KASTAMONU
İL MİLLİ EĞİTİM MÜDÜRLÜĞÜ

TÜRKİYE YÜZYILI

AİLE AKADEMİSİ

"GÜÇLÜ AİLE, GÜVENLİ GELECEK"

24 EKİM 2024
17 ARALIK 2024

Aile Akademisi Eğitimleri

Bilinçli Teknoloji ve Sosyal Medyanın Güvenli Kullanımı

İçindekiler

Genel Bakış

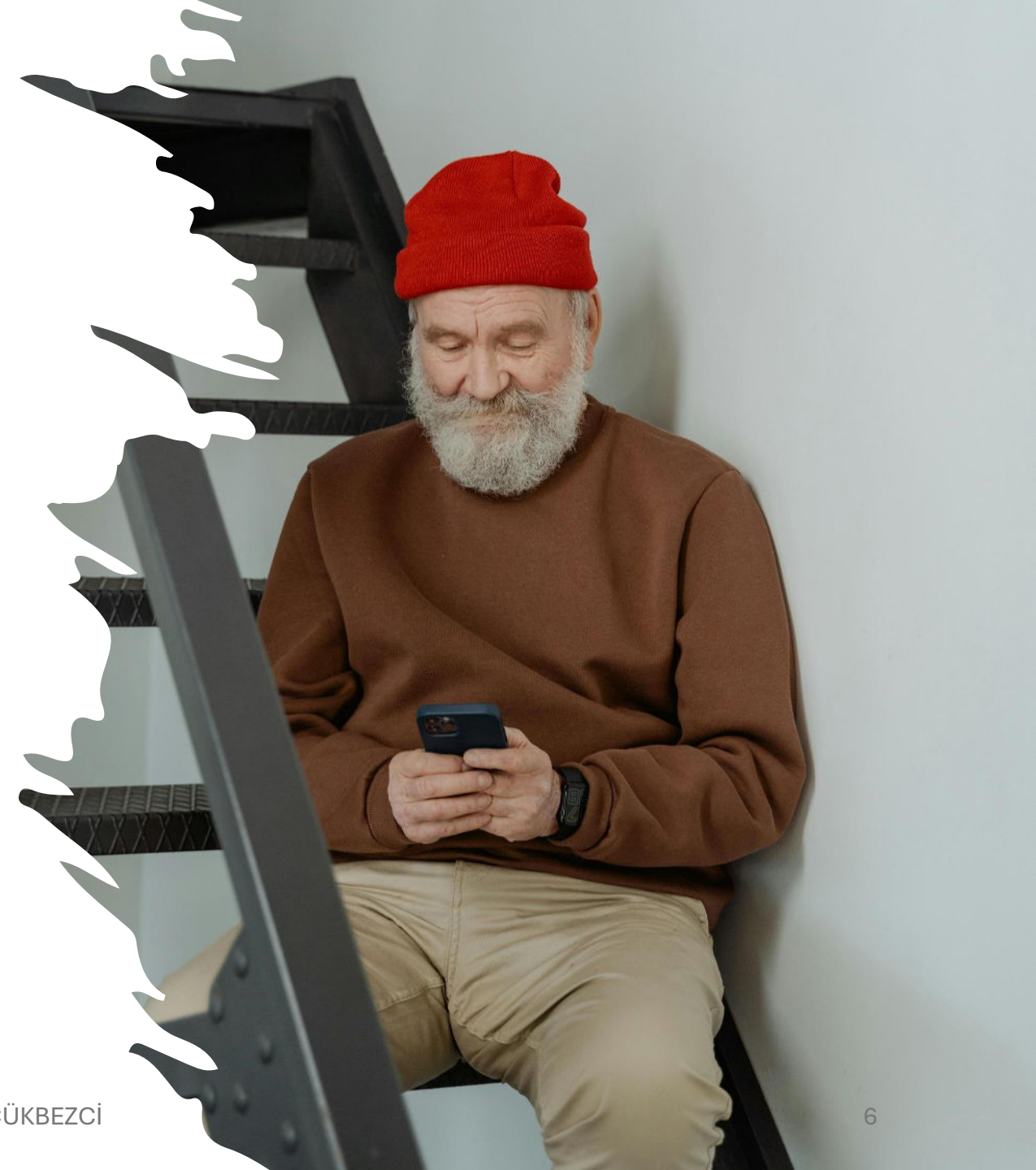
- Günümüzde birçok sosyal ağ ortaya çıkmıştır ve bu sosyal ağlar genellikle birçok kişi tarafından gerçek kimlikleri ile kullanılmaktadır. Ayrıca, sosyal ağlar sohbet, çevrimiçi oyunlar oynama, dosya paylaşımı gibi farklı amaçlar için aktif şekilde kullanılmaktadır.

Genel Bakış

- Sosyal ağlar yaşamımızda kullanmaktan keyif aldığımız, eski dostlarımızla haberleştiğimiz ve yeni arkadaşlar edindiğimiz, gruplar oluşturduğumuz, kendimiz ve fikirlerimiz hakkında paylaşımlar yaptığımız ve çeşitli aktivitelerde bulunduğumuz alanlar haline gelmiştir.

Genel Bakış

- Arayüzlerinin ve üyeliğin kolay ve anlaşılır olması, sosyal ağların birçok kullanıcıya hitap etmesini sağlamaktadır.
- Günümüzde sosyal ağ kullanıcısı kendi hayatlarında olup bitenleri, güncel olayları, ilgi alanlarını rahat bir şekilde arkadaşı olduğu birçok insanla paylaşabilir, fikirlerini belirtebilir.
- Ayrıca video, resim gibi sosyal içerik paylaşımlarında bulunabilir, başkalarının paylaştıklarından haberdar olabilir.



Genel Bakış

- Sosyal ağlar, günümüz dünyasının vazgeçilmezi haline gelmiş olup yaptığımız dijital faaliyetlerin büyük bir çoğunluğu bu sosyal paylaşım sitelerinde gerçekleştirilmektedir.

Genel Bakış

- Sosyal ağların bu kazandırdıkları yanında davranışlarımızın analiz edilmesine izin verme, düşmanlarımıza fırsat sunma, tehditler alma, kişisel bilgilerimizi paylaşarak güvenliğimizi tehlikeye atma gibi riskleri de beraberinde barındırmaktadır.
- Sosyal ağlarda güvenliğin sağlanması oldukça önemli ve zor bir problemdir.

Neden İnternet Ortamında Güvenliğe Önem Vermeliyiz?

- İnternet’te gezinirken; yaptığımız faaliyetler, tüm alışverişler veya gönderilen tüm e-postalar üçüncü şahıslar tarafından izlenebilmektedir.
- İnsanlar sosyal ağlarda fotoğraflarını, yediğini içtiğini, hatta özel hayatlarına ilişkin bilgileri de paylaşmaktadır. Kimi zaman bunu farkında olmadan, kimi zamanda kendini başkalarına ne kadar sosyal olduğunu göstermek amacıyla yapmaktadır. Bu bilgiler kötü düşünceli kişilerin eline geçtiğinde, farklı amaçlar için kullanılabilmektedir.

Neden İnternet Ortamında Güvenliğe Önem Vermeliyiz?

- Bu durumdan kurtulmak imkânsız gibidir, çünkü bilgilerinizi silseniz hatta hesaplarınızı kapatsanız bile veri tabanından verileriniz silinmemektedir. Böyle bir ortamda güvenlik ve mahremiyet ile ilgili çözümler her geçen gün daha da önem kazanmaktadır.

Düşünelim

-if you don't pay for the product you are the product-

-eğer ürün için ödeme yapmazsan ürün sensin-

Düşünelim

- Örneğin; Sosyal ağlar verdikleri hizmet karşılığı ücret almazlar ama kullanıcıların bilgilerinin gizli tutulmadığı bir gerçektir.

Düşünelim

- Birçok dijital platform, aslında kazançlarını kullanıcıların verilerini toplayarak ve bu verileri reklamlara veya diğer pazarlama stratejilerine dönüştürerek elde eder. Genellikle kişisel verilerini (ilgi alanları, alışveriş alışkanlıkları, konum verisi vb.) toplar ve bu veriler, şirketlerin ürün ve hizmetlerini daha etkili bir şekilde pazarlamalarına olanak tanır.

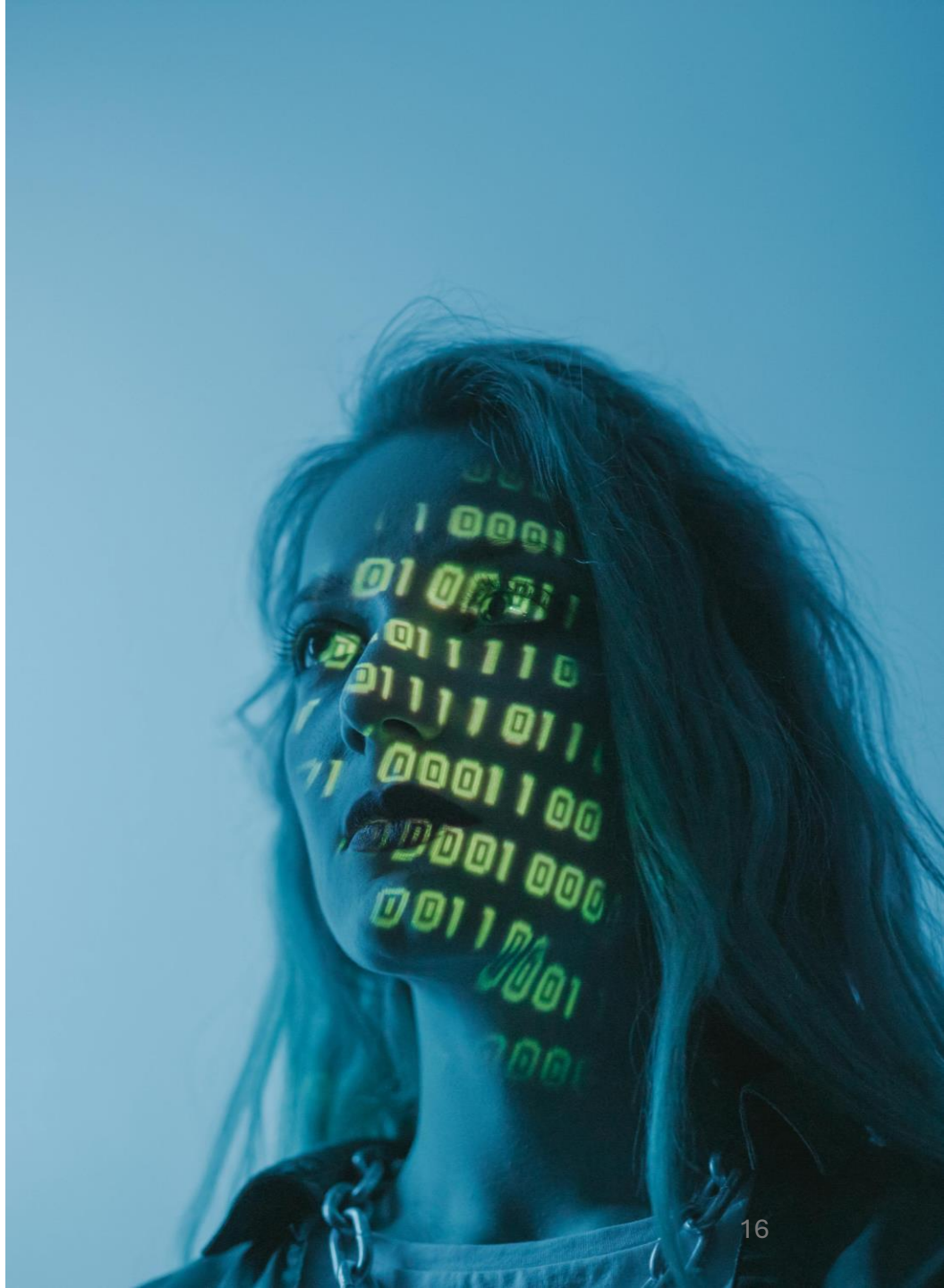
Sosyal Ağlarda Güncel Güvenlik Tehditleri

Kimlik Hırsızlığı

- Kimlik hırsızlığı, istenmeyen kişilerin bilgilere ulaşması ve bu kişilerin bilgileri kötü amaçları doğrultusunda kullanmasıdır. Kullanıcıların sosyal ağlardaki paylaşımları hırsızların işlerini daha da kolaylaştırmaktadır. Bazı saldırganlar da kullanıcıdan izin isteyen uygulamalar ile saldırı yapmaktadır.
- Kullanıcı, kendi bilgilerine erişilebilmesi izni verdiğinde, saldırgan kullanıcının bilgilerine erişebilmekte ve kötüye kullanabilmektedir. Kimlik hırsızlığında genellikle kullanıcı şifresini ve bireylerin banka hesap bilgilerini çalma hedeflenmektedir. Kimlik hırsızlığında aktif olarak kullanılan yöntemler oltalama ve zararlı yazılımlardır.

Kimlik Hırsızlığı

- Oltalama yönteminde dolandırıcılar sahte e-posta göndererek kişileri sahte web sitesine yönlendirir ve kullanıcı bilgilerinin girilmesi durumunda bütün bu bilgiler dolandırıcıların eline geçmiş olur. Bu e-postanın sahte olduğunun anlaşılması da oldukça zordur. Çünkü kuruluşun simgesi ve web sayfasının kopyası kullanılabilmektedir. Diğer bir yöntemde zararlı programların, kullanıcının dikkatini çekmek için isminin değiştirilip bilgisayara indirilmesi sağlanarak yapılmaktadır.



E-Dolandırıcılık

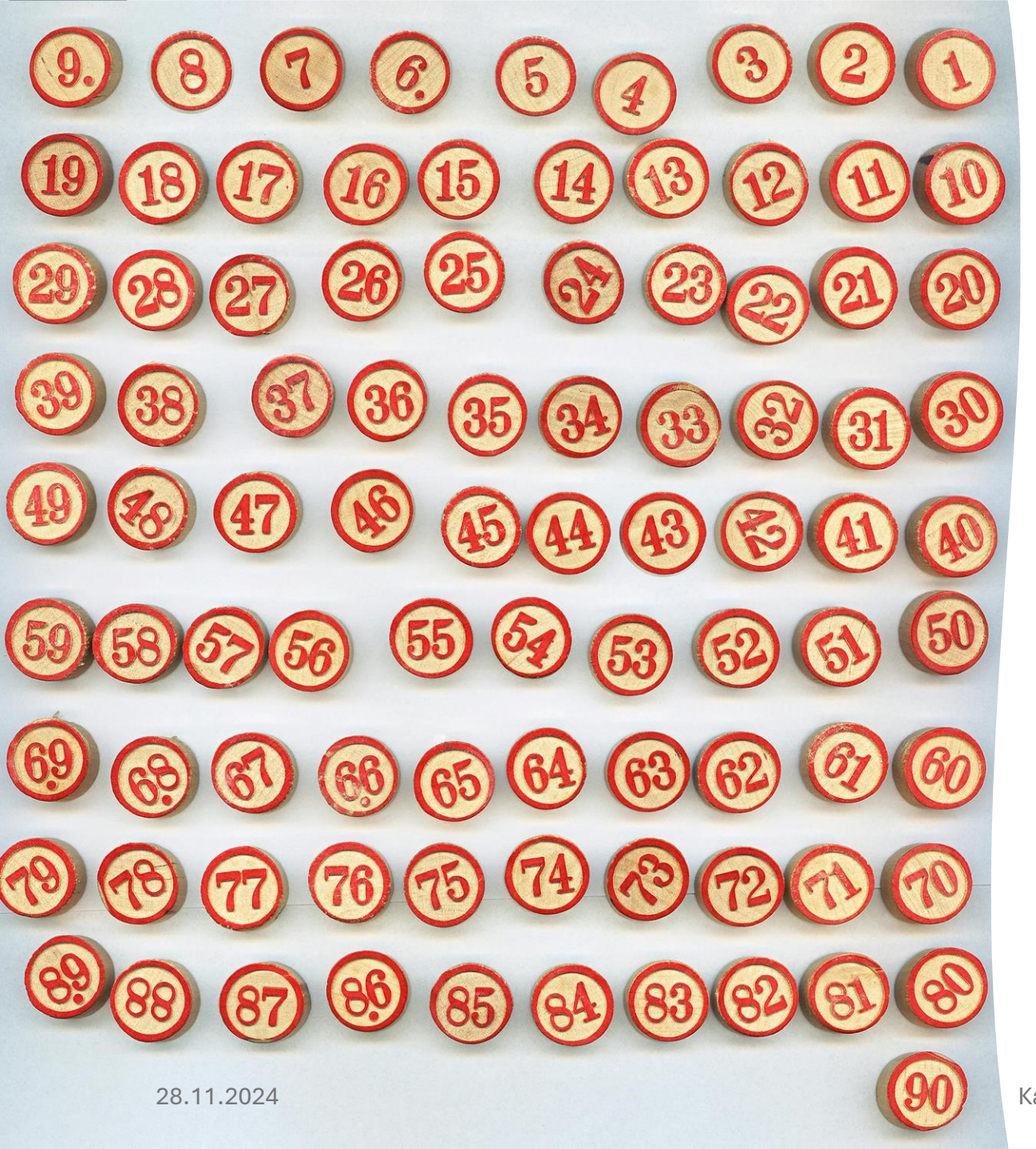
- Başka bir kullanıcının şifresini izinsiz kullanma ve banka hesap bilgilerini çalma gibi teknikler e-dolandırıcılık yöntemleri kapsamındadır. Bu yöntemlerle dolandırıcılar, kullanıcı bilgilerini elde etmek için yasal bir siteden posta gönderiyormuş gibi yaparlar. Kullanıcı ilgili linki tıkladığında bilgilerinin çalınacağı sayfaya yönlendirilmiş olur.

Bilinen Bazı E-Dolandırıcılıklar

Günümüzde insanlar bu yöntemlerle dolandırılıp, mağdur olmaktadır.

İyi Bilinen Şirketlerin Adlarını Kullanma

- Bu yöntemde ünlü firmaların adını kullanan sahte eposta iletileri veya web siteleri kullanılır. E-posta mesajında, bir yarışmanın kazanıldığı ve oturum açma bilgileri veya parolaya ihtiyaç olduğu söylenir. Bu sahte teknik destek dolandırıcılıkları genelde telefonla yapılır.



Piyango Dolandırıcılıkları

- Sosyal ağ kullanıcısına piyango kazandığına dair bir mail gelir. Aslında böyle bir piyango yoktur ve bu mail siber suçlular tarafından gönderilmiştir. Bu epostalar, kişiyi kendilerine para göndermeye ikna etmek ve kişiyle iletişim kurmak amacıyla hazırlanmıştır. Farklı sebeplerle para koparmak için kişiyle iletişime tekrar geçmeye çalışırlar. Kurgusal nitelikteki ödülü almak içinde bazı masraf ücretleri talep edilir. Suçlular bu konularda çok üretkendir.

Sahte Güvenlik Yazılımı Dolandırıcılıkları

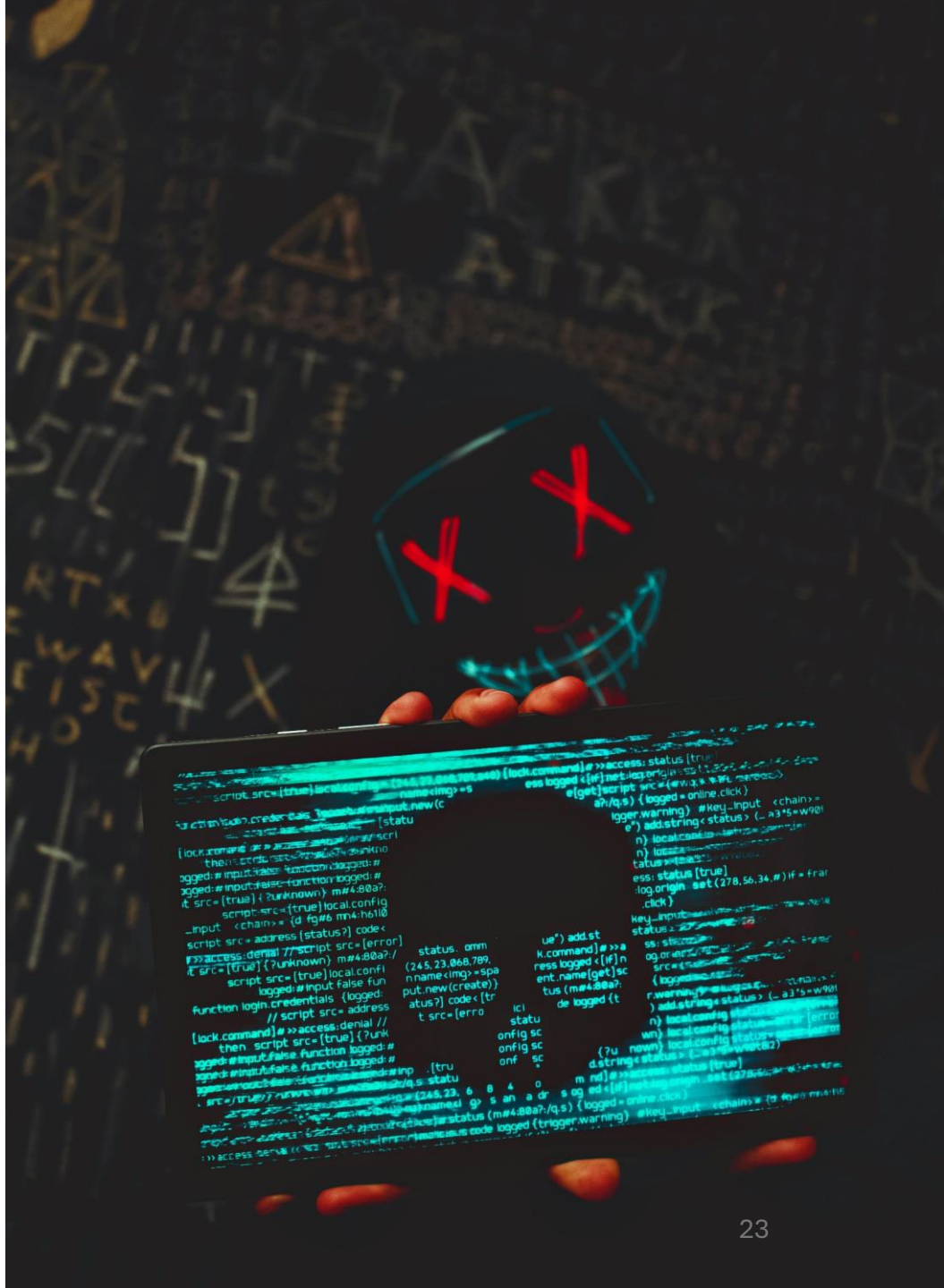
- "Korkutma amaçlı yazılımlar" olarak da bilinen sahte güvenlik yazılımları, güvenlik açısından yararlı gibi görünse de sınırlı veya sıfır güvenlik sağlayan yazılımlardır. Bu dolandırıcılıklar ile sosyal ağ sitelerinde, reklamlarda, arama motoru sonuçlarında veya bilgisayarda açılan pencereler şeklinde karşılaşılabilir. İşletim sisteminin bir parçası gibi görünebilirler, fakat gerçekte zararlı yazılımlardır.

Profil Klonlama

- Bu saldırı yöntemi sosyal ağ sitelerinde oldukça sık kullanılır çünkü profil klonlamayla ilgili güvenlik önlemi neredeyse hiç yoktur. Bu suç tipinde kullanıcının profil resmi kopyalanır aynı isim ve soyisim ile profil oluşturulur. Oluşturulan bu profil sayfasına pornografik resimler koyma ve cep telefon numarası yazarak cinsel konularda görüşme talebinde bulunma gibi durumlarla karşılaşılmaktadır.
- Saldırgan ilgili kişinin profilinin aynısını oluşturur ve genelde profilini çaldığı bu kişinin itibarını zedelemeyi hedefler. Facebook kullanıcılarının resimlerini ve kişisel bilgilerini sınırlandırmaları bu gibi durumlardan korunmalarını sağlayacaktır.

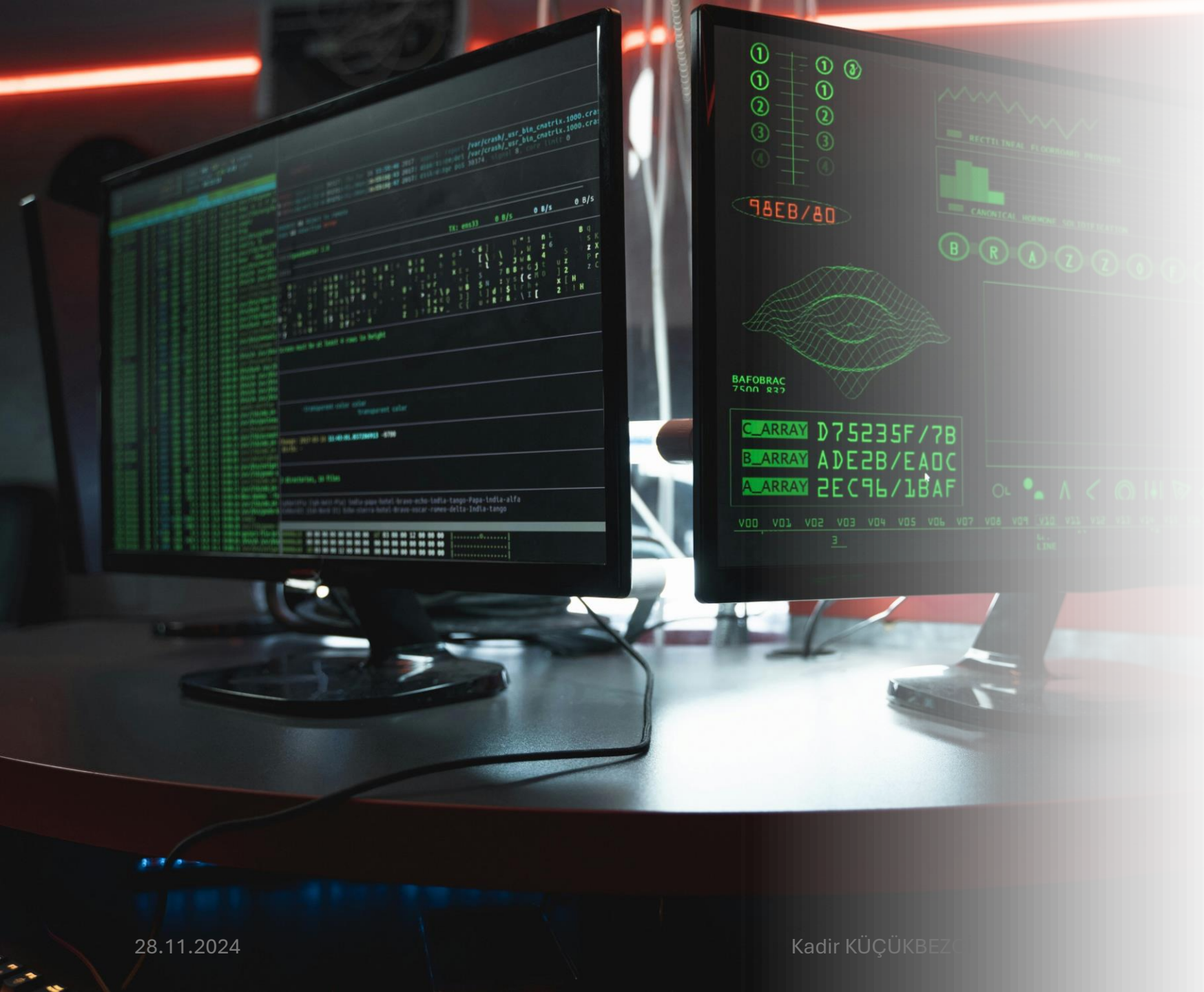
Üçüncü-Kişi Uygulama Tehlikeleri

- Saldırgan, kullanıcı bilgilerine ulaşmak için oyunlar gibi sosyal ağ uygulamalarını kullanır. Bu sayede kullanıcı, sahte uygulamayı kullanarak bilgilerinin saldırgan tarafından ele geçirilebilmesine sebep olmaktadır.



Sahte Ürün Satışı

- Saldırgan, dikkat çeken indirimler ile süslenen çok satan bir ürünün reklamlarını sosyal ağ ortamlarına koyar. Sattığını iddia ettiği ürünün alınabilmesi için kullanıcıdan kullanıcı bilgileri ve banka şifreleri gibi kişisel bilgilerini ister. Eğer kullanıcı ürünü almak için kişisel bilgilerini verirse, saldırgan bu bilgileri elde eder ve amacı doğrultusunda kullanır.

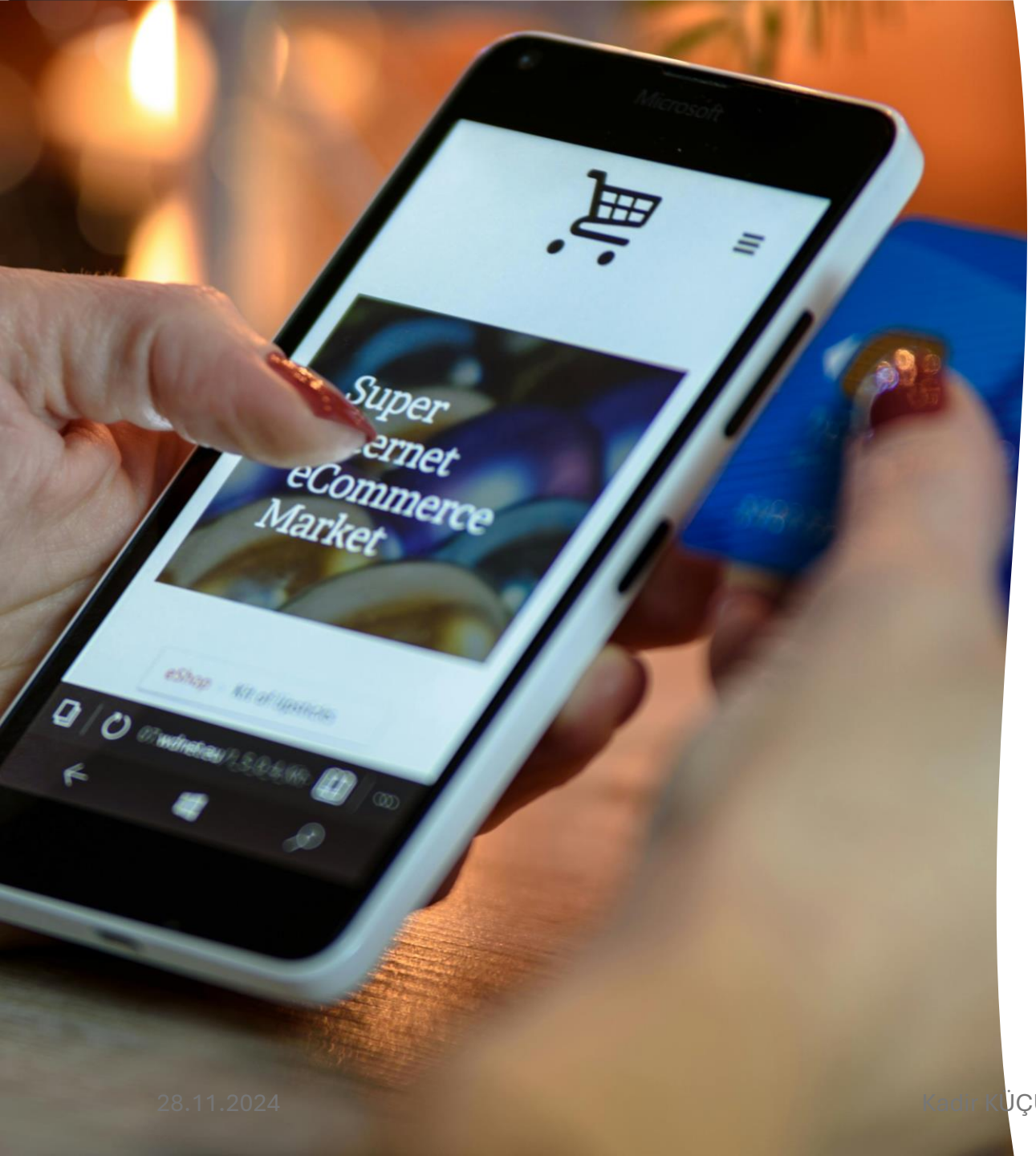


Kötü Bağlantı İstekleri

- Dolandırıcılar, sahte profil oluştururlar ve hedef kullanıcıların onlarla iletişime geçmesi için arkadaşlık istekleri gönderirler. Kullanıcı gelen arkadaşlık isteğini kabul ederse, diğer arkadaşlarıyla paylaştığı bilgileri dolandırıcıların da görmesine neden olur. Bu şekilde dolandırıcılar kullanıcının bilgilerini kötü amaçlı kullanabilirler.

İstenmeyen E-postalar

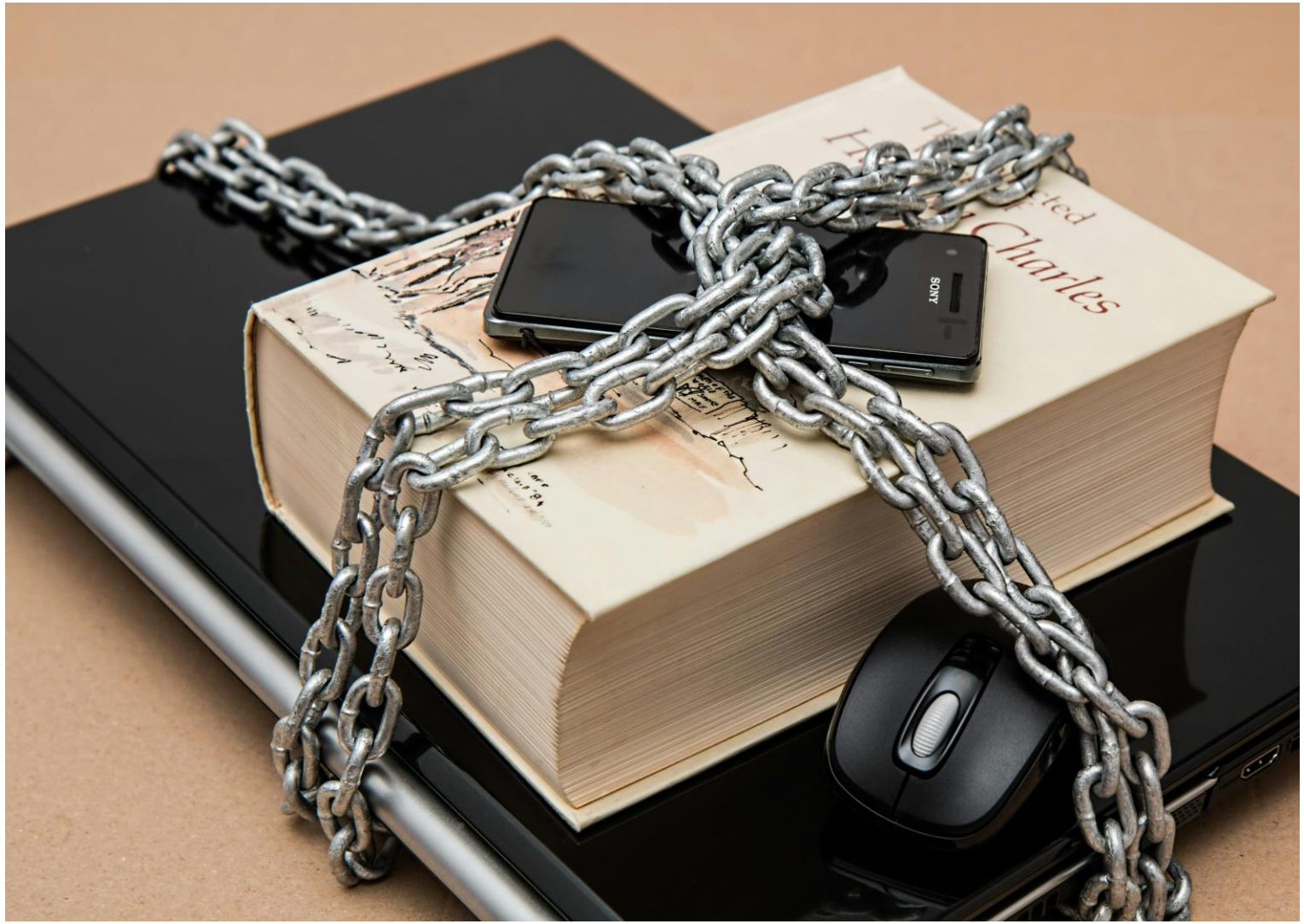
- İstenmeyen epostalar, kişinin isteği olmadan kişiye gelen reklam içerikli maillerdir. Internet üzerinde aynı mesajın, bu mesajı alma talebinde bulunmamış kişilere toplu olarak gönderilmesi de genelde istenmeyen epostalar olarak adlandırılır. İstenmeyen epostalar genellikle ticari reklam niteliğinde olup, güvenilmeyen ürünlerden fazla para kazanma amacına yöneliktir.



Düzenbaz Site Kodlamaları

- Bu yöntemle kullanıcı web'de gezinirken kullanıcının haberi olmadan zararlı yazılım çalıştırılır ve bu sayede kullanıcı bilgileri elde edilmeye çalışılır.

Sosyal Ağlardaki Mevcut Sorunlardan Korunma Yöntemleri

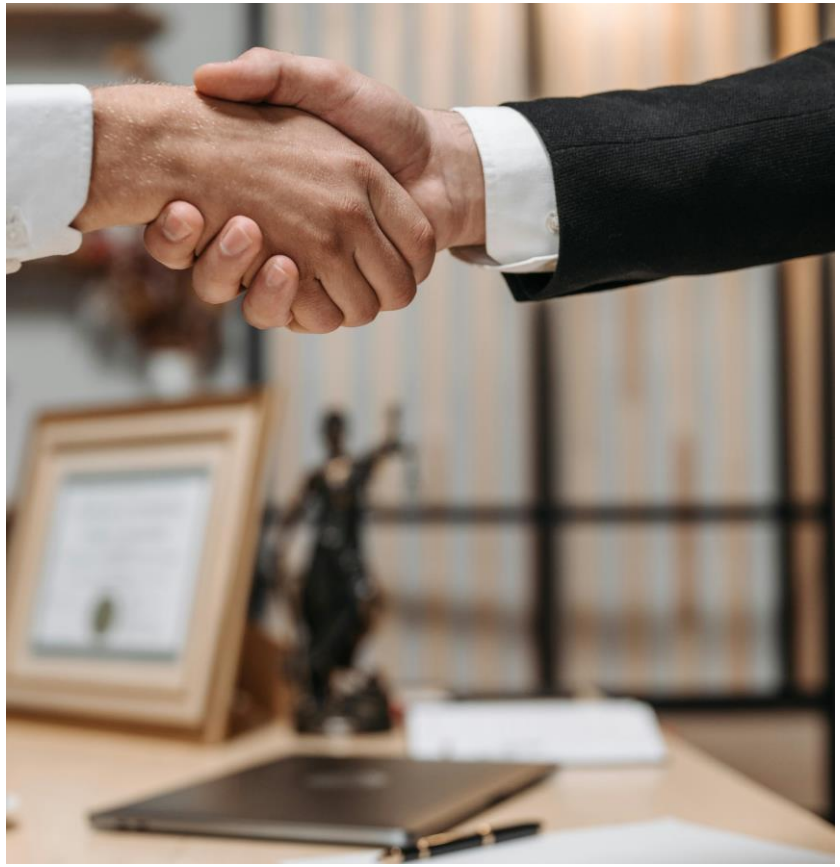


Sosyal Ağlardaki Mevcut Sorunlardan Korunma Yöntemleri

- Sosyal ağ kullanıcıları her geçen gün artmaktadır ve bu siteler hayatımızda önemli bir yer edinmiştir. Sosyal ağları; hackerlar, siber mühendisler ve spam gönderenler bilgi toplama amacıyla hedef edinmişlerdir.

Alınabilecek Tedbirler Nelerdir?

- Öncelikle kullanılacak sosyal ağ dikkatlice seçilmelidir. Üye olmadan önce gizlilik politikası, kullanım şartları ve özel şartlar okunmalı, kişisel bilgilerin hangi şartlarla 3. şahıslarla paylaşılacağı bilincine sahip olunmalı ve ona göre karar verilerek üyelik işlemlerine başlanmalıdır.
- Sitenin insanların yayınladıkları içerikleri izleyip izlemediği öğrenilmelidir. Bu web sitesine kişisel bilgiler verileceğinden, kredi kartı bilgilerinin girildiği bir siteyi seçerken gösterilen hassasiyetin aynısı gösterilmelidir.

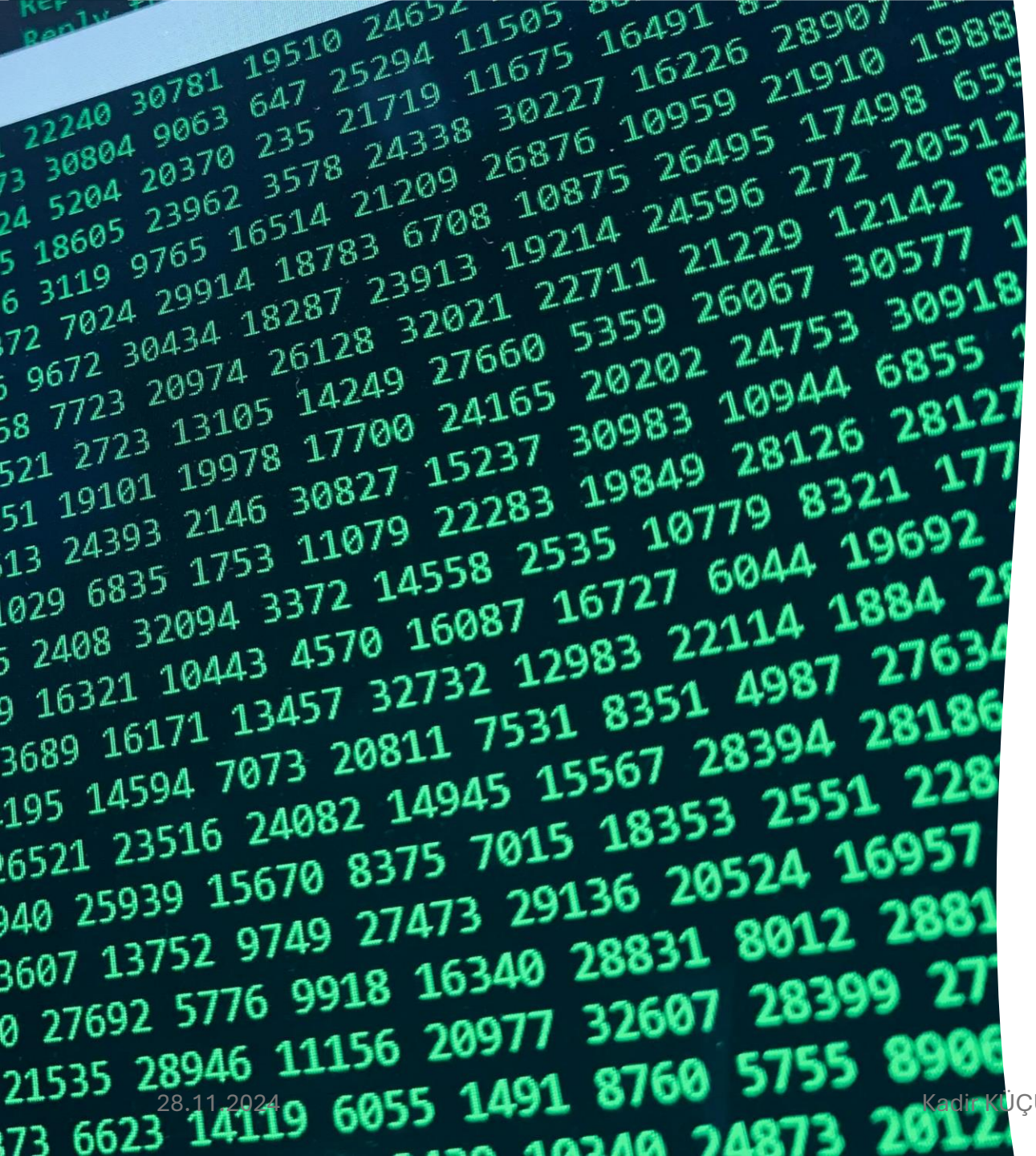


Alınabilecek Tedbirler Nelerdir?

- Çocuk kullanıcılar için en önemli görev ailelerine düşmektedir. İlk olarak aileler çocukları olabildiğince bu ortamlardan uzak tutmalıdır. Bu mümkün olmadığı zamanlarda ise dikkatli olmaları için uyarılarda bulunulmalı, güvenli kullanmaları konusunda eğitilmelidirler. Bunun için ebeveynin çocukla yüz yüze iletişim kurması gerekmektedir. Çocukların bu ağlar hakkındaki deneyimleri öğrenilmeli, çocuğun durumuna göre bilgilendirme yapılmalıdır.

Alınabilecek Tedbirler Nelerdir?

- Sosyal ağda çocukların gerçek adlarını kullanmadığından, adres, telefon, okul, sınıf ve kimlik bilgileri gibi bilgileri paylaşmadığından emin olunmalıdır. Çocuklar kontrol edilmeli, verilmiş olan önemli bilgiler varsa düzeltilmelidir. Fotoğraflarda detay verilmemesi, fotoğraf etiketlemelerinden kaçınılması, kişisel resimlerin paylaşılmaması ve tanımadıkları kişilerle haberleşmemeleri konusunda kesinlikle uyarılarda bulunulmalıdır.



Alınabilecek Tedbirler Nelerdir?

Paylaşılması risk içeren bilgi varlıklarından bazıları şunlardır.

- E-devlet bilgileri
- İşyeri ve konum bilgileri
- Nüfus cüzdan bilgileri
- Sağlık güvenlik bilgileri
- Ehliyet, pasaport bilgileri
- İnteraktif banka hesap bilgileri
- Kredi kart bilgileri
- Kurum ve maaş bilgileri
- Her türlü kullanıcı adı ve şifre bilgileri

Bu bilgilere ek olarak anlık konum bilgisi, kullanıcıya ve yakın çevresine ait fotoğraflar, eğitim bilgileri ve özel hayata ilişkin bilgiler de paylaşılmamalıdır.

Alınabilecek Tedbirler Nelerdir?

- Bu gibi bilgilerin paylaşılmadığından emin olunmalıdır. Bilgi içeren adresler kullanmaktan kaçınılmalı ve içinde büyük küçük harf, rakam, özel karakterler içeren güçlü şifreler tercih edilmelidir.

Sosyal Ağlardaki Riskleri Azaltmak İçin Öneriler

- Sadece yayınlanması istenilen bilgiler paylaşılmalıdır.
- Sadece güvenilen kişiler arkadaş listesine eklenmelidir.
- Asla tam olarak hiç kimseye güvenilmemelidir. Tanınmayan kişilerden gelen beklenmedik bağlantıları tıklamaktan kaçınılmalıdır.

Sosyal Ağlardaki Riskleri Azaltmak İçin Öneriler

- Sosyal ağın adı doğrudan tarayıcıya yazılmalı veya kişisel sık kullanılanlar listesi kullanılarak giriş yapılmalıdır. Bu işlem daha güvenilirdir. Tıklanan herhangi bir bağlantının, kişisel bilgileri çalmak için düzenlenen sahte bir link olabileceği ve bunun bir casus veya kötücül yazılımı tetikleyebileceği unutulmamalıdır.

- İnternet ve sosyal medya her zaman dikkatli kullanılmalıdır.Kişisel veri veya bilgiler sosyal ortamlarda paylaşılmamalıdır.

Sosyal Ağlardaki Riskleri Azaltmak İçin Öneriler

- Paylaşılan dokümanların/belgelerin veya bilgilerin telif hakkı oluşturabileceği hatırda bulundurularak kullanılmalı veya paylaşım yapılmalıdır.
- Sosyal medya ortamlarının çok yakın takip edildiği dikkate alınarak mümkün olduğunca az resim, bilgi veya belge paylaşılmalıdır.
- Çocukların sosyal medya kullanımı belirli bir yaşa kadar yasaklanmalı veya gözetimli olarak kullanmalarına izin verilmelidir. Kontrol veya denetim yoksa açılmasına müsaade edilmemeli veya açılmış ise hesapları kapatılmalıdır.

Sosyal Ağlardaki Riskleri Azaltmak İçin Öneriler

- Bu ortamlarda suç unsuru barındıran içerikler paylaşılabilmektedir. Bunların paylaşımının adli sonuçlar doğurabileceği unutulmamalıdır.
- Bu ortamlarda kişilere hakaret edici yazılar yazılmamalı veya paylaşılmamalıdır. Bunun sonucu olarak adli takip yapıldığı ve ceza alınabileceği unutulmamalıdır.
- Sosyal ortamlara saldırılar sıkça yapılmaktadır. Erişim şifreleri en önemli hedeflerden birisidir. Şifrelerin çalınmaması ve kolay kırılmasının önüne geçmek için kırılması zor şifreler kullanılmalı ve sıklıkla değiştirilmelidir.

Sosyal Ağlardaki Riskleri Azaltmak İçin Öneriler

- **Bir bilgiyi dijital ortama taşırken bunun gerekli olup olmadığını düşünüp karar verdikten sonra bunu gerçekleştirmeliyiz.**

Sosyal Ağlardaki Riskleri Azaltmak İçin Öneriler

- Ülkemizde ücretsiz olarak verilen Güvenli İnternet hizmetinden mutlaka faydalanılmalıdır. Operatörler tarafından ücretsiz verilen bu hizmetin dünyada bu alanda sunulan ilk hizmetlerden birisi olması da önem arz etmekte olup karşılaşılabilecek tehditlerin filtrelenmesi sağlanmakta, kullanılarak farklı hizmetler sunabilmektedir.

Hazırlayan-Düzenleyen

Beni dinleyip zamanınızı ayırdığınız için teşekkür ederim.

Kadir KÜÇÜKBEZCİ-

Psikolojik Danışman

Kaynakça

E. B. Ceyhan, E. Demiryürek, and B. Kandemir, “SOSYAL AĞLARDA GÜNCEL GÜVENLİK RİSKLERİ VE KORUNMA YÖNTEMLERİ”, UBGMD, vol. 1, no. 1, pp. 1–10, 2015, doi: 10.18640/ubgmd.192646.