Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Çocukları Siber Güvenlik Konusunda Eğitmek

Arka Plan

Çocukların çevrimiçi ve diğerleri ile etkileşim yollarının sayısı bugün oldukça şaşırtıcı. Yeni sosyal medya uygulamaları sürekli çoğalıyor ve çevrimiçi bağlantıda olabilen uygulama ve oyunların sayısı giderek artıyor. Buna ek olarak birçok okul Google Drive gibi servisleri kullanarak, bazı ödevlerin veya hepsinin tamamlanması ve gönderilmesi sürecini çevrimiçi ortamlara taşıyor. Çocuklar tam anlamıyla "bağlı (connected)" olarak büyüyor. Bu durumun pek çok faydası olduğu gibi, riskleri de beraberinde getiriyor. Bu bültenimizde, çocuklar için risk oluşturan üç alanı ve onların güvenli kalmasına yardımcı olmak için neler yapabileceğimizi keşfedeceğiz.

Konuk Yazar

Verizon'da Veri Bilimcisi olarak görev yapan Bob Rudis, 2015 Veri İhlali Soruşturmaları Raporu'nun (Data Breach Investigations Report) yazarı ve dört harika çocuğun babasıdır. Bob birçok Fortune 100 şirketi için etkin güvenlik farkındalığı programları oluşturmuş ve yönetmiştir. Kendisini Twitter'da **@hrbrmstr** hesabından izleyebilirsiniz.

Riskler

1. **Davranış**: Çocuklar çevrimiçi topluluklar ya da sanal dünyalarda etkileşim yaparken, asla gerçek dünyada yapmayacakları biçimlerde davranabilir. Fiziksel varlığın olmayışı özellikle çocuklarda, güçlü bir anonimlik duygusu yaratabilir. Çocuklar bu durumda kendilerini, diğer çocuklara zarar verebilen ve siber zorbalık veya "griefing" adı verilen yollarla ifade etme eğilimi gösterir. Ek olarak, sizin çocuklarınız onlara zarar verebilecek başka çocukların kurbanı haline gelebilir.

2. **İletişim**: Çocuklar şimdi ya yazılı, ya çevrimiçi topluluklarla etkileşerek ya da sanal dünyalarda oynayarak, başkaları ile neredeyse sürekli iletişim halindeler. Fiziksel varlığın eksikliği genellikle diğer taraftakilerin, söyledikleri birey olmayabileceği gerçeğini unutmalarına yol açıyor. Kötü niyetli kişiler genellikle çocukların kendilerini kılığında, bu dijital sokaklarda dolaşmak ve potansiyel mağdurları ile ilişkiler kurmak için ellerinden gelen her taktiği kullanacaklar.

3. **İçerik**: Video, ses, görüntü veya metin tabanlı mesajları çevrimiçi ortamlarda kısa yoldan yakalamanın bir yolu yok. Çocuklar genelde, gerçekte yaratabileceği sonuçları farkında olmadan kendileri veya diğer aile bireyleri hakkında gerektiğinden çok daha fazla ve aşırı paylaşım yapma eğiliminde. Ayrıca çocuklar, ucu açık sorular sorarak veya bazı bağlantıları tıklamaları istenerek yapılabilecek kimlik hırsızlığı ya da kötü niyetli yazılım bulaştırılması gibi tehlikeleri de farketmeyebilir. Son olarak, çevrimiçi yayınlanan veya yapılan herhangi bir paylaşımın "geri al" seçeneğinin olmadığı bir çağda yaşıyoruz. Çocuklar Kik, Instagram, Snapchat ve diğer uygulamalardaki gönderilerinin geçici olduğunu düşünebilir ama bu gönderiler kendilerinin veya diğer aile üyelerinin daha sonraki hayatında karşılarına çıkabilir.

Çocukları Siber Güvenlik Konusunda Eğitmek

Çocukları Eğitmek

Çocukları korumak için yapabileceğiniz en önemli şey onlarla konuşmaktır. Çocuklarınızın çevrimiçi ne yaptığını bilin, bugünün riskleri ve kendilerini korumak için ne yapmaları gerektiği konusunda onları eğitin.

Çocukları siber dünyada korumanın anahtarı, karşılaşabilecekleri tehlikeler hakkında onları eğitmek ve sadece sizin onlarla konuştuğunuzdan değil, onların sizinle konuştuğundan emin olmaktır.

1. **Evde güvenlik**: Güvenli çevrimiçi davranışlar oldukça mobil olunmasına rağmen evde başlar. Siz onlarla ne kadar erken konuşmaya başlarsanız, ki bu onların da sizinle o kadar erken konuşmasına yol açar, en iyisidir. Çevrimiçi güvenlik sorunları hakkında onlarla düzenli konuşmalar ayarlayın, hatta gerçek hayatta yaşanmış ve olumsuz sonuçları olmuş olayları gösterecek kadar ileriye gidin. Eğer çocuğunuzun neler yaptığını bilmiyorsanız, sadece sorun. Cahil ebeveyn rolü oynayın, son teknolojilerin neler olduğunu ve onların bunları nasıl kullandığını göstermelerini isteyin. Çocuklar öğretmen olma fikrini sevecekler ve açılacaklardır. Örneğin, belki de, Instagram hesapları vardır, onlara Instagram'ın nasıl çalıştığını sorun, sizin için bir hesap açmalarını isteyin ve onları takip edin. Böylece sadece onların ne yaptığını öğrenmiş ve onları izlemiş olmayıp, böyle konuları sizinle konuşmalarını kolaylaştırmış olursunuz. Buna ek olarak, tüm çevrimiçi aktivitelerin evin merkezi bir yerinde iken yapıldığından ve kullanım için zaman sınırlamaları getirildiğinden emin olun. Bilgisayarları evin merkezi konumlarına yerleştirmek, çocukların tehlikeli davranışlar içine girmeleri olasılığını azaltır. Ayrıca çocukların yatağa gitmeden önce bütün mobil cihazlarını oraya götürülmesi kuralı ile birlikte, tüm mobil cihazlar için merkezi bir şarj istasyonu kurma fikrini düşünün.

2. **Başkaları ile güvenlik**: Çocuklar evden uzak olduğunda, daha çok risk altındadır. Onların nerede olurlarsa olsunlar siber kuralların geçerli olduğunu anlamalarına ve sizin kısıtlamalarınızla güvendikleri kişilerle iletişim kurmalarına yardımcı olun. Eğer mobil cihazları varsa, kullanım alışkanlıklarını (zaman ve bant genişliği) kontrol edin ve evinizin dışında, bir şekilde daha az kısıtlama ile karşılaştıkları zaman, bunun avantajını kullanıp kullanmadıklarının işaretlerini arayın. Tüm ihlalleri durdurmanız mümkün olmayacaktır, ama mobil cihazlarını kullanmaya başladıklarında sizin sevecen sözleriniz akıllarına gelecektir.

3. **Sayılarla Güvenlik**: Bu siber izleme işinde yalnız değilsiniz ve potansiyel bir zararlı davranışı farkedebilmek için mutlaka diğer veliler, görevliler, kardeşler, öğretmenler ve arkadaşlar ile işbirliği yapmalısınız. Tehlikeli bir yola girdiklerini farkettiğinizde çocuklarınız ve onların olumlu etkileşimler içinde bulunmalarını cesaretlendirmek için grubunuzu canlı tutmaya çalışın.

Son olarak, çocuklar hata yaptığında, hemen bir disiplin cezası ile karşılık vermek yerine, her birinden bir deneyim çıkarmaları için yardımcı olun. Her seferinde "neden" olduğunu anlatın ve sadece, göremedikleri tehlikelerden onları korumaya

çalıştığınızı hatırlatın. Çevrimiçi etkileşimlerinde herhangi bir rahatsızlık duyduklarında size gelebileceklerini hatta konuyla ilgili bir ekran görüntüsü bile paylaşacabileceklerini bilmelerini sağlayın. Aynı zamanda, uygun olmayan bir davranışlarında bile size anlatmak konusunda rahat olmalarını sağladığınızdan emin olun. Gerçek dünya iletişimini sürekli açık ve aktif tutmak, çocukları bugünün dijital dünyasında güvenli tutmanun en iyi yoludur.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Mustafa Emrah Ünsür, Güvenlik Araştırmacısı olarak araştırmaları, makaleleri ve çevirileri vardır. Beyaz Şapkalı Hacker olarak kendisi tarafından kodlanan ve kodlanmakta olan 'exploit'ler ve 'tool'lar bulunmaktadır. Ayrıca, Sızma Testi Uzmanı olarak özel şirketlere ve devlet kurumlarına Zafiyet ve Sızma Testi yapmış ve yapmaya devam etmektedir.

Kaynaklar

Siber Zeka: http://www.cybersmart.gov.au/Parents.aspx

OnGuard Online: http://www.onguardonline.gov/topics/protect-kids-online

Çevrimiçi Güvenle Kalmak (StaySafeOnline):
https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens

Çocukları Koruma Paneli:
http://www.rsaconference.com/media/into-the-woods-protecting-our-youth-from-the-wolves-of-cyberspace

Çocuklar için Güvenli Internet: http://www.bilgimikoruyorum.org.tr/?b425_cocuklar-icin-guvenli-internet

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

