10 Ağustos 2023

Siber Tehditler ve Bilgi Güvenliği Semineri

Temel Kavramlar

Bilgi Nedir?
Bir kurumun faaliyetlerini yürütmekte kullandığı verilerin anlam kazanmış halidir.

Kişisel verilerimiz, çalıştığımız kurum verileri, bir işi yaparken kullandığımız kişi için önem arz eden her şey bilgidir!..

Bilgi kurumun en değerli varlığıdır!
Korunması ve verimli kullanılması şarttır!

Bilginin bulunduğu yerler:
- İnsanda (sözlü)
- Kağıt Üzerinde
- Bilgisayar Sisteminde
- Fiziksel Ortamlarda

Bilgi Güvenliği Nedir?
Kurumun en değerli varlığı olan bilgiyi kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve kötü niyetli kişilerin eline geçmesini engellemektir!

GİZLİLİK (Kim?)
Bilgi ve erişime izni olan yetkili kişilerin bilgiye erişimini sağlamaktır!

BÜTÜNLÜK (Ne?, Ne zaman?)
Bilginin yetkisiz kişi veya işlemler tarafından değiştirilmemesini sağlamaktır.
Amaç bilginin tutarlılığının korunmasıdır.

Erişilebilirlik (Ne zaman?, nasıl?)
Bilgiye doğru zamanda erişimin ve erişim sürekliliğinin sağlanmasıdır.

Temel Kavramlar

Bilgi Güvenliğini oluşturan diğer 3 unsur:

Teknoloji

Süreç

İnsan

Teknoloji
Siber Güvenlik Risklerine Karşı Sistemleri Koruyan Yazılım ve Donanımlardır.

Süreç
Kurum ve Kuruluşların Bilgi Güvenliğini Sağlamak Üzere Hazırladıkları Politika/Prosedür ve Risk Analizi Çalışmalarıdır.

İnsan
Bilgi Güvenliği Sürecinin En Zayıf Halkasıdır!

Bilincinin ve Farkındalığının En Yüksek Olması Gereken Noktadır!

Güçlü Teknoloji Alt Yapısı ve İyi Tasarlanmış Süreçler Düşük İnsan Farkındalığı Karşısında Zayıf Düşecektir!

Temel Kavramlar

Bilgi Güvenliği Politikası Ne İşe Yarar?

- Personele yaptıkları iş kadar, iş yapış yöntemlerinin ve işledikleri bilginin değerini fark ettirir.
- Kurumu bilgi kaybı dolayısıyla uğrayacağı zarardan korur. Rekabetçi bir avantaj sağlar.
- Riskleri yönetilebilir kılır.
- Toplam kalitenin artmasına neden olur.

UYARILAR:

- Bilgi güvenliği politikası sadece bilgi işlemi ilgilendiren bir husus değildir.
- Tüm kurumun sahiplenmesi gereken bir süreç yönetimidir.
- Riskleri sıfırlamaz ama yönetilebilir kılar.
- Son kullanıcı desteği çok önemlidir.
- İşten önce gelmez.
- Zaman geçtikçe güncellenmesi gerekir
- Sadece idari yada teknik bir politika değil, bir farkındalık sürecidir.

Temel Kavramlar

Personelden Beklenenler:

- Binanın korunması
- Kilitlerin kontrolünün sağlanması
- BT bileşenlerinin korunması
- Fiziksel saldırı engelleme sistem ve alt yapısının olması
- Güvenlik personellerinin farkındalıkları
- Kapı giriş sistemlerinin tam teşekkülü olması
- Kamera sistemlerinin etkin kullanımı
- Temiz ekran temiz masa politikasına uyulması

Parola Güvenliği:

- En az 8 harften oluşmalıdır.
- Büyük, küçük harf ve özel karakter içermelidir.
- Harflerle oluşturulan kısım anlamlı olmamalıdır.
- Düzenli olarak değiştirilmelidir
- Başkaları ile paylaşılmamalıdır.
- Rahat erişilebilir şekilde saklanmamalıdır.
- Kolay temin edilebilecek yerde olmamalıdır.

We Are Social - Dijital Türkiye 2023

- 2023 yılında dünya nüfusu 8.1 milyara ulaşırken Türkiye nüfusu 85.59 milyona ulaşmış durumdadır.
- Dünya genelinde internet kullanıcıları 5.16 milyara ulaşmış durumda ve nüfusa göre kullanım oranı %64.4 ‘tir.
- Türkiye’de ise İnternet kullanıcıları 71.38 milyon kullanıcı ile nüfusun %83.4 ‘üne gelmektedir.
- Bu oran dünya geneline bakıldığından ortalamanın bir hayli üzerinde kalmaktadır.
- Dünya genelinde sosyal medya kullanıcılarının sayısı 4.76 milyar iken bu sayının nüfusa oranı da %59.4’tür.
- Türkiye'de ise aktif sosyal medya kullanıcıları 62.55 milyon kişiye ulaşmıştır.
- Türkiye’de nüfusa göre aktif sosyal medya kullanıcılarının oranı %73.1 iken internet kullanıcılarının büyük bir çoğunluğu sosyal medya kullanmaktadır.

We Are Social - Dijital Türkiye 2023

- Türkiye'de internet kullanıcıları tüm cihazlardan günlük ortalama 7 saat 24 dakika internette zaman geçirmektedir.
- Türkiye'deki internet kullanıcıları ortalama 2 saat 58 dakikasını sosyal medya üzerinde geçirmektedir
- Sosyal medya kullanıcılarının aylık ortalama kullandığı sosyal medya platformu sayısı da 7.6 'dır.
- İnternet kullanıcıları %90.6 ile en çok Instagram kullanmaktadır.
- Kullanıcılar aylık ortalama 21 Saat 24 Dakika ile en çok Instagram da zaman geçirmektedir.
- Türkiye'de en fazla kullanıcısı bulunan sosyal medya uygulaması ise 57.9 milyon kullanıcı ile YouTube 'dur.

We Are Social - Dijital Türkiye 2023

- Finansal içeriklere baktığımız zaman herhangi bir finansal kuruluşta hesabı bulunanların oranı %73.4'tür.
- Çevrimiçi ürün satın alma faktörlerinde en etkili sebep %57.3 ile ücretsiz teslimattır.
- İnternet üzerinden Tüketim mallarını satın alan kullanıcıların sayısı 44.03 milyon iken bu ürünler için kişi başına düşen yıllık harcama miktarı 474 dolardır.
- Dijital ödeme yöntemlerinin kullanan kişi sayısı 44.26 milyon iken bir yılda bu yolla yapılan ödeme miktarı 63.45 milyar dolar büyüklüğündedir.

Perspektif 2022-2023

Dijital, mobil ve sanal sosyal medya, dünyanın her yerindeki insanlar için günlük yaşamın vazgeçilmez bir parçası haline geldi. Şu anda 4,95 milyardan fazla insan interneti kullanırken, sosyal medya kullanıcıları 4,62 milyarı aştı.

- Yıllık ortalama 40 Zettabyte veri üretiyoruz.
- Bu verilerden sadece %25 değerlendirilebilir.
- Değerlendirilebilir Verinin %0.05 işleniyor..
- Dünya nüfusunun %60'ı sosyal medyada..
- Tiktok ve youtube kullanıcılarının %48'i mobil erişimli..
- Mobil uygulamalara harcanan para 170 Milyon $..
- Yıllık kişi başı online alışveriş miktarı 1000 $..
- Çin'de alışverişlerin %10'u online yapılmaktadır.
- Çalışan nüfustan internet kullanıcılarının %10'u Kriptoparalardan en az birini aldı.
- Gelişmekte olan ülkelerde kripto para pazarı diğerlerine göre çok daha hızlı artıyor. Türkiye'de Kripto para pazarı 2021 de %30 üzerinde arttı.

Rakamlar bize geniş bir Perspektif Sunar!

%58.4

4.62/7.91 Milyar İnsan Sosyal Ağlarda..

%62.5

4.95 Milyardan Fazla İnsan İnternette..

%33

Sosyal Ağ (2.24dk) İnternette (6.43dk) (Günlük)

%40

Uyku dışı İnternette Geçirilen Zaman

Dijital Obez misiniz?

Dijital medya içeriğinin aşırı tüketimi sonucunda bireyler bağımlı hale gelerek, daha fazla tüketme isteği duymakta ve dijital obez adayı haline gelmektedirler.

- Teknolojinin gün içerisinde aşırı tüketilmesi bireylerde fiziksel ve psikolojik sorun yaşatmaktadır!
- Ortalama 7 saat internetteyiz. 2 dakikada da 1 telefon ekran kontrolü yapıyoruz!
- Simüle edilmiş bir dünyada yaşamaya başladık ve isteklerimiz, arzularımız ve eylemlerimiz gerçeklikten uzaklaştı ve dijitalleşti.
- 40'a yakın dijital hastalık türü var. Dijital obezite, nomofobi, siberhondrik, fomo etkisi, tıkınmalı izleme, ego sörfü, sosyal medya dismorfofobisi bu hastalıkların en yaygın türleridir!
- Yapılan araştırmalara göre dünyada her 3 kişiden 1'i dijital obez adayı ya da obez şu anda. Nasıl ki vücuda ihtiyacı olan kalori miktarından fazla yükleme yapılınca obez bireyler olmaktadır!
- aynı biçimde dijital ortamlarda zihne aşırı yükleme de dijital obeziteye yol açıyor!

Teknolojinin Etkileri

Google Takibi
Etrafındaki insanları sürekli olarak internette aratmak.

Nomofobi
Cep telefonundan uzaklaşma kaygısı.

Ego Sörfü
Sürekli olarak ismini internette aratarak hakkında yazılanları öğrenme isteği.

Selfitis
Sürekli kendi fotoğrafını çekip sosyal medyada paylaşmak.

Siberkondri
Hastalığını internet üzerinden araştırarak çözmeye çalışmak.

Elektronik Uykusuzluk
Dinlenme saatleri esnasında dahi akıllı telefonla, tabletle, bilgisayarla uğraşmak.

Facebook Depresyonu
Olumsuz olayların sosyal platformlarda tekrar tekrar paylaşılması nedeniyle insanların depresyona sürüklenmesi.

Borderline Selfitis
Kişinin sosyal medyada paylaşmasa bile kendi fotoğrafını günde en az 3 kere çekmesi.

Fomo
Gelişmeleri takip edememe kaygısı.

Internet Siniri
Cihazlardaki performans düşüklüğünün kişide sinire neden olması.

Phubbing
Akıllı telefon bağımlılığı.

Photolurking
Sosyal medya hesaplarında sürekli fotoğraflara bakarak zaman geçirmek, paylaşımlarını kimlerin takip ettiğini kontrol etmek.

Hayalet Titreşim
Telefon çalmadığı zamanlarda dahi sürekli olarak titreşim hissetmek.

Cheesepodding
İnternetten sürekli olarak mp3 indirmek.

Dijital Obezite Ne Yapar!

- Dikkat dağınıklığı,
- konsantrasyon ve odaklanma sorunu,
- yüz yüze iletişimde azalma,
- sosyal hayattan kaçınma ve gerçek hayattan kopma,
- akademik gelişimin olumsuz etkilenmesi,
- sorumluluk almaktan kaçınma,
- kas ve iskelet ağrıları vb.
- bedensel sorunlar,
- dijital göz yorgunluğu ve diğer göz sorunları, uyku bozuklukları,
- anksiyete, depresyon vb. psikolojik hastalıklar,
- davranışsal bağımlılık, aile içi zayıf iletişim,
- sürekli veri-bilgi akışı ile zihnen ve bedenen yorgunluk,fizikselobezite

Bilgi Güvenliği

- Çalışanlar İçin Siber Güvenlik
- Sosyal Mühendislik
- Parola Güvenliği
- Fiziksel Güvenlik
- Web Güvenliği
- Mobil Güvenlik
- Sosyal Ağlar Güvenliği
- Yöneticiler için Siber Güvenlik
- Zararlı Yazılımlar
- USB Cihaz ve Diğer Taşınır Cihaz Güvenliği

Çalışanlar İçin Siber Güvenlik

Kurum çalışanlarının, bilgisayar, mobil cihaz veya ofis yazıcıları gibi bilgi sistemleri kaynaklarını ev ortamında, iş yerinde veya ofis dışında kullanırken dikkat etmeleri gerekir.
Çalışanların güvenlik zafiyeti oluşturabilecek eylemler ve siber güvenlik tehditleri hakkında bilgi sahibi olması gerekir.

- İş Yeri Ortamında Güvenlik
  a. Ziyaretçiler ve Eşyalar
  b. Fiziksel Erişim Kuralları
  c. İç Tehditler
  d. Fiziksel ve Teknik Tedbirler
  e. Özel Bilgilerin Gizliliği
  f. Sosyal Mühendislik Teknikleri
- Ofis Dışında Güvenlik
  a. Çevre Farkındalığı
  b. Mobil İletişim Güvenliği
  c. İnternet Sitelerine Güvenli Erişim
  d. Sanal Özel Ağ
  e. Herkese Açık Cihazlar
  f. Wi-Fi Kullanımı
- Ev Ortamında Güvenlik
  a. Kablosuz Ağ Güvenliği
  b. Bilgi Güvenliği
  c. Veri Güvenliği
  d. Dosya Paylaşımı
  e. Güvenli Yazılımlar
  f. Cihaz Güvenliği

Sosyal Mühendislik

Kurum çalışanları, etkileme ve ikna yöntemlerini kullanarak insanı aldatmayı hedefleyen sosyal mühendislik saldırıları konusunda dikkat etmelidir. Çalışanların, sosyal mühendisliğin ana unsurları, yaygın kullanılan yöntemleri ve bu saldırılardan korunmak için nasıl tedbirler alması gerektiği bilinmelidir.

Sosyal Mühendisliğin Ana Unsurları

a. Siber Saldırıların Sosyal Tarafı
b. Sosyal Mühendislik Nedir?
c. Bunları Daha Önce Yaptın mı?
d. Herkes Hedef Olabilir
e. Sosyal Mühendislik Neden İşe Yarar?
f. Sosyal Mühendisliğin Dört Adımı
    i. Bilgi Toplama
    ii. Güven Oluşturma
    iii. İnsan Zafiyetini Kullanarak Saldırı Yapma
    iv. Hedeflenen Bilgileri Elde Etme
g. Örnek Vaka - Hileli Banka Transferi
h. Sosyal Mühendisliğin Dört Aşaması

Yaygın Sosyal Mühendislik Yöntemleri

a. Siber Olmayan Yöntemler
    i. Rol Yapma
    ii. Çöp Karıştırma
    iii. İçeri Sızma
    iv. Omuz Sörfü
b. Siber Yöntemler
    i. Oltalama Nedir?
    ii. Yem Atma

KORUNMA ama NASIL?

a. Sosyal Mühendislik Saldırılarına Karşı Korunma
b. Şüpheci Olun
c. İçeriği Doğrulayın
d. Güvenli Telefon Görüşmesi Yapın
e. Olduğunca Az Bilgi Paylaşın
f. Kimlik Doğrulayın
g. Fiziksel Güvenlik Kurallarına Uyun
h. Bilgi Güvenliği Kurallarına Uyun

Parola Güvenliği

Kurum çalışanlarının, parola güvenliği konusunda dikkat etmesi gereken önemli noktaları bulunmaktadır.
Çalışanların, güçlü parola özellikleri, güçlü parola oluşturma yöntemleri, parolayı korumak için en iyi uygulamaları bilmeleri gerekir!

Parolayı Korumak için En İyi Uygulamalar

- Parolalar Nasıl Ele Geçirilir?
- Her Hesap için Aynı Parolayı Kullanmayın
- Parolayı Kimseyle Paylaşmayın
- Parola Yöneticisi Kullanın
- Parolayı Sık Sık Değiştirin
- İş Yerinin Parola Politikasını En İyi Şekilde Uygulayın
- Genel Kullanıma Açık Yerlerde Dikkatli Olun
- İki Faktörlü Doğrulama Kullanın
- Token Kullanın
- İşi Biten Hesapları Kapatın
- Mobil Cihazlarda Pin Yerine Parola veya Parmak İzi Kullanın
- Hatırla Seçeneğini Kullanmayın
- Parolaları Görünür Hale Getirmeyin
- Parolayı Elektronik Ortamlarda Saklamayın
- Kişisel Sorulara Dikkat Edin!
- Güvenlik Sorularını İyi Belirleyin
- Şüpheli Durumlarda Parolayı Hemen Değiştirin

Fiziksel Güvenlik

Kurum çalışanlarının, önemli bilgi içeren cihaz ve belgelerin fiziksel güvenliğinin sağlanmasında dikkat etmeleri gereken noktaları içermektedir. Çalışanların fiziksel güvenlik zafiyeti oluşturabilecek eylemler ve fiziksel güvenlik tehditleri hakkında bilgilendirilmeleri gerekir!

1. Fiziksel Güvenlik Önlemleri
    a. Personel
    b. Erişim Kontrolü
    c. Fiziksel Engel
    d. Gözetleme
2. Fiziksel Güvenlik Seviyeleri
    a. Düşük
    b. Orta
    c. Yüksek
3. Fiziksel Güvenlik İhlalleri ve Önlemleri
    a. Sosyal Mühendislik Taktikleri
    b. Güvenli Gezinme
    c. Temiz Masa Politikası Pekiştirme Uygulaması
4. Fiziksel Güvenlik için En İyi Uygulamalar
    a. Fiziksel Güvenliği İyileştirecek Fiziksel Olmayan Eylemler
    b. En İyi Uygulamalar
    c. Sistem Odası Güvenliği
        i. Erişim Güvenliği
        ii. Personel Güvenliği
        iii. Cihaz Güvenliği
        iv. Medya Güvenliği
        v. Ziyaretçi Güvenliği
        vi. Pekiştirme Uygulaması
    d. Bir İhlal Durumunda Yapılacaklar

Mobil Uygulama Güvenliği

Kurum çalışanlarının, mobil güvenliği konusunda dikkat etmesi gereken önemli noktaları içermektedir. Çalışanların, mobil cihaz güvenliği, mobil iletişim ve bağlantı güvenliği ve mobil uygulama güvenliği önemlidir!

1. Mobil Cihaz Güvenliği
    a. İş ve Özel Hayatın Mobil Ortamda Birleşmesi
    b. Mobil Cihazda Hangi Bilgiler Saklanır
    c. Bilgisayardan Daha da Fazlası
    d. Mobil Cihazlara Yönelik Tehditler
    e. Mobil Cihaz Güvenliği için En İyi Uygulamalar
2. Mobil İletişim ve Bağlantı Güvenliği
    a. Mobil İletişim Riskler İçerir
    b. Mobil İletişim ve Bağlantı Güvenliği için En İyi Uygulamalar
    c. İletişim Risk Faktörünü Ortadan Kaldırın
    d. Konum Takibi
    e. Wi-Fi Bağlantı Riskleri
    f. Bluetooth Bağlantı Riskleri
    g. Bağlantıların Gizliliği İfşa Edilebilir

3) Mobil Uygulama Güvenliği
    a. Mobil Uygulamaların Güvenli Kullanılması
    b. Güvenilir Kaynaklardan İndirin
    c. Her Uygulama İyi Niyetli Olmayabilir
    d. Zararlı Mobil Uygulamalar
    e. Mobil Uygulama Bileşenleri
    f. Mobil Uygulamanın Anatomisi
    g. Mobil Uygulama Özelliklerini Değerlendirmek
    h. Hile ve Tuzaklara Dikkat
    i. Uygulama İzinleri
    j. Uygulama İzinlerine Dikkat
    k. Potansiyel Riskli İzin Örnekleri
    l. İzinleri Körü Körüne Hemen Kabul Etmeyin
    m. Mobil Uygulama Güvenlik Rehberi

Sosyal Ağ Güvenliği

Çalışanların, Facebook, Twitter, Instagram ve LinkedIn gibi sosyal ağların doğurduğu riskler konusunda dikkat etmesi gereken önemli noktaları içermektedir. Çalışanların, sosyal ağ ortamındaki tehditler, çok paylaşım yapmanın riskleri ve güvenli sosyal ağ kullanımı için en iyi uygulamaları bilmek önemlidir!

Sosyal Ağ Ortamındaki Tehditler

a. Sosyal Ağları Kullanmanın Riski Var mı?
b. Sosyal Mühendisler Sosyal Ağları Nasıl Kullanır?
c. Herkesin Değerli Bilgileri Vardır
d. Saldırganlar Fırsat Bekliyor
e. Sosyal Ağlar Paylaşmak İçindir
f. Sosyal Ağlarda Sosyal Mühendislik Teknikleri
g. Sosyal Ağlar İşletmeler için Tehdit Kaynağıdır
h. Arkadaşlarınızı Akıllıca Seçin

Çok Paylaşım Yapmanın Riskleri

a. Bireysel Kariyerin Etkilenebilir
b. Özel Bilgilerin Sana Karşı Kullanılabilir
c. Kuruluşuna Zarar Gelebilir
d. Sosyal Medya Gafları İşinden Edebilir
e. En Mahrem Bilgilerin Yabancılara Açılabilir
f. Gizlilik Ayarları
g. Gizlilik Ayarları Değiştirilebilir
h. Gizliliğin Garanti Altında Değildir
i. Ne Kadar Çok Bilgi O Kadar Çok Risk
j. Sosyal Bilgilerin Aleyhine Kullanılabilir
k. Sosyal Medya Gafları İşinden Edebilir
l. Uzmanlık ile İlgili Çok Bilgi Vermeyin
m. Arkadaşların Senin Kadar Dikkatli Olmayabilir
n. Güvenli Gezinme

Sosyal Ağ Güvenliği

Çalışanların, Facebook, Twitter, Instagram ve LinkedIn gibi sosyal ağların doğurduğu riskler konusunda dikkat etmesi gereken önemli noktaları içermektedir. Çalışanların, sosyal ağ ortamındaki tehditler, çok paylaşım yapmanın riskleri ve güvenli sosyal ağ kullanımı için en iyi uygulamalar bilmek önemlidir!

Güvenli Sosyal Ağ Kullanımı İçin En İyi Uygulamalar

a. Seninle İlgili Paylaşımlara Dikkat
b. İş Yeri Sosyal Medya Kullanım Politikasına Uyun
c. Giriş Güvenliği
d. Sosyal Medya Hesapların Ele Geçirilebilir
e. Güvenlik Soruları veya Cevaplarını Özelleştirin
f. Oltaya Gelmeyin
g. Zararlı Bağlantılar, ‘Scam’
h. Https Şifrelemeyi Aktifleştirin
i. Mobil Uygulamalar
j. Sosyal Oyunlar Her Zaman Güvenli Değildir
k. Ne Kurduğuna Dikkat Et
l. Profil Bilgilerini Körü Körüne Açmayın
m. Kullanılmayan Hesapları Kapatın

Zararlı Yazılımlar

Kurum çalışanlarının, kötü amaçlı eylemleri kendilerinden habersiz gerçekleştiren ve kişisel veya kurumsal sistemleri tehdit eden en tehlikeli saldırı tipi olan zararlı yazılımları öğrenmeleri gerekir. Çalışanların, zararlı yazılım çeşitleri, zararlı yazılımlardan korunma yöntemleri, fidye yazılımlar konuları hakkında bilgi edinmeleri önemlidir!

Web Ortamı Riskleri

Bilgisayara Zararlı Yazılımın Bulaştığını Nasıl Anlarsın?

1. Bilgisayarın Aşırı Yavaşlaması
2. Açılır Pencereler ve Reklamlar
3. İnternet ve Ağ Bağlantılarındaki Tuhaflık
4. İşletim Sistemi, Uygulama ve Dosyalardaki Tuhaflık

Hesaplarının Ele Geçtiğini Nasıl Anlarsın?

1. Bilgisayar Solucanları
2. Bilgisayar Virüsleri
3. Bilgisayar Truva Atları
4. Kök Kullanıcı Takımları (Rootkit)
5. Reklam Yazılımları
6. Casus Yazılımlar
7. Gelişmiş Sürekli Tehditler
8. Fidye Yazılımlar
9. Test

Zararlı Yazılımlar

Zararlı Yazılımlardan Korunma

a. Taşınabilir Medya Kullanırken Riskli Davranışlardan Kaçının
b. Hesapları Kullanırken Riskli Davranışlardan Kaçının
c. Yazılım Güncellerken Riskli Davranışlardan Kaçının
d. Web'de Gezinirken Riskli Davranışlardan Kaçının
e. Yedek Alırken Riskli Davranışlardan Kaçının
f. Kablosuz Ağa Bağlı İken Riskli Davranışlardan Kaçının
g. Güvenlik Duvarını Ayarlarken Riskli Davranışlardan Kaçının
h. E-posta'ları Açarken Riskli Davranışlardan Kaçının
i. İnternet'ten Yazılım Yüklerken Riskli Davranışlardan Kaçının
j. Ele Geçirildiğinden Şüpheleniyorsan
k. Test

Zararlı Yazılımlar

Fidye Yazılımlar

a. Fidye Yazılım Nedir?
b. Fidye Yazılımların Çalışma Yöntemi
c. Fidye Yazılımı Neye Benzer?
d. Ya Para ya Veriler
e. Fidye Yazılımı Kimi veya Neyi Hedef Alır?
f. Fidye Yazılımı Saldırısı Örneği
g. Ülkemizde Görülen Fidye Yazılımları
h. Fidye Yazılım Bulaşırsa Ne Yapmalısın?
i. Fidye Yazılımın Bulaşmış Olup Olmadığı Nasıl Anlaşılır?
j. Verileri Yedekleri Kullanarak Kurtarın
k. En Son Çare Olarak Fidyeyi Ödeyin
l. Şifrelenmiş Verileri Çözmeye Çalışmayın
m. Bilgisayarın Fişini Çekin
n. Test

USB Cihaz Güvenliği

USB Cihazları Kullanmanın Riskleri

a. USB Cihazları Zararlı Olabilir
b. USB Cihazı Çalınabilir
c. Taşınabilir Depolama Amaçlı USB Cihazları
d. Diğer USB Cihaz Çeşitleri
e. Neden Dikkatli Olmalısın?
f. USB Cihazlarının Olumsuz Yönleri
g. Nereden Alındığına Dikkat Edin
h. Diğer Riskler
i. Yaşanmış USB Vakası Örnekleri

1. USB Cihazları Kullanmak için En İyi Uygulamalar

a. Ev ve İş Yeri USB Cihazlarını Ayrı Tutun
b. USB Cihazları Tek Bir Yerde Saklayın
c. İş Yerinde Güvenlik Önlemlerini Alın
d. Üçüncü Taraflara Ait USB Cihazlarını Doğrudan Kullanmayın
e. Promosyon veya Hediye USB Cihazları Reddedin
f. Evde Gerekli Önlemleri Alın
g. Cihazı Şarj Etmek için Priz Kullanın

2. USB Cihazında Saklanacak Veriler

a. Hangi Verileri USB Cihazında Tutmalısın
b. USB Cihaz Kullanarak Veri Paylaşım

E-Posta GÜVENLİĞİ

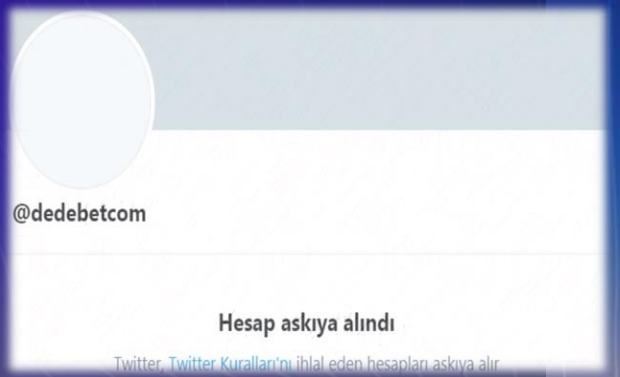
urum çalışanlarının, elektronik posta güvenliği konusunda dikkat etmesi gereken önemli noktaları içermektedir. Çalışanların, elektronik posta kullanımında dikkat edilmesi gereken hususlar, elektronik posta ile yapılan riskli eylemler ve oltalama e-postalarının tespit etme yöntemlerini bilmeleri kritiktir!

1. E-Posta Nasıl Çalışır?
2. E-Posta Kullanımı ile İlgili Genel Riskler
    a. Mahremiyetin ve Gizliliğin Bozulması
    b. E-Postayı Dikkatsiz Göndermek
    c. İstenmeyen E-Posta (SPAM)
    d. Oltalama Saldırısı
3. Şüpheli E-Postaların Kontrolü
4. Oltalama E-Postalarını Tespit Etme Yöntemleri
    a. E-Posta Analizi
    b. Şüpheli E-Postalar için Eyleme Geçmek
        i. Araştırma
        ii. Bildirim
        iii. Silme
        iv. Dosyalama
5. E-Posta ile Yapılan Riskli Eylemler
    a. Linke Tıklama
        i. Zararlı E-Posta Linkleri
        ii. E-posta Linklerinin Analizi
        iii. Zararlı Linklerden Korunma Yöntemleri
    b. Ekleri Açma
        i. Zararlı E-Posta Eklentileri
        ii. Dosya Adı Uzantıları
        iii. Zararlı Eklentilerden Korunma Yöntemleri
    c. Veri Girişi
        i. Veri Girişi Oltalama Saldırısı
        ii. Saldırı Türleri
            1. E-Posta Formları
            2. E-Posta Linkleri
            3. Tuzak Siteler
        iii. Dolandırıcılık Amaçlı Sitelerden Korunma Yöntemleri
        iv. Aldatıcı İnternet Siteleri Tespit Etme Yöntemleri

Kötücül Hesap Aktiviteleri

1. 1000 sahte hesap 1$
2. 24 saatte 1000 sahte hesap temini yapılabilmektedir.
3. Sanal Atölye İşçileri - Captcha
4. 100 Sahte E-posta 1$ - Yahoo (1 hesap 1 sent)
5. Social Dilemma – Zihnimizin sosyal medya platformları tarafından bükümü ve hacklenmesi..
6. Arap Baharı, Turuncu Devrim Twitter Etkisi
7. The Great Hack - Cambridge Analytica – ABD Seçimi
8. Hotel-Influencer sosyal medya savaşı
9. Kurumsal sosyal medya takip/manipülasyon/dezenformasyon merkezleri

Kötücül Hesap Aktiviteleri



SCIENCE & TECH
Twitter: 1 million accounts suspended for 'terrorism promotion'

SCIENCE & TECH
Twitter sets crackdown on automated 'bot' accounts

Twitter's war on the multimillion-dollar fake follower business
Source New York Times

TECH • TWITTER
Trump's Fake Twitter Following Climbs, Sparking Fears of a Bot War
FORTUNE

Twitter Türkiye'ye saldıran hesaplara savaş açtı VATAN

Twitter sahte bilgilerle insanları yanıltan hesapları siliyor Sözcü

Twitter Sahte Hesaplara Savaş Açtı: Telefon Numarası Doğrulama Şartı TECHNOTODAY

Dünyada Ses Getiren Siber Saldırılar

1. Melissa Virüsü (1999)
2. Nasa Siber Saldırısı (1999)
3. Estonya Siber Saldırısı (2007)
4. Sony Playstation Ağı Siber Saldırısı (2011)
5. Adobe Systems Siber Saldırısı (2013)
6. Yahoo Siber Saldırısı (2013)
7. Ukrayna Elektrik Şebekesi Siber Saldırısı (2015)
8. WannaCry Ramsomware (2017)
9. Marriott Otelleri Siber Saldırısı (2018)
10. RockYou2021 (2021)
11. İran Siber Saldırıları (2010-2021)
12. Türkiye Root DNS (Nic. TR) Saldırıları (2015)
13. Rusya'nın Ukrayna Saldırısı (2017-2022)
14. Sri Lanka Siber Saldırıları (2019-2020-2021)
15. OpsIsrael Cyber Attacks
16. Romania Cyber Attacks (2022)

Dünyada Ses Getiren Siber Saldırılar

1. Melissa Virüsü: Microsoft'un tüm sistemlerini çökertip 80 milyon dolarlık hasar bıraktı.
2. NASA Siber Saldırısı: 15 yaşında bir çocuk, NASA'nın 41.000 dosyasını indirdi..
3. Estonya Siber Saldırısı: Dünya tarihinde ülkeler arasındaki ilk siber saldırı bir Avrupa ülkesi olan Estonya'da yaşandı. Estonya'ya ait banka ve medya kuruluşlarının web siteleri ele geçirildi.
4. Sony Playstation Ağı Siber Saldırısı: Kullanıcılar online servislere erişemezken, 100 milyondan fazla kişinin şahsi bilgileri de çalındı.
5. Adobe Systems Siber Saldırısı: 2.9 milyon müşterisinin kredi kartı ve parola bilgilerinin de ele geçirildi.
6. Yahoo Siber Saldırısı: 500 milyon kişinin hesabı hackerların eline geçti..
7. Ukrayna Elektrik Şebekesi Siber Saldırısı: 225 bin kişi elektriksiz kaldı. Enerji firmaları, saldırının BlackEnergy virüsü aracılığı ile gerçekleştiğini belirtti.
8. WannaCry Ramsomware: Melissa Virüsü'nün ardından bir de WannaCry. Microsoft Windows'u hedef alan WannaCry virüsü, 2017 yılında 150'den fazla ülkede yaklaşık 200 bin bilgisayara ulaştı. Saldırının küresel maliyeti toplamda 6 milyar Sterlin oldu.
9. Marriott Otelleri Siber Saldırısı: 339 milyon misafirinin kişisel bilgileri çalındı. Bir süre gizli tutulan ancak 2018 yılında ortaya çıkan bu olay sonrası İngiltere Hükümeti, Marriot Hotels'a 18.4 milyon Sterlin para cezası kesti.
10. RockYou2021: Siber saldırı tarihindeki en büyük şifre hırsızlıklarından bir, 8.4 milyar çalıntı şifreden oluşan 100 GB'lık bir TXT dosyası..
11. Bitcoin Saldırısı ile 148.000.000.000 BTC üretim atağı

İnternette gizlenen bir tehdit var. Mali durumunuzu yok etme, kişisel verilerinizi çalma ve hayatınızı tehlikeye atma gücüne sahip gizli bir savaş!

[Spam Nation, Brian Krebs – New York Times Best Seller]

Bilgisayarım Hacklendi mi?

1. Tarayıcınızda veya masaüstünde çıkan pop-uplar görüyorsanız, büyük ihtimalle bir reklam veya pazarlama virüsü aldınız. *Bu durumda hemen task manager üzerinden işlemleri kontrol edin.*
2. Tarayıcınızda sizin yüklemediğiniz araçlar toolbar içerisinde yer alıyor mu? Eğer böyle bir araç tarayınızda ise tarayıcıdan kaldırın ve tarayıcınızı yeniden kurun.
3. Sürekli bir güvenlik e-postası farklı konumlardan oturum açtığınıza dair bilgi veriyor ise bu mesajı önemseyin. Parolaları değiştirin ve tekrar bu tarz e-postalar almaya devam ederseniz. Güncel bir anti-virüs yazılımı edinin.
4. Bilgisayarınızda özellikle PDF uzantılı dosyaları açarken normalden fazla bir yavaşlama yaşıyorsanız. Crypto Locker adı verilen virüs konusunda dikkatli olun.
5. Kontrol etmeniz gereken en kritik metrik ise ağ trafiğiniz olacaktır. İnternette sadece sosyal medyada dolaşıyorsunuz fakat buna rağmen kota sorunları mı yaşıyorsunuz? Aynı zamanda upload işlemlerinizi internet servis sağlayıcısı üzerinden kontrol edin. Son aylarda bir artış söz konusu ise, bilgisayarınızı yedekleyip hemen reboot işlemi yapın. İnsanlar bu tarz durumlarda bilgisayar yedeklerini olduğu gibi yeni bilgisayara atıyor. Bu durumda reboot yapmanın bir anlamı yok, bunu da hatırlatayım.

Bilgisayarım Hacklendi mi?

6. Windows task manager aracını kontrol ettiğinizde ismini duymadığınız işlemler görebilirsiniz. İşinize yarayan çoğu program bu adını bilmediğiniz işlem parçacıklarını kullanır. Dolayısıyla adını bilmediğiniz işlemler virüstür gibi bir algıya kapılmayın. Tüm programları kapattıktan sonra task manager aracını izleyin bu ekranda gereksiz bir artış görüyorsanız. O işlem sizin bilgisayarınızdaki bir virüstür.
7. Genelde internet kullanıcıları her platform için aynı şifreleri kullanırlar. https://haveibeenpwned.com/PwnedWebsites sitesi üzerinden yakın zamanlarda burada yer alan firmalardan birine kayıt olup olmadığınıza bakın. Eğer buradaki bir firma aracılığıyla size güvenli e-postalar gelmeye başladıysa, bilgisayarınıza indirmiş olabilirsiniz.
8. Bilgisayarınızı kullanırken birden kaybolan pencereler görüyorsanız, sisteminizden ara sıra veri upload ediliyor olabilir. Bilgisayarınızı hemen temizleyin.
9. Bir dizüstü kullanıyorsanız ve pili aniden düşmeye başladıysa ki her dizüstü bilgisayar bir süre sonra daha az şarj süresi verir. Buna rağmen eğer uzun süredir kullandığınız cihazınız bir iki gündür aniden şarj sürelerinde yeterli gelmiyorsa, bilgisayarınız uzak masaüstü ile izleniyor olabilir. Petya virüsü isimli yazıda da benzer bir konuyu anlatmıştık.
10. Programlar listesinde adını duymadığınız bir program varsa bunu hemen kaldırın. Çoğu kullanıcı adını bilmediği programları bilgisayarında saklıyor fakat bu programlar uzun bir süre uyku durumunda iken en önemli verilerinizi tespit edip can yakabiliyor.

BAŞKANLIĞIMIZ ISO27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ SERTİFİKASINI TEKRARDAN ALMAYA HAK KAZANDI

International Organization for Standardization

ISO

27001:2013

Bilgi Güvenliği

Bilişim Teknolojilerinde Trendler

Dijitalleşen Yaşam

Üretiyoruz!..

Endüstri 4.0
(Mekanik, Elektrik, Otomasyon, Internet)
Nesnelerin İnterneti (IoT)
Büyük Veri (Ölçülebilir, Büyük Hacimli)
Bilgi Çağından 2. Makine Çağına

Bağlantıdayız!..

Internet ile Her an Her Yerde
Akıllı Telefonlar
Aplikasyonlar
Web 2.0, Web 3.0

Dijitalleşiyoruz!..

Birey, firma, kurumlar..
İletişim, Etkileşim, Üretim, Eğitim
Sürücüsüz Araçlardan Akıllı Evlere..
Kriptoparalardan NFT lere..

Sanallaşıyoruz!..

Sanal Kişilik, Etkileşim ve
Yaşamlar..
Sanal Sosyal Ağlar
Metaverse

2023 ve Ötesi İçin Teknoloji Trendleri

- Yapay Zeka (AI)
- 5G ve Gelişmiş Bağlantı
- Edge Bilişim
- Davranışların İnterneti (IoB)
- Kuantum Hesaplama
- Blokzincir Teknolojileri
- Siber Güvenlik
- İnsan Geliştirme
- Dağıtılmış Bulut
- Artırılmış Gerçeklik ve Sanal Gerçeklik (AR-VR)

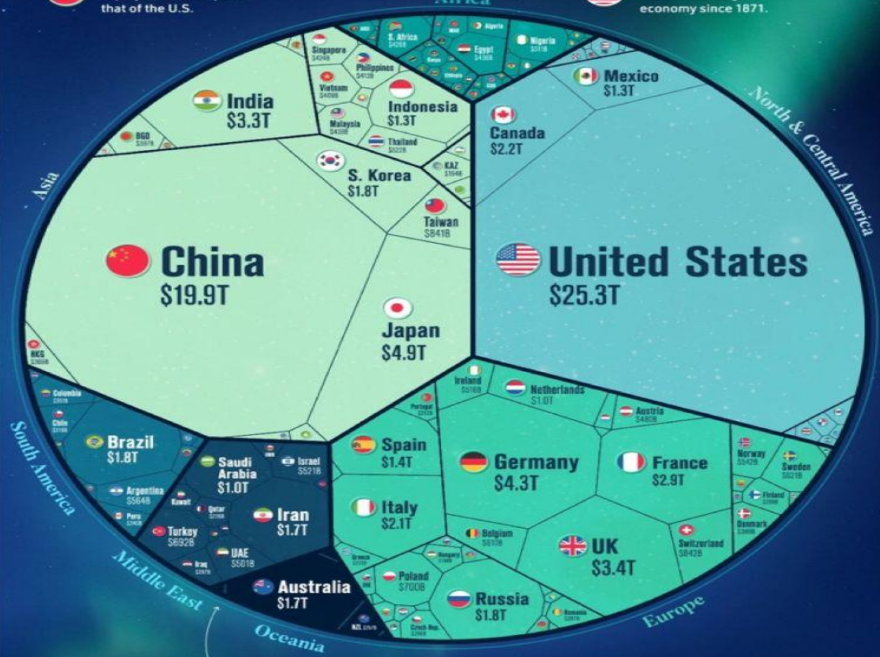
The $100 Trillion World Economy

GLOBAL GDP 2022

Despite conflict and looming stagflation, the global economy will hit an impressive new milestone, reaching **$104 trillion,** according to the latest IMF projections for end of year.

By 2030, **China's GDP** is projected to surpass that of the U.S.

The U.S. has been the world's largest economy since 1871.



Many of the world's smallest economies are located in the Oceania region, such as **Tuvalu** with a GDP of $66 million.

Ireland is expected to be the fastest growing economy in the Eurozone, with a 5.2% increase this year.

*2022 data was not available for a handful of countries, including Ukraine and Pakistan.
For full data notes and detailed version of this visualization, visit visualcapitalist.com/100-trillion-global-economy/

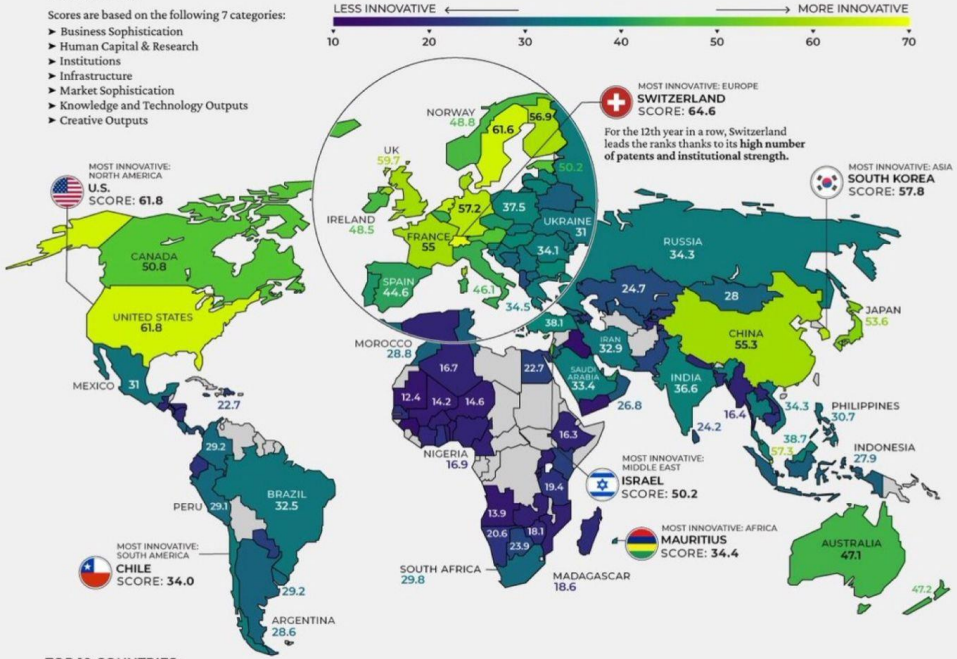
Source: IMF (April 2022)

Global Innovation Index 2022

Below, we show the most innovative economies in the world, based on analysis from the WIPO Global Innovation Index.

Scores are based on the following 7 categories:

- Business Sophistication
- Human Capital & Research
- Institutions
- Infrastructure
- Market Sophistication
- Knowledge and Technology Outputs
- Creative Outputs



TOP 10 COUNTRIES:

SOURCE: Global Innovation Index 2022

Yapay Zeka

İnsan zekasını taklit eden ve bilgisayar uygulamalarının yinelemeli işleme ve algoritmik eğitim yoluyla deneyimlerden öğrenmesine olanak tanıyan bir teknolojidir.

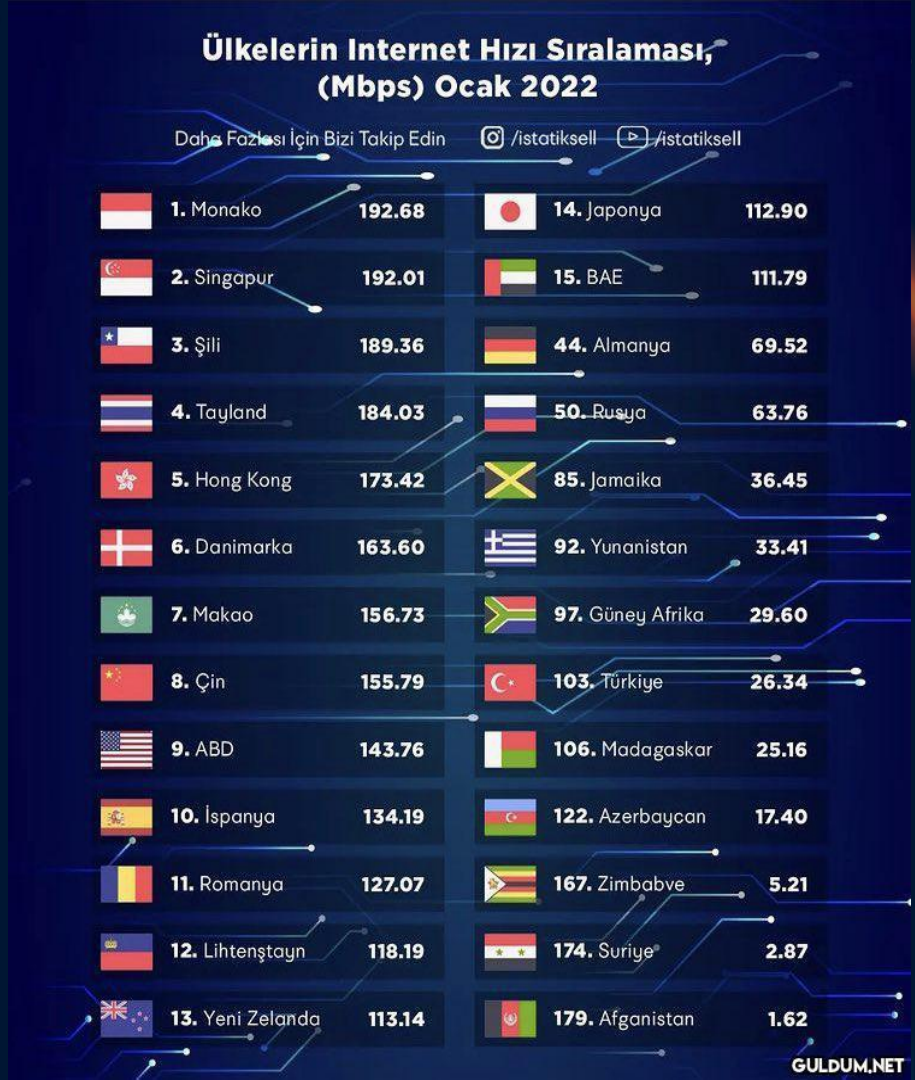
Hayatımızın her alanında varlığını hissettiğimiz yapay zeka tüm teknolojilerde temel aktör olacak.

Nasıl?
5 Aktör: Makine Öğrenmesi, Derin Öğrenme, Yapay Sinir Ağları, Doğal Dil İşleme, Bilgisayarlı Görü

Neden?
Bilgisayarların temelde insanlar gibi düşünmesine ve davranmasına izin verir.
Birçok durumda AI sistemleri insanlardan önemli ölçüde daha iyi performans gösterme yeteneğine sahiptir.
Görüntü ve konuşma tanıma, Araç paylaşım uygulamaları, Mobil kişisel asistanlar, Navigasyon uygulamaları

5G ve Gelişmiş Bağlantı

- Daha hızlı ve kararlı internet
- Bant genişlikleri arttıkça, 3G mobil cihazlarda çevrimiçi erişimi ve veriye dayalı hizmetleri etkinleştirdi.
- 4G, video ve müzik platformlarının artmasını sağladı.
- 5G de aynı şekilde mümkün olduğunca yeni gelişmeleri destekleyecektir.
- 5G, artırılmış gerçeklik ve sanal gerçeklik dahil olmak üzere en son teknolojiyi kullanan ağları ifade eder.
- Özetle 5G ve diğer gelişmiş, yüksek hızlı ağlar, tartıştığımız diğer tüm trendlere her yerden, her zaman erişilmesine izin veriyor.



Dünyanın en değerli kaynağı artık petrol değil, veridir!

The Economist

GROUP	SUPPORTING	ATTACKS	COMMS	LOC	Date started
AgainstTheWest (ATW)	Ukraine	Data Breach & ransomware	Twitter	West Europe	2021
Belarusian Cyber Partisans	Ukraine/Free Belarus	Ransomware	Twitter	Belarus	2020
Anonymous	Ukraine	DDoS	Twitter	Global	FEB 2022
GhostSec	Ukraine	Hack	Telegram	UNK	FEB 2022
IT Army of Ukraine	Ukraine	DDoS	Telegram	Ukraine	FEB 2022
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK	FEB 2022
BlackHawk	Ukraine	DDoS	Twitter	Georgia	FEB 2022
Anonymous Liberland & the PWN-BAR hack team	Ukraine	DDoS	Twitter	Global	FEB 2022
Raidforums Admin	Ukraine	Sanction	Raidforums	UNK	FEB 2022
Netsec	UNK	Hack	Twitter	UNK	FEB 2022
Free Civilian	Russia	Data Breach	Onion	UNK	JAN 2022
Cooming Project	Russia	Data Breach	Onion	UNK	2021
Conti Ransomware	Russia	Ransomware	Onion	Russia	2019
The Red Bandits	Russia	Data Breach	Twitter	Russia	2021
CyberGhost	Russia	Hack	UNK	Belarus	UNK
SandWorm	Russia	Hack & DDoS	UNK	Russia	UNK
28 FEB	----	-------	------	-------	------
GNG	Ukraine	DDoS	Twitter	Georgia	2022
NB65	Ukraine	Hack	Twitter	UNK	2022
ECO	UNK	UNK	Twitter	UNK	2022
Raidforums2	Ukraine	DDoS	Twitter	UNK	2022
ContiLeaks	Ukraine	Data Breach	Twitter	UNK	2022
SHDWSec	Ukraine	Hacks/Activism	Twitter	Global	2022
GhostClan	Ukraine	Hacks/DDoS	Telegram	Global	2022
Eye of the Storm	Ukraine/Free Belarus	Hacks	Twitter	Global	2022

Ukrayna Devleti olarak ilk hibrit savaşla karşı karşıyayız. Karada olduğu gibi siber uzayda da savaşıyoruz. Elektrik şebekelerimize, nükleer santrallerimize, İletişim hatlarımıza ve siber vatanımızdaki diğer kurum ağlarımıza yapılan saldırılar karşısında siber savunma geliştiriyoruz!

Viktor Zahora, Ukrayna Başkan Yardımcısı

01

Dış Erişim Kısıtlama

02

Dos/DDoS Atağı Engelleme

03

Web Uygulama Güvenlik Duvarı Güvenliği

04

Güncellemeler Güvenlik Yama Yönetimi

05

Erişim ve Yetkilerin Düzenli Kontrolü

06

Yedekleme Yedekten Geri Dönme

07

Katmanlı Güvenlik Mimarileri (Güvenlik Duvarı, DMZ)

08

Sosyal Mühendislik Önlemleri

09

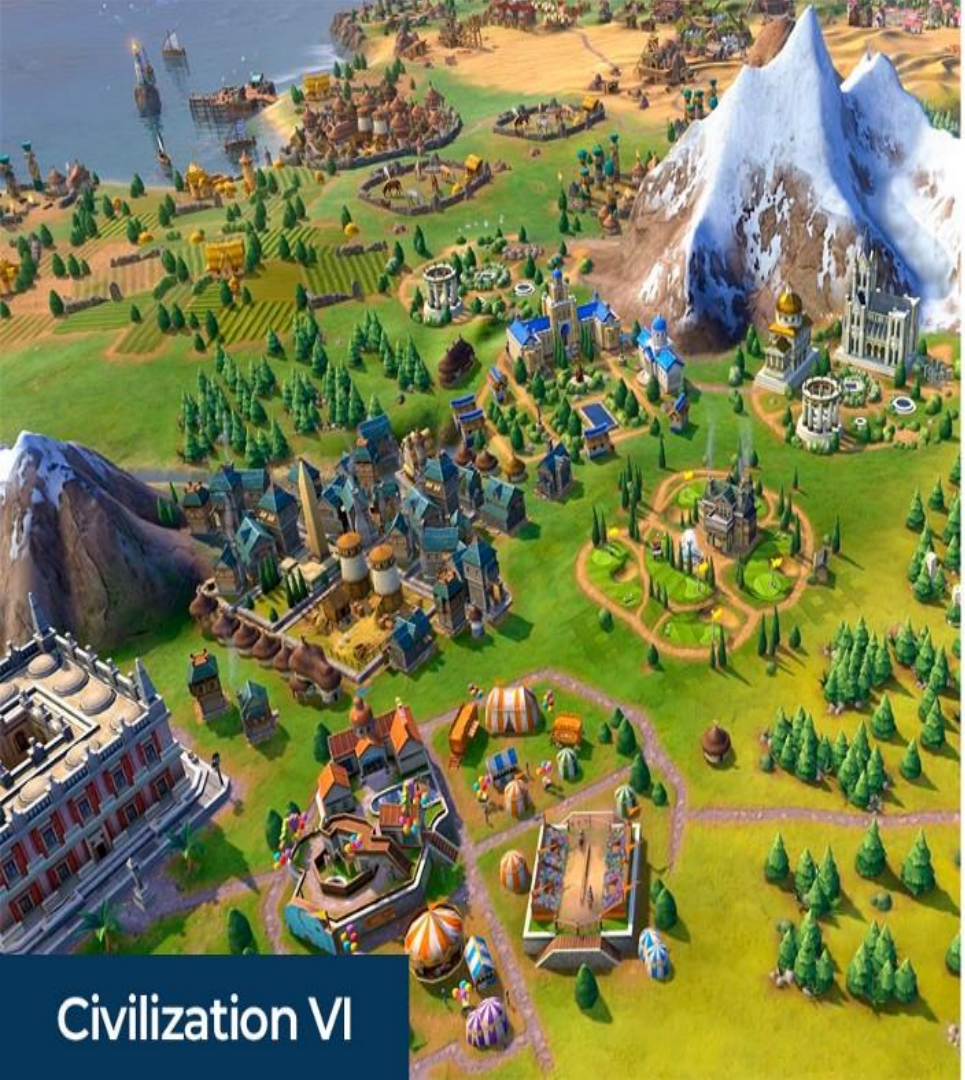
SOME Müdahale Planları

OYUNLAŞTIRILMIŞ DERS PLANI 32

DERS : Ingilizce
KONU : Weather Cyle
SINIF : 5
SÜRE : 5 Gün

KAZANIM :

1. Hava durumu ve iklim arasındaki farkı ayırt eder.
2. Meteoroloji uzmanı ve hava tahmincisi arasındaki farkı ayırt eder.
3. Iklim türlerini ifade eder, gruplara ayırabilir.
4. Hangi iklim türünde hangi ev türünün olabileceğini bilir.

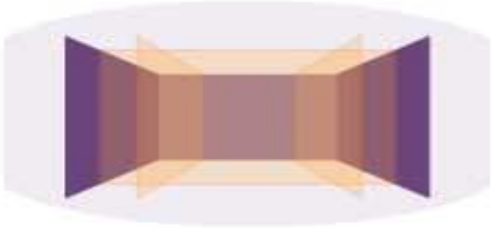

Civilization VI


49
1 185 895
104/200
5/60
69 750
100%
SimCity


ArcheAge
UNCHAINED

Sanal (virtual) Gerçeklik (VR)

Tamamen sanal çevre

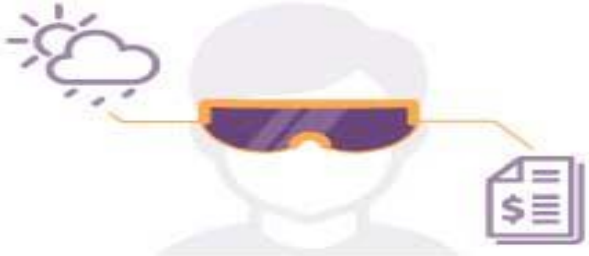


Tamamen sanal ortamda olma

Artırılmış (augmented) Gerçeklik (AR)

Sanal nesneler, gerçek dünya çevresinin üstüne giydirilir

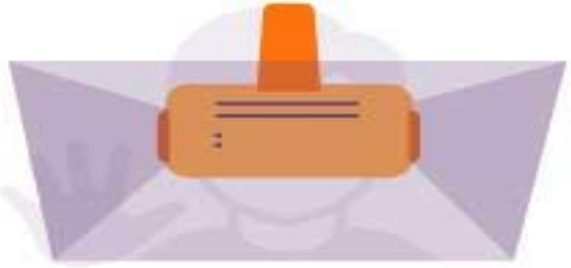
Dijital nesnelerle, gerçek dünya zenginleştirilir



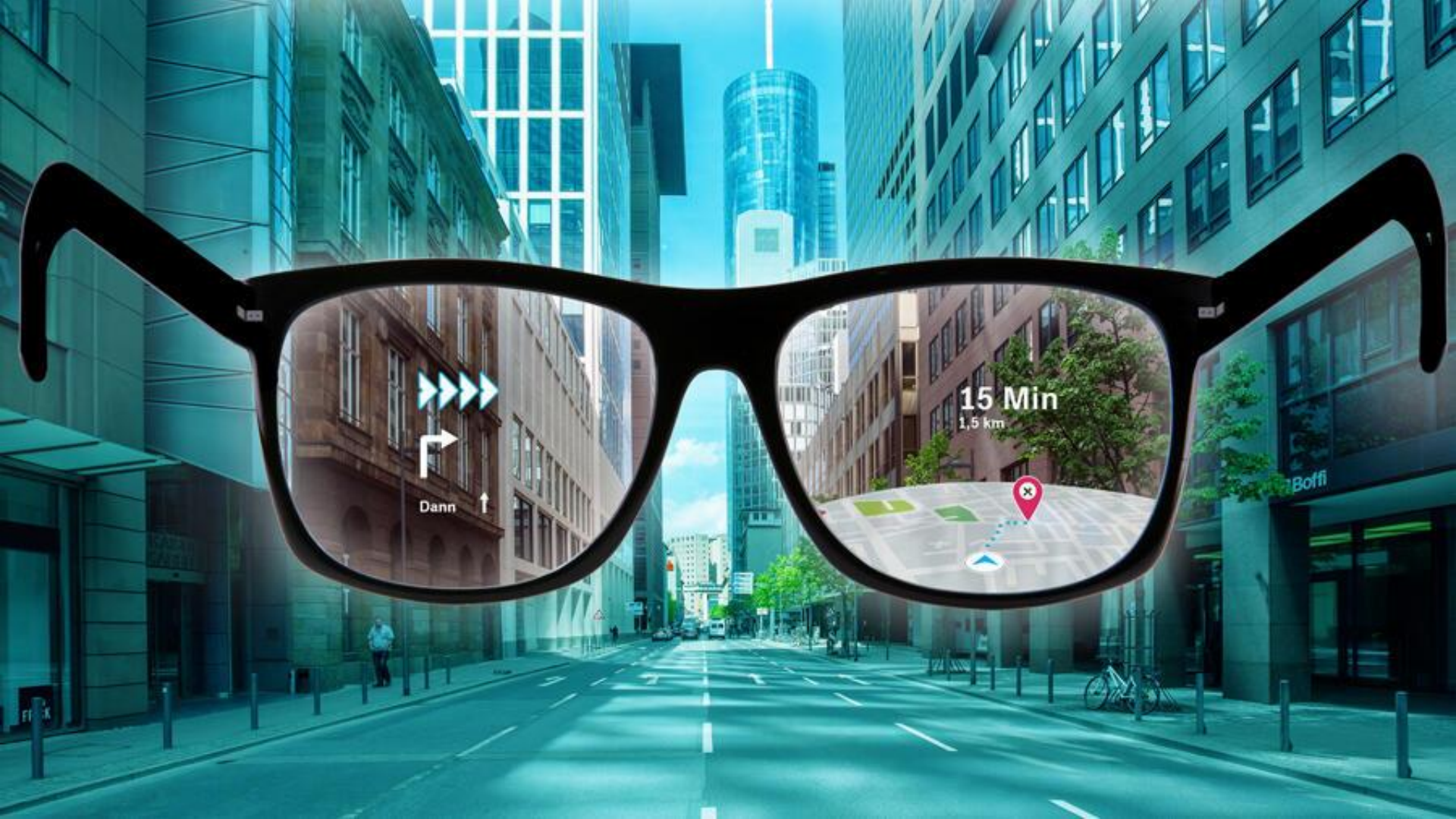
Karma (mixed) Gerçeklik (MR)

Sanal çevre, gerçek dünya ile kombine edilir

Hem gerçek dünya hem sanal çevre ile etkileşim




Virtual Reality
Augmented Reality
Mixed Reality


Dann
15 Min
1,5 km
Boffi

Web 1.0

"Read Only",
Decentralized

Web 2.0

Participatory,
Centralized

Web 3

No Intermediaries,
Decentralized

Metaverse Summit

IMMERSED'S METAVERSE MARKET MAP 2022 (V2)

AS WE BRING THE WORLD'S ECONOMY INTO VR, WE WANTED TO HIGHLIGHT SOME THE BEST METAVERSE APPLICATIONS LEADING THE WAY IN 2022.

Hardware

Hardware infrastructure on which Metaverse applications are built on top of.

Meta Quest, ByteDance, PlayStation VR, Apple, VIVE, Microsoft HoloLens, VALVE, Magic Leap

Decentralized Worlds

Platforms where users have the freedom to control their own digital assets.

The Sandbox, Decentraland, immersed, Wilder World, Somnium Space, neos, Worldwide Webb, CryptoVoxels

Centralized Worlds

Metaverse platforms which are created and managed by one core entity.

ROBLOX, MINECRAFT, FORTNITE, Second Life

Virtual Real Estate

Entities that are focused on building and investing in metaverse platforms .

Landvault, Sandstorm, EVERYREALM, pangea, Parcel

Gaming & P2E

These platforms are focused on building Metaverse gaming experiences. Leveraging gaming economies.

Axie Infinity, animoca brands, Illuvium, BYDPILLS, MYTHICAL, HUMAN PARK, STAR ATLAS, ZED, HOUSE OF KIBAA

Guilds

Gaming Guilds are organizations that provide training, tools, NFTs, & funds to players.

Yield Guild, GAMEFI, vEMPIRE

Consortiums

Entities that are focused on creating Web3 & metaverse creation standards

Metaverse Standards Forum, W3C, KHRONOS, OMIgroup

Marketplaces & Game Launchers

Marketplace platforms that enable users to list and sell metaverse assets.

elixir, METAMUNDO, FRACTAL

Gaming Engines

A software framework used for the development of video games & VR applications which includes relevant libraries.

Unity, Unreal Engine, CRYENGINE, lumberyard

Social, Art, & Entertainment

Metaverse applications focused on connecting users and players through dynamic social & immersive experiences.

VRChat, horizon Worlds, MONA, AltspaceVR, MALOKA, Rec Room, Spatial, bigscreen

Digital Identity

Companies tackling digital identity by building avatar creation platforms and interoperability systems.

Ready Player Me, Genies, soul machines, Tafi, YUGALABS, RTFKT

Tools

Companies building tools to streamline metaverse asset creation.

Rove, zesty, STEAMVR, blender

BROWSER

STORAGE

VIDEO AND AUDIO CALLS

OPERATING SYSTEM

SOCIAL NETWORK

MESSAGING

REMOTE JOB

WEB 2.0 APPS

CHROME

DROPBOX

SKYPE

ANDROID

FACEBOOK

WHATSAPP

UPWORK

WEB 3.0 DAPPS

BRAVE

IPFS

EXPERTY

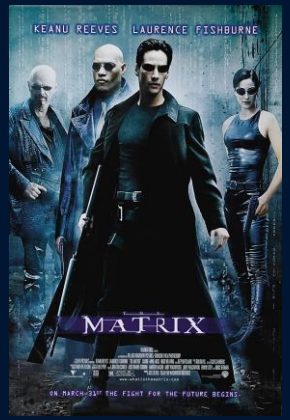
EOS

STEEMIT

STATUS

ETHLANCE


READY PLAYER ONE
20 MART'TA SİNEMALARDA


KEANU REEVES LAURENCE FISHBURNE
MATRIX

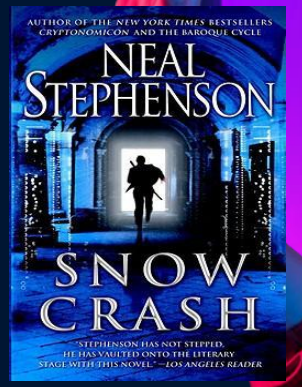

FROM THE DIRECTOR OF TERMINATOR 2 AND TITANIC
AVATAR
EXPERIENCE IT IN IMAX 3D


THE ONLY RULE IS SURVIVAL
TRON
LEGACY


AVATAR
SUYUN YOLU
16 ARALIK'TA


CHARLIE BROOKER'S
BLACK MIRROR


SECOND LIFE


AUTHOR OF THE NEW YORK TIMES BESTSELLERS CRYPTONOMICON AND THE BAROQUE CYCLE
NEAL STEPHENSON
SNOW CRASH
"STEPHENSON HAS NOT STEPPED, HE HAS VAULTED ONTO THE LITERARY STAGE WITH THIS NOVEL." —LOS ANGELES READER

I. Metaverse, birbirleriyle bağlantılı dünyalar arasında sorunsuz bir şekilde sonsuz geçişler yapabileceğiniz bir teknolojisi olarak tasarlanmaktadır.

II. İnsanların sanal gerçeklik yoluyla dijital bir dünyada gerçek dünyada yaptıkları gibi zaman geçirebildiği, etkileşim kurabildiği bu dünyanın kalıcı olması ve kullanıcıların yarattığı içeriklere dayanması bu işin büyük bir parçasını oluşturmaktadır.

III. Metaverse fikri, insanların etkileşimlerinin daha çok boyutlu olabileceği, kullanıcıların sadece görüntülemek yerine kendilerini dijital içeriğe kaptırabilecekleri yeni çevrimiçi alanlar yaratması olarak tanımlanabilir.

Metaverse, gerçek dünyaya paralel deneyimler sunar.

I. Dijital İkizlik
II. Matrix Robot Şehri Deneyimi
III. Sanal Gerçeklik Gözlükleri ve IoT cihazlar, giyilebilir teknolojiler ile yüksek algılama yeteneği
IV. Sanal Dünya ve Gerçek Dünya Etkileşimi
V. Avatarlarla Sanal Anonim Yaşamlar
VI. Kripto Paralar, NFTler, Arsa Alımları
VII. ·Dijital arazi satın almak ve sanal evler inşa etmek
VIII. Sanal bir sosyal deneyime katılmak
IX. Sürükleyici ticaret yoluyla sanal alışveriş merkezlerinde alışveriş
X. Sürükleyici öğrenme deneyimi için sanal sınıfları kullanma
XI. Dijital sanat, koleksiyon ve varlık satın alma (NFT'ler)

Ama Nasıl?

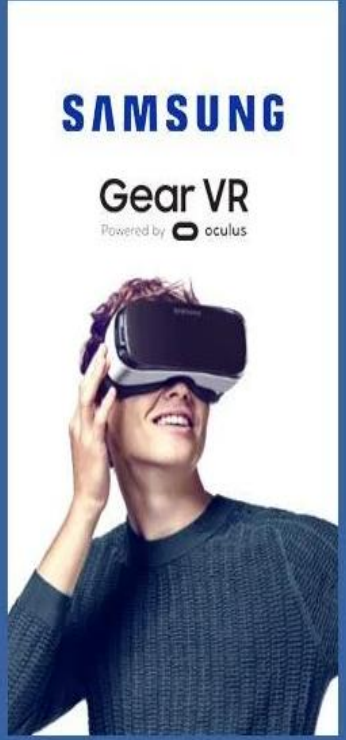
1. Metaverse, işlev görmesi için birden fazla teknoloji ve trend gerektiriyor.

2. Bunların bir kısmı şöyle sıralanabilir: Artırılmış gerçeklik (AR), esnek çalışma stilleri, başa takılan ekranlar (HMD'ler), AR bulutu (AR Cloud), Nesnelerin İnterneti (IoT), 5G, yapay zeka ve farklı uzamsal teknolojiler.

3. Gartner, 2026 yılına kadar insanların %25'inin iş, alışveriş, eğitim, sosyal medya ve/veya eğlence için Metaverse'te günde en az bir saat geçirmesini bekliyor.

4. Meta veri deposunun derinliklerine dalmadan önce, günümüzün meta veri deposunun özellikleri olan Web 2.0 özellikleri ile ortaya çıkan Web 3.0 özellikleri arasında temel oluşturmak önemlidir.

Google
Daydream



Samsung
Gear VR

Oculus
Rift

Sony
Playstation VR

HTC / Valve
Vive

Oculus founder Palmer Luckey says he has designed a new VR headset loaded with explosives that can actually kill you: "If you die in the game, you die in real life". - Copyright Courtesy Palmer Luckey


BANKLESS


WELCOME TO
METAVERSE
THAILAND


BATMAN ÜNİVERSİTESİ
ULUSLARARASI BİLİŞİM KONGRESİ
UBK'22
KONFERANS


Çağdaş
HABER


BİLİŞİM FUARI
PANELLER
HID
HID
PANELLER


BATMAN ÜNİVERSİTESİ


PARTNER
ERBİL


WORKSHOPLAR
ERBİL
Canon
CANON BASKI VE TARAMA ÇÖZÜMLERİ
HOŞGELDİNİZ
Canon
come
and
see
océ


BATMAN ÜNİVERSİTESİ
BATMAN ÜNİVERSİTESİ
ULUSLARARASI BİLİŞİM KONGRESİ
IIC'22
2007
PANELLER
PANELLER
NETCOM
getirecem.com
Saray Gülü


reset
DIGITAL
reset
reset
reset


HASANKEYF
UYGULAMA OTELİ
BATMAN ÜNİVERSİTESİ HASANKEYF UYGULAMA OTELİ
HOŞGELDİNİZ


HOŞGELDİNİZ

BATMAN ÜNİVERSİTESİ

BİLİŞİM FESTİVALİ IFEST 2023

DİJİTAL DÖNÜŞÜM | BLOKZİNCİR TEKNOLOJİLERİ | SİBER GÜVENLİK

ANA TEMALARIYLA

DEGİŞİM BİLİŞİMLE GELECEK

- Bilişim Teknolojileri Fuarı
- Kamu Bilişim Çalıştayı
- Uluslararası Bilişim Kongresi
- Bilişim Akademisi
- ETKİNLİKLER KATILIM ÜCRETSİZ!
- Bilişim Teknolojileri Konferansı
- Sosyal Etkinlikler
- Ödüller Çekilişler
- Deneyap Atölyeleri

9-11 ŞUBAT 2023 | BATMAN ÜNİVERSİTESİ

ifest@batman.edu.tr | ifest.batman.edu.tr | bilisimbatmanda | #bilisimbatmanda

BATMAN ÜNİVERSİTESİ 2007

ULUSLARARASI BİLİŞİM KONGRESİ IIC2023

DİJİTAL DÖNÜŞÜM | BLOKZİNCİR TEKNOLOJİLERİ | SİBER GÜVENLİK

ANA TEMALARIYLA

KONGRE NİTELİKLERİ

- Uluslararası Katılımlı Kongre
- En az 2 Hakemli Değerlendirme (En az 1 hakem kurum dışından)
- ISBN Kitaplarda Makale Yayını
- Seçilen Makaleleri İndeksli ve Açık Erişimli Dergilerde Yayınlama İmkanı

DERGİLERİMİZ

- Balkan Journal of Electrical and Computer Engineering (BAJECE)
- European Journal of Technique (EJT)
- Journal of Engineering and Technology (JETECH)
- Cyber Politik Journel Siber Politikalar Dergisi

KONULAR

Siber Güvenlik	Yapay Zeka	Veri Merkezleri	Veri Sıkıştırma Argoritmaları
Blokzinciri	Roket Teknolojileri	Akıllı Sistem Odaları	Oyunlaştırma Teknolojileri
Metaverse,NFT	Savunma & Uzay Teknolojileri	Akıllı Ev Sistemleri	GameFI,DeFI,SocialFI
Haberleşme Teknolojileri	Dijital Dönüşüm Uygulamaları	Siber İstihbarat	Kriptografi
İnsansız Hava Araçları	Dijital Güvenlik Sistemleri	Sağlık Bilişimi	Büyük Veri
Robotik	Akıllı Şehir Sistemleri	Veri Güvenliği	Elektrikli Araç Teknolojileri
Makine Öğrenmesi	Bulut Bilişim	İş Zekası Uygulamaları	Yönetişim Sistemleri
Derin Öğrenme	Sosyal Ağlar	Adli Bilişim	Sanal Gerçeklik
Dijital Yaşam	Bilişim Hukuku	Nesnelerin İnterneti	Kablosuz Ağ Uygulamaları
E-Ticaret	Sanallaştırma	Bilgisayar Ağ Güvenliği	İnsan-makine Etkileşimi
Kayıt Zinciri,kripto Paralar	Güvenlik Duvarları	Mobil Uygulamalar	Veri Modelleme
Dijital Ekonomi	Veri Depolama Üniteleri	Enerji Bilişim Sistemleri	Güvenlik Sistemleri

25.01.2023
MAKALE SON KABUL TARİHİ

bilisimbatmanda
ifest.batman.edu.tr
ifest@batman.edu.tr

BİLİŞİM FESTİVALİ IFEST 2023

9 - 11 ŞUBAT 2023 | BATMAN / TÜRKİYE

Slidesgo

Ref 1: We Are Social Dijital Türkiye Raporu, link

Ref 2: Havelsan Akademi, link

Ref 3: Bilgi Güvenliği Derneği, link

Ref 4: Technofesör, link

Ref 5: Batman Çağdaş, link

TEŞEKKÜRLER

Dr. Hafzullah İŞ