SANS SECURITY AWARENESS

# Güvenlik Farkındalığı Uygulama Kılavuzu – Evde Güvenli Çalışma

# İdari Özet

Coronavirus nedeniyle çoğu kuruluş, iş gücünü evden çalışmaya yönlendirme yoluna gitmek zorunda kaldı. Tabii, pek çok kurum faaliyetlerini uzaktan çalışma ile yürütmek için gerekli politikalara, teknolojiye ve eğitime sahip olmadığı için bu durum çeşitli zorlukları da beraberinde getirebiliyor. Ayrıca çoğu personel de evden çalışma fikrine aşina değil ve bundan rahatsız olabiliyor. Bu rehberin amacı, bu kişileri hızlı bir şekilde mümkün olduğunca güvenli bir şekilde çalışmaları için eğitmektir. Bu rehberi nasıl kullanacağınız hakkında sorularınız varsa support@sans.org adresinden bizimle iletişime geçin.

İş gücünüz muhtemelen büyük bir stres ve değişim içinde olduğu ve kurumunuzun zamanı ve kaynakları sınırlı olduğu için bu stratejik rehber, eğitimi mümkün olduğunca basitleştirmeye odaklanmıştır. Aşağıda açıkladığımız, en ağır zarara yol açabilecek en önemli risklere odaklanmanızı öneriyoruz. Bunu bir başlangıç noktası olarak düşünün. Eklemek istediğiniz ek riskler ve konular varsa lütfen ekleyin. Ancak çalışanlarınızın öğrenmesini istediğiniz davranış, prosedür veya teknolojiler ne kadar fazla olursa burların tümünün öğrenilmesi ve uygulamaya geçirilmesi de o kadar zor olacaktır.

# Bu Rehberi Nasıl Kullanmalısınız

Bu rehberdeki materyalleri okuyarak başlamanızı ve mevcut olan bilgiler hakkında size bir fikir vermesi için farklı materyallere olan bağlantıları incelemenizi öneriyoruz. Kurumunuzu angaje etmek ve eğitmek için kullanabileceğiniz, her risk türü için farklı materyaller sunulduğunu göreceksiniz. Bu sayede, kurumunuzun kültürü ve ihtiyaçlarına en uygun, en etkin yöntemleri seçebilirsiniz. Bu belgeyi okuduktan sonra ulaşmaya çalıştığınız hedefi daha iyi anlayabilmek için beraberinde gelen İletişim Taslağını ve Bilgi Formunu da okuyun. Belgeleri inceledikten sonra, bu süreci koordineli bir şekilde yürütmeniz gereken iki ana grup vardır.

1. **Güvenlik Ekibi**: Hangi riskleri yönetmeye çalıştığınızı daha iyi anlamak için güvenlik ekibinizle iş birliği yapın. Bu rehberde evden çalışan personel için en genel riskleri tanımladık ancak sizin karşılaştığınız riskler farklı olabilir. Güvenlik ekiplerinin en sık yaptığı hatalardan biri, tüm riskleri birden yönetmeye çalışarak kişileri çok sayıda politikaya ve prosedüre boğmaktır. Ele alacağınız risklerin sayısını mümkün olduğunca sınırlı tutun. Risklerinizi belirleyip öncelik sırasına aldıktan sonra bu riskleri yönetecek davranışları tespit edin. Daha önce de belirttiğimiz üzere, kurumunuz bunun için gerekli kaynaklara veya zamana sahip değilse aşağıdakilerden faydalanın.
2. **İletişim**: İnsan kaynaklı en önemli risklerinizi ve bu riskleri yönetmek için gereken davranışları belirledikten sonra iletişim ekibinizle iş birliği yaparak çalışanlarınızı bu davranışlar konusunda eğitin ve harekete geçirin. Etkin bir güvenlik farkındalığı eğitim programı için iletişim ekibinin de mutlaka güçlü bir şekilde sürece katılması gerekir.

Mümkünse iletişim ekibinden birini güvenlik ekibinize katın. Çalışanlarınızla iletişim kurarken, dikkatlerini çekmek ve ilgilerini canlı tutmak için, bu eğitimin sadece iş yerinde değil evlerinde kendileri ve ailelerinin güvenliği için de büyük katkı sağlayacağını vurgulayabilirsiniz.

Nihayetinde, bu iki grupla birlikte çalışanlarınız için güvenliği kolay bir hale getirmeye ve onları buna motive etmeye çalışacaksınız. Unutmayın ki, kolaylık ve motivasyon davranış değişikliği yaratan iki temel faktördür. Programı yürütürken görüşlerine ve geri bildirimlerine ihtiyaç duyacağınız önemli kişilerden bir Danışma Kurulu oluşturmanızı da öneriyoruz. Güvenlik ve iletişim ekiplerinizin yanı sıra İnsan Kaynakları ve Hukuk birimlerinizle de iş birliği yapabilirsiniz.

## MGT433 Dijital İndirme Paketi

SANS Institute, MGT433: Etkili Bir Güvenlik Farkındalığı Programı Nasıl Hazırlanır, Korunur ve Ölçülür adlı iki günlük bir eğitim kursu sunmaktadır. Bu hızlandırılmış kurs, insan kaynaklı riskleri etkin bir şekilde yönetip ölçebilmenizi sağlayacak verimli bir farkındalık programı hazırlamanız için gereken tüm teoriyi, becerileri, çerçeveyi ve kaynakları sunmaktadır. Bu rehberin bir parçası olarak, kursun taslaklardan ve planlama kaynaklarından oluşan Dijital İndirme Paketine ücretsiz erişim sağlıyoruz. Bu materyaller, bu programın ihtiyaçlarının ötesinde, büyük kuruluşlar ve daha karmaşık programlar için de faydalı olabilir.

## Çalışanların Sorularına Yanıt Verme

Çalışanlarınızla iletişim kurmanın ve onları eğitmenin yanı sıra tercihen gerçek zamanlı olarak insanların sorularına yanıt verebileceğiniz bir ortamı veya teknolojiyi kullanmanızı da önemle tavsiye ediyoruz. Bu özel bir e-posta adresi, Skype veya Slack sohbet kanalı ya da Yammer gibi çevrim içi bir forum olabilir. Bir diğer fikir de haftada birkaç defa insanların istedikleri zaman ulaşabilecekleri, isterlerse canlı katılıp sorular sorabilecekleri güvenlik web yayını yapmaktır. Bunun amacı, güvenliği mümkün olduğunca ulaşılabilir kılıp sorulara cevap verebilmektir. Bu, çalışanlarınızla iletişim kurmak ve güler yüzlü bir güvenlik yaklaşımı geliştirmek için mükemmel bir fırsat olacaktır. Bunu mutlaka değerlendirin. Unutmayın ki, bunun etkili olması güvenlik kanallarını yönetmek ve sorulara aktif olarak yanıt vermek için kaynak ayırmanıza bağlıdır.

# Riskler ve Eğitim Materyalleri

Uzaktan çalışan personel için ilgilenmeniz gereken üç ana risk belirledik. Bunlar, bir başlangıç noktasıdır ve sizin için muhtemelen en önemli olan risklerdir. Aşağıdaki her risk için konuyu aktarmaya ve eğitime yardımcı çeşitli kaynaklara bağlantılar sağlanmıştır. Kurum kültürünüze en uygun, en etkili olanları seçebilmeniz için farklı iletişim materyalleri sunulmuştur. Ayrıca, neredeyse tüm materyaller birden fazla dilde mevcuttur. Tüm bu materyaller vakit darlığından ötürü başa çıkamayacağınız kadar fazla gelirse aşağıdaki iki materyali kullanmanızı öneririz.

1. Evden Güvenli Çalışma Bilgi Formu (Uygulama Setinizde mevcuttur).
2. Siber Güvenlikli Bir Ev Yaratma videosu (İngilizce) ayrıca buradan diğer dillerde de mevcuttur

## Sosyal Mühendislik

Büyük değişikliklerin ve acil durumların bulunduğu böyle bir ortamda uzaktan çalışanların karşılaşabileceği en büyük risklerden biri sosyal mühendislik saldırılarıdır. Sosyal Mühendislik, saldırganların kurbanlarını kandırarak hataya zorladığı, özellikle de değişim ve karmaşa durumlarında daha da kolaylaşan psikolojik bir saldırı türüdür. Önemli olan, insanları sosyal mühendisliğin ne olduğu konusunda eğitmek, böyle bir saldırıya yönelik işaretlerin nasıl fark edileceğini ve saldırı karşısında ne yapılması gerektiğini öğretmektir. Sadece e-postayla kimlik avına değil, telefon çağrıları, mesajlar, sosyal medya veya sahte haberler gibi yöntemlere de odaklanmalısınız. Sosyal Mühendislik Destek Materyalleri klasöründe bu konuda eğitim vermek ve konuyu desteklemek için ihtiyacınız olan materyalleri bulabilirsiniz. Ayrıca, buradaki iki SANS Güvenlik Farkındalığı videosunu da kullanabilirsiniz. Bunlar diğer dillerde de mevcuttur.

- Sosyal Mühendislik (İngilizce), ayrıca burada diğer dillerde de mevcuttur
- Kimlik Avı (İngilizce), ayrıca burada diğer dillerde de mevcuttur

## Güçlü Parolalar

Yıllık Verizon DBIR'de belirtildiği üzere, zayıf parolalar küresel çapta ihlallerin en büyük sebeplerinden biri olmaya devam etmektedir. Bu riskin üstesinden gelmeye yardımcı olan dört temel davranış vardır. Bu konuda eğitim vermek ve bu dört temel davranışı güçlendirmek için gereken materyalleri Parolalar klasöründe bulabilirsiniz.

- Kelime Grupları (karmaşık parola oluşturma ve parolaları düzenli olarak değiştirme yöntemleri artık geçerliliğini kaybetti).
- Her hesap için farklı bir parola
- Parola Yöneticileri
- MFA (Çok Faktörlü Doğrulama). Genellikle İki Adımlı veya İki Faktörlü Doğrulama da denir

## Sistemlerin Güncel tutulması

Üçüncü nokta, çalışanların kullandığı tüm teknolojilerin en son işletim sistemi, program ve mobil uygulama sürümleri ile daima güncel tutulmasını sağlamaktır. Bu kapsamda, kişisel cihazlar kullananların otomatik güncellemeleri etkinleştirilmesi gereklidir. Bu konuda eğitim vermek ve konuyu desteklemek için gereken materyalleri Kötü Amaçlı Yazılımlar veya Siber Güvenlikli Bir Ev Yaratmak klasörlerinde bulabilirsiniz.

### Dikkat edilmesi gereken diğer konular

- **Wi-Fi**: Wi-Fi erişim noktasının güvenceye alınması. Bu konu, Siber Güvenlikli Bir Ev Yaratmak materyallerinde açıklanmaktadır. Ayrıca, bu Siber Güvenlikli Bir Ev Yaratma videosunu (İngilizce) da kullanabilirsiniz. Video burada diğer dillerde de mevcuttur.

- **VPN'ler**: VPN nedir ve neden kullanılmalıdır. VPN'ler hakkında OUCH haber bültenini kullanmanızı öneririz.

- **Uzaktan Çalışma**: Bu materyal evden DEĞİL ama uzaktan, ofis dışında kafe, havaalanı veya otel gibi yerlerde çalışan personele yöneliktir. Uzaktan Çalışma eğitim videomuzu (İngilizce) kullanmanızı öneririz. Video burada diğer dillerde de mevcuttur.

- **Çocuklar / Misafirler**: Aile bireylerinin / misafirlerin iş cihazlarından uzak tutulması konusundaki farkındalığı artırmak için Uzaktan Çalışma eğitim videosunu (İngilizce) i kullanmanızı öneririz. Video burada diğer dillerde de mevcuttur.

- **Algılama / Yanıt**: Kişilerin evden çalışırken yaşadığı olayları rapor etmelerini istiyor musunuz? Peki, ne zaman rapor etmelerini istiyorsunuz? Bu konudaki materyalleri Hacklendiniz başlığı altında bulabilirsiniz.

# OUCH Haber Bültenleri

Ayrıca, programınızı desteklemek için herkese açık olan ve yirminin üzerinde dile çevrilen OUCH haber bültenlerini kullanabilirsiniz. Evden Güvenli Çalışmayı destekleyeceğine inandığımız OUCH haber bültenleri aşağıda listelenmiştir. Tüm haber bültenlerini çevrim içi OUCH Güvenlik Farkındalığı Haber Bülteni Arşivlerinde bulabilirsiniz.

## GENEL BAKIŞ

Four Steps to Staying Secure (Güvende Kalmak için Dört Adım)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Siber Güvenlikli Ev Yaratma)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

## SOSYAL MÜHENDİSLİK

Social Engineering (Sosyal Mühendislik)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Mesaj / SMS Yoluyla Kimlik Avı)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Kişiye Özel Dolandırıcılık)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (CEO Dolandırıcılığı)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Telefonla Saldırı / Dolandırıcılıkk)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Kimlik Avını Durdurun)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Sosyal Medya Yoluyla Dolandırıcılık)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

## PAROLALAR

Making Passwords Simple (Parolaları Sadeleştirmek)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Oturumu Kilitleme - 2FA)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

### DİĞER

Yes, You Are a Target (Evet, Hedef Sizsiniz)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Akıllı Ev Cihazları)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

## Kısa İpuçları

Kolayca kullanılabilecek formatta paylaşabileceğiniz ipuçları.

- Evinizdeki kablosuz ağı güvenceye almak için atabileceğiniz en iyi adımlar, varsayılan yönetici parolasını değiştirmek, WPA2 şifrelemesini etkinleştirmek ve kablosuz ağınız için güçlü bir parola kullanmaktır.
- Bebek monitörleri, oyun konsolları, televizyonlar, ev aletleri ve hatta arabanız da dahil olmak üzere ev ağınıza bağlanan tüm cihazlara dikkat edin. Tüm bu cihazların güçlü bir parolayla korunduğundan ve/veya işletim sisteminin son sürümünü kullandığından emin olun.
- Evinizdeki bilgisayarı korumanın en etkin yollarından biri, işletim sistemi ve uygulamalar için en son yama ve güncellemeleri yüklemektir. Ayrıca mümkünse otomatik güncellemeyi etkinleştirin.
- Nihayetinde, en iyi savunma sağduyunuzdur. Bir e-posta, telefon konuşması veya çevrim içi bir mesaj size garip, şüpheli veya fazlasıyla iyi geliyorsa bu bir saldırı olabilir.
- Her hesabınızın ayrı ve eşsiz bir parolaya sahip olduğundan emin olun. Her parolanızı/kelime grubunuzu hatırlayamıyor musunuz? Tüm parolalarınızı yönetmek için bir parola yöneticisi kullanabilirsiniz.
- İki adımlı doğrulama, tüm hesaplarınız için atabileceğiniz en iyi güvenlik adımlarından biridir. İki adımlı doğrulama, hesaba giriş için parolanızın yanı sıra mobil cihazınıza gönderilen veya cihazınız tarafından oluşturulan bir kodun da kullanılması demektir. İki adımlı doğrulamayı destekleyen hizmetler arasında Gmail, Dropbox ve Twitter bulunmaktadır.
- Kimlik avı, saldırganın sizi kandırarak kötü amaçlı bir bağlantıya tıklamaya veya bir e-

posta ekini açmaya zorlamasıdır. Aciliyet hissi yaratmaya çalışan, imla hataları bulunan veya "Değerli müşterimiz" gibi genel hitaplar kullanan e-posta ya da çevrim içi mesajlara dikkat edin.

## Ölçümler

Bu durumda davranış ölçümleri yapmak zordur zira kişilerin evlerinde nasıl davranış davrandığını izlemek kolay değildir. Ayrıca, bu davranışlardan bazıları (Wi-Fi cihazlarını güvenceye almak gibi) yalnızca işle ilgili de değildir. Fakat yine de çalışanların angajmanı ölçülebilir. Kişisel veya duygusal unsurlar içeren konuların insanlara daha cazip geldiğini, ilgi ve dikkatlerini daha fazla çektiğini biliyoruz. Bu bakımdan, aşağıdaki ölçümleri kullanmanız faydalı olabilir.

- **Etkileşim**: İnsanlar, hazırladığınız güvenlik kanallarında veya forumlarda ne sıklıkla soru soruyor, fikirlerini paylaşıyor ya da yardım istiyor?
- **Simülasyon**: Kimlik avı, mesaj veya telefonla arayarak sosyal mühendislik simülasyonları yapın.

Ölçümlerin çok daha kapsamlı bir listesi için MGT433 Dijital İndirme Paketinden interaktif Güvenlik Farkındalığı Ölçümleri Matrisini indirebilirsiniz.

## Lisans



## Uygulama Seti Yazarı

Lance Spitzner siber tehdit araştırmaları ile güvenlik mimarisi, farkındalığı ve eğitimi konularında 20 yıllık güvenlik tecrübesine sahiptir. Kurdugu Honeynet Projesi ile, siber sahtekarlık ve siber istihbarat alanlarında büyük adımlar atılmasına destek olmuştur. SANS eğitmenlerinden biri olarak MGT433: Güvenlik Farkındalığı ve MGT521: Güvenlik Kültürü kurslarını geliştirmiştir. Lance, ayrıca üç güvenlik kitabı yazmış, 25 ülkede güvenlik danışmanlığı yapmış ve 350'den fazla kurumun, insan kaynaklı risklere yönelik güvenlik farkındalığı ve güvenlik kültürü programları kurmasına katkıda bulunmuştur. Lance, sık sık sunumlar yapmakta, @lspitzner adresinden tweet'ler atmakta ve farklı güvenlik projeleri üzerinde çalışmaktadır. Lance Spitzner, bilgi güvenliği kariyerinden önce ABD Kara Kuvvetleri Hızlı İntikal Kuvvetinde zırh subayı olarak hizmet vermiş ve yüksek lisans derecesini Illinois Üniversitesi'nden almıştır.

## SANS Institute Hakkında

SANS Institute, 1989 yılında müşterek bir araştırma ve eğitim kurumu olarak kurulmuştur. SANS, dünya çapında devletler ve ticari kurumlar için en güvenilen ve açık ara en büyük siber güvenlik eğitim ve sertifikasyon sağlayıcısıdır. Alanlarında tanınmış SANS eğitmenleri, 200'ün üzerinde canlı etkinlikte ve İnternet üzerinden 60'ın üzerinde kursla siber güvenlik eğitimi vermektedir. SANS Institute'un bağlı kuruluşlarından GIAC, çalışanların siber güvenlik alanındaki yeterliliklerini belgelemek üzere 35'in üzerinde pratik ve teknik sertifikasyon hizmeti sunmaktadır. Bölgesel olarak akredite edilmiş bağımsız bir alt kuruluş olan SANS Technology Institute, siber güvenlikte yüksek lisans eğitimi sağlamaktadır. SANS; konsensüs projeleri, araştırma raporları ve haber bültenleri de dahil olmak üzere InfoSec topluluğuna sayısız ücretsiz kaynak sunmakta ve ayrıca İnternet'in erken uyarı sistemi olan Internet Storm Center'ı işletmektedir. SANS'ın temelinde, şirketlerden üniversitelere farklı küresel kurumlardan gelen ve tüm bilgi güvenliği topluluğuna yardımcı olmak için birlikte çalışan birçok güvenlik uzmanı vardır. (https://www.sans.org)