak kaydedilebilir. Bu sohbet içerikleri üçüncü taraflarca çeşitli siber dolandırıcılık saldırıları için kullanılabilir.

DİJİTAL AYAK İZİMİZİ NASIL AZALTIRIZ?

Sosyal medya hesaplarında gizlilik ayarı yapmak: Kişisel yaşamımıza dair birçok bilgiye yer verdiğimiz sosyal medya platformlarında temel bir gizlilik ayarı yapmamız şart. Hesabımızı sadece takipçilerimiz için açık tutmalı ve gerekirse paylaşımlarımızı yalnızca güvendiğimiz hesapların erişimine açmalıyız.

Kayıt esnasında verilen bilgilerin kontrolü: Üyelik esnasında birçok site doğum tarihi, konum, adres bilgisi gibi veriler ister veya bu verilere izinler dâhilinde otomatik olarak erişir. Kullanmadığımız web platformlarındaki hesapları silmek, kullandığımız hesaplarda ise verdiğimiz izinleri kontrol etmek güvenliğimiz için büyük önem taşır.

E-bülten üyeliklerinin kontrolü: E-posta adresimizi yalnızca güvenilir kurumlara verdiğimizden emin olmalıyız. Aksi durumda adresimiz ve kişisel bilgilerimiz birçok kurum ve sektör tarafından kullanılabilir. Bülten aboneliklerimizi düzenli kontrol ederek çeşitli güvenlik açıklarının önüne geçebiliriz.

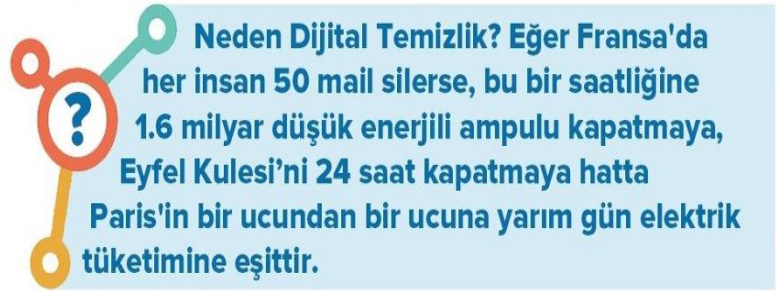
Sosyal medya hesap şifreleri: Farklı sosyal medya platformları için aynı şifreleri kullanmamalı, şifreleri 6 ayda bir düzenli olarak değiştirmeliyiz. Bu platformlarda İki Faktörlü Kimlik Doğrulaması özelliğini aktif hale getirmeliyiz. Herhangi bir hesabın şifresinin ele geçirilmesi durumunda tüm hesaplarda yer alan verilerimiz tehlikeye girebilir.

Dijital karbon ayak izi ve azaltma yolları

Dijital ayak izimiz olduğu gibi, bir de bunun çevreye olan etkileri var tabii ki:

Dijital karbon ayak izi.

Web'de yaptığımız her bir gezinti ve işlemin karbon emisyonuna katkıda bulunması anlamına geliyor. Dünyanın en popüler arama motoru olan Google'da 1 günde gerçekleşen 3 küsur milyar arama işleminin internetteki tüm karbon ayak izinin yaklaşık %40'ını oluşturduğu biliyor muydunuz? (1) Buna sosyal medya paylaşımlarını, arka planda çalışan uygulamaları, mail



trafiğini, video akışını da dahil edersek, internet kullanımının önemli oranda karbon ayak izine neden olduğunu söyleyebiliriz. Peki dijital karbon ayak izimizi azaltmak için neler yapabiliriz?

- Depolamayı düşürmek için e-posta kutusunu düzenli olarak temizleyebiliriz.
- İş maillerinde gerek olmadıkça CC ve BCC kullanmaktan kaçınabiliriz.
- Kullanmadığımız anlarda bilgisayarları tamamen kapalı tutabiliriz. Uygulamalarımızdan çıkış yapabiliriz.
- Kesintisiz video izlemek yerine daha az enerji harcamak için videoyu indirebilir veya düşük çözünürlükte izlemeyi tercih edebiliriz.
- Sosyal medya platformlarında daha az zaman geçirmeye çalışabiliriz.
- Web sitelerindeki otomatik video oynatma özelliğini kapatabiliriz.
- Bulut depolama yerine harici bellekleri tercih edebiliriz.

NEDEN DİJİTAL TEMİZLİK YAPMALIYIZ?



Akan çevrimiçi **videonun** ortalama CO2 tüketimi yılda **300 milyon tonun** üzerindedir. Bu, **İspanya'nın** bir yıl içinde yaydığı CO2 ile aynı.