

OUCH!

Sizin İçin Aylık Güvenlik Farkındalık Bülteni

Güvenli Şekilde Bir Sanal Konferansa Katılmak

Sanal Konferans Nedir?

Bugünlerde çoğumuz evden çalışıyoruz, büyük ihtimalle siz de Zoom, Slack ya da Microsoft Teams gibi sanal konferans çözümlerinden biriyle kendinizi iş arkadaşlarınızla çalışıyor bulacaksınız. Aile bireyleriniz, hatta belki çocuklarınız bile arkadaşlarıyla buluşmak ve uzaktan öğrenme için aynı teknolojiyi kullanıyor olabilir. Bağlanma nedeninizden bağımsız olarak, güvenli bir şekilde bu teknolojileri kullanmak için atmanız gereken temel adımları sizinle paylaşacağız.

Sanal Bir Konferansa Katılmak

Eğer sanal bir konferansa katılacaksınız, işte size 5 önemli adım.

1. **Yazılımınızı Güncelleyin:** Her zaman konferans yazılımının son ve güncel versiyonunu kullandığınızdan emin olun. Yazılımınız ne kadar yeni ve güncel ise o kadar güvenli olacaktır. Otomatik güncelleme ve sonrasında kapatma özelliği aktifleştirin. Böylece yazılımı yeniden başladığında en yeni güncellemeleri kontrol edebilecektir.
2. **Ses / Video Özelliklerini Ayarlayın:** Bir toplantıya katıldığınızda mikrofonunuzun sessiz ve kameranızın kapalı olacak şekilde tercihlerinizi ayarlayın. Ses ve videoyu sadece siz istediğiniz zaman aktifleştirin. Aktif olarak yayın yapmadığınız zamanlarda gizliliğinizi korumak için web kameranızın üzerini örtün ya da bant ile üzerini kapatın. Unutmayın, eğer kameranız açıksa, konuşmasanız bile herkes ne yaptığınızı görür.
3. **Arka planda ne olduğuna iki kez kontrol edin:** Eğer web kameranızı aktifleştirmek istiyorsanız, arka planda ne olduğuna dikkat edin. Bir konuşma sırasında arka planınızda kişisel ya da gizli bilginin görünür bir şekilde olmadığından emin olun. Bazı konferans yazılımları, diğer insanların arka planınızdakileri görmelerini engellemek için arka planınızı bulanıklaştırır ya da sanal bir arka plan kullanmanıza olanak verir.
4. **Davet Bağlantısını Paylaşmayın:** Davet bağlantısı, toplantıya katılmanız için size özel olarak oluşturulmuş bir bilettir. Güvenilir iş arkadaşlarınız bu bağlantıya ihtiyaç duysa bile, konferansı düzenleyen kişiden davet almaları daha iyi olacaktır.
5. **Kaydetmeyin:** İzin almadan ekran görüntüsü almayın ya da konferansı kaydetmeyin. Eğer ekran görüntüleri ya da video görüntüleri genele açık hale gelirse, yanlışlıkla gizli bilgileri paylaşmış olursunuz.

Sanal Bir Konferansa Ev Sahipliği Yapmak

Eğer bir konferansa ev sahipliği yapıyorsanız ya da organize ettiyseniz, atmanız gereken ek adımlar şunlardır.

1. **Parola Gerekliliği:** Konferansın güvenliği ve katılımcı kontrolü için toplantınızı bir parola ile koruyun. Böylece sadece parolayı bilenler konferansa katılabilirler.
2. **Katılımcıları Gözden Geçirin:** Konferans katılımcılarını gözden geçirin. Eğer tanımadığınız ya da tanımlayamadığınız bir katılımcı var ise, o kişinin kimliğini doğrulamasını isteyin. Eğer bir katılımcı kaba ya da rahatsız edici bir şekilde davranıyorsa, kişiyi konferanstan çıkartın. Bir çok çözüm, konferans başladıktan sonra siz istemediğiniz sürece yeni kişilerin katılmasına izin vermez. Bir diğer seçenek de katılımcıları bekleme odasına almak ve tek tek onaylayarak kimin katılacağına karar vermektir.
3. **Eğer Konferans Kayıt Edilecekse Bildirim Yapın:** Eğer etkinliği kaydetmek istiyorsanız (ve kayıt etme hakkınız varsa), başlangıçta tüm katılımcıları bu durumdan haberdar ettiğinizden emin olun.
4. **Ekran Paylaşımı:** Eğer herhangi bir zamanda ekranınızı paylaşacaksanız, öncelikle diğer tüm uygulamaları kapattığınızdan ve gizli dosyalarınızı masa üstünden kaldırdığınızdan emin olun. Ayrıca beliren ileti bildirimlerini kapatın. Bu, ekranınızı paylaşırken yanlışlıkla gizli ya da utandırıcı bilgileri paylaşmamanıza yardım eder. Bir diğer seçenek ise tüm ekran yerine sadece göstermek istediğiniz programın görüntüsünü paylaşmaktır.

Bu teknolojiler birçok bakımdan harika araçlardır ve gelecekte bizim nasıl çalışacağımızı, diğerleri ile iletişim kuracağımızı ve birlikte iş yapacağımızı gösterirler. Bu basit adımlar sizin güvenliğinizi sağlamada etkili olacaktır.

Konuk Editör

Lodrina Cherne, bugünün açık ve bağlı dünyasında kişileri ve bilgileri koruyan [Cybereason](#) şirketinde güvenlik baş avukatıdır. Ayrıca SANS enstitüsünde [Windows ile Adli Bilişim](#) dersini vermekte ve [ThisWeekin4n6](#) adlı web günlüğüne katkıda bulunmaktadır. Kendisini Twitter üzerinde [@hexplates](#) hesabından takip edebilirsiniz.



Kaynaklar

Parolalar: <https://www.sans.org/security-awareness-training/resources/making-passwords-simple>

Parola Yöneticileri: <https://www.sans.org/security-awareness-training/resources/password-managers-0>

Tarafından toplum için çevirisi yapılmıştır: Sema Yüce ve Selma Süloğlu

OUCH! SANS Security Awareness tarafından yayınlanır ve Creative Commons BY-NC-ND 4.0 lisansı ile dağıtılır. Satmadığınız veya değiştirmediniz sürece bu bülteni paylaşabilir veya dağıtabilirsiniz. Yayın Kurulu: Walter Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley