İnternet Etiği Nedir?

İnternet etiği, internet kullanımı sırasında kabul edilebilir davranışların ne olduğu konusunda bireyi veya grubu yöneten ahlaki ilkelere denir.

İnternet Etiği Nedir?

İnternet etiği, internet kullanımı sırasında kabul edilebilir davranışların ne olduğu konusunda bireyi veya grubu yöneten ahlaki ilkelere denir.

İnternet Etiğinin Boyutlar Nelerdir?

İnternet etiği, bireysel ve sosyal ilkelere dayanmakla birlikte küresel seviye geçerliliğini sürdürmektedir.

İnternet etiği içinde yer alan konulardan bazıları nelerdir?

Sosyal medya
Sosyal medyanın insan ilişkilerinin oluşmasında aldığı rol
Mahremiyet
Tarafsızlık
İnternete erişim sorunları
Büyük veri ekosisteminin gelişimi
Verilerin kontrolü

İnternet Etiği İlkeleri Nelerdir? Neleri İçerir?

İnternet etiği ilkeleri toplumdaki tüm etik kuralları ile aynı özelliklere sahiptir. Bireyin günlük sosyal yaşantısında önem verdiği ve uyguladığı ilkeler internet için de geçerliliğini sürdürmektedir. İnternet etiği ilkeleri birbirleri ile ilişkilidir ve bağlantılıdır.

Etik ilkelerinin en başında adalet ve eşitlik ilkesi gelmektedir. Her bireyin devredilemez bir onuru vardır ve eşit haklara sahiptir. Bireylerin birbirlerine olan derin saygısı adaleti geliştirir. Bilgiye adil ve eşit erişim, toplumdaki bireylerin birbirlerini anlamalarına olanak sağlar.

Özgürlük, eşitlik ve sorumluluklar yaşam içinde birbirini dengeleyecek şekilde gelişim göstermelidir. İnternet etiği konusunda özgürlük, istenilen bilgiye erişme, ifade ve inanç özgürlüğünü ifade etmektedir.

İnternet etiği ilkelerinden empati ve saygı önemli bir başka ilkeyi oluşturmaktadır. Kurulan diyaloglarda empati yapılmalı, karşıdaki bireyin konumu ve sosyal statüsü düşünülerek iletişime geçilmelidir. Konuşmalar, saygı çerçevesinde yapılan konuşmalar dayanışma ve karşılıklı desteğe yol açmaktadır.

İnternet etiği içerisinde önemli yere sahip olan bir başka ilke, katılım ve paylaşma ilkeleridir. Toplumsal hayata ve önemli karar alma süreçlerine katılma hakkı ve yeteneği temel değerlerdir. Bilgi ve bilginin internet ortamında paylaşılması insanlar arasında sürdürülebilir ilişkiler kurulmasını sağlar ve sonuç olarak toplumları güçlendirir.

İnternet etiğinin önemli ve son ilkeleri sorumluluk ve sürdürülebilirliktir. Kişinin kendi eylemlerinin sorumluluğunu üstlenmesi, sosyal bir ortamda temel bir gerekliliktir. Sorumluluk seviyesi, bireyin gücünün, kapasitesinin ve kabiliyetinin seviyelerine uygun olmalıdır. Uzun vadede, sorumluluğun getirdiği durumları sürdürebilmek de önemlidir. Sürdürülebilir projeler tüm insanlar açısından önemlidir.

İnternet Etiği'nde Telif Hakkı ve Korsanlık

İnternet etiğinde önemli bir başlık da telif hakkı ve korsanlık sorunlarıdır. Telif hakkının temel amacı, bir sanatçıya, yazara veya fikri mülkiyetin yaratıcısına hak ettiği ödülü vermektir. Aynı zamanda telif hakkı ile yaratıcılık teşvik edilir. Bu amaçla, telif hakkı, yazarların orijinal ifadelerini kullanma hakkını güvence altına almakla birlikte başkalarını da fikirlerini özgürce geliştirme konusunda teşvik eder. Buradaki etik sorun yasadışı kopyalama konusudur. İnsanlar istedikleri zaman dijital kopyalar üretebilirler ve bu kopyalar internet üzerindeki herkes tarafından kullanılabilir. İnternet üzerinde kontrolsüz şekilde gelişen müzik, film, blog vb. siteler bu duruma en uygun örnektir. Kaynak gösterilmeden materyal kullanılması yazılı çalışmalara uygulandığında intihal oluşturur. Bu durumun aynısı standart internet üzerindeki belgeler ve web siteleri için de geçerlidir. İnternet ortamında gezenler tarafından indirilmek istenen eserlerin telif haklarının gasp edilerek fikri mülkiyet haklarının ihlal edilmesinde dosya paylaşım siteleri ve uygulamaları araç olarak kullanılabilir. Yasadışı telif hakkıyla korunan materyalleri indirmek hırsızlıktan farklı olmasa da, internetteki sanatçıların kreasyonlarına kolay erişim, normalde hiçbir zaman fiziksel bir kopyasını bir mağazadan çalmayı düşünmeyen internet kullanıcılarını cesaretlendirebilir.

İnternet Etiği'nde Gizlilik

İnternet etiği ile ilgili önemli etik sorunlardan biri online mahremiyettir. Bir bireyin bilgisayarı, veriyi ve bilgiyi depolamak için en güvenli yeridir. Ancak etik olmayan bireyler ağ güvenliğini ihlal etmek ve kişisel verilere erişmek için çeşitli yollar kullanır. Hackleme yalnızca büyük bir gizlilik ihlalini temsil etmekle kalmaz, aynı zamanda bilgisine erişilenlere kişisel ve finansal olarak zarar verebilir.

İnternetin kullanım boyutunun artmasıyla internet kullanan birey sayısı da artmaktadır. Bu da internete giren her bireyin çeşitli şekillerde kimlik bilgilerini internet üzerinden paylaşması anlamına gelir. Burada internet etiği yönünden sorun, bu kimlik bilgilerinin bireylerin istemediği ve farkına varmadığı şekilde toplanması ve kullanılmasıdır.

Online işletmeler rutin olarak müşterilerinden kişisel ve finansal bilgiler toplar ve birçoğu müşterilerinin gizlilik ve güvenlik gereksinimlerine saygı gösterir. Bununla birlikte, etik dışı çalışan şirketler müşterileriyle iletişim kurma, tüccarlara duydukları güveni kötüye kullanma konusunda müşterilerin iletişim bilgileri, gelirleri ve üçüncü taraflarla harcamaları hakkında bilgileri paylaşabilir.

İnternet, genel anlamda kurumlar veya hükümetler tarafından gözetim altıda tutulmaktadır. Tabi ki bu gözetimin boyutu tartışmalıdır. Bu boyutun artması yaratıcılık ve ifade özgürlüğü sınırlarının daralmasına neden olabilir. Fakat tersi bir durumda da internet üzerinde bazı kontrol dışı durumlar ortaya çıkabilir.

Sosyal Ağlar

Facebook, Google, Twitter ve benzer online sosyal ağların yalnızca geniş kapsamlı ekonomik değil aynı zamanda online dünya üzerinde sosyal ve kültürel etkileri de vardır. Son birkaç yıl içinde üyelerde ve kullanıcılarda büyük bir artış yaşadıktan sonra, online sosyal ağlar artık internet etiği ilkelerine uyumun bir sorun olduğunu kabul etmiştir. İnternet etiği ilkelerine uygun hareket etmek, sosyal ağların itibarını arttırır ve bu da kullanıcıların güvenini kazanmalarına yardımcı olur. Bu durum ayrıca servis sağlayıcıları potansiyel müşteriler için daha cazip hale getirir. Fazla sayıda müşteri kazanmak ve elde tutmak ağların reklam gelirlerini de arttırır. Bu nedenle, sosyal ağlar son dönemde izledikleri etik standartları ve kurumsal sosyal sorumluluk ilkelerini giderek daha fazla ilan etmektedir. Sohbet odaları veya

diğer sosyal ortamlardaki kişilerle iletişim kurulurken, bir ortamda yüz yüze iletişim halindeymiş gibi davranılmalıdır. Bir tartışma ve anlaşmazlık içinde olunsa bile, daima saygılı olunmalıdır. Yeni olduğunuz bir sosyal ağda sitenin davranış standartlarını öğrendiğinizden ve hiç bir ihlal yaşamayacağınızdan emin olmak için site kurallarını okumayı unutmayın.

En iyi 15 internet güvenliği kuralı ve çevrimiçi ortamlarda yapılmaması gerekenler

İşten eğitime ve hatta arkadaşlarımızla konuşmaya kadar günlük hayatımızın büyük bir kısmı internet etrafında dönüyor. 2021 yılında yapılan bir anket, ABD'deki ortalama bir hanenin internete bağlı yaklaşık 25 cihaza sahip olduğunu ortaya koydu. 2019'da bu sayı 11'di. Ne kadar çok çevrimiçi hesabınız ve cihazınız varsa, siber suçluların size zarar verme kapsamı o kadar fazladır. Bu nedenle, sizi ve ailenizi verilerinize ve cihazlarınıza zarar verebilecek tehditlerden koruyan internet güvenliği kurallarını anlamak artık çok daha önemlidir. Önemli internet tehlikeleri ve çevrimiçi ortamlarda güvende kalmanın yolları hakkında bilgi edinmek için okumaya devam edin.

İnternetin Başlıca Tehlikeleri

Ailenizle birlikte interneti kullandığınızda (çoğu zaman bunun farkında olmadan) kendinizi bir dizi olası çevrimiçi tehdide maruz bırakırsınız. Siber suçlular internet kullanıcılarını hedef almak için yeni yollar geliştirdikçe bildiğimiz dijital ortamlar sürekli olarak evrim geçiriyor. Sizin ve ailenizin dikkat etmesi gereken en büyük internet tehlikelerinden bazıları şunlardır:

- Kimlik hırsızlığı.
- Veri ihlalleri.
- Zararlı yazılımlar ve virüsler.
- Kimlik avı ve dolandırıcılık e-postaları.
- Sahte web siteleri.
- Çevrimiçi dolandırıcılıklar.
- Aşk dolandırıcılıkları.
- Uygunsuz içerik.
- Siber zorbalık.
- Hatalı gizlilik ayarları.

Temel İnternet Güvenliği İpuçları

Tüm bu tehlikelerden kaçınmak için, siz veya aileniz çevrimiçi olduğunuzda temel internet güvenliği ipuçlarımızı uygulamanızı öneririz:

1. Güvenli bir internet bağlantısı kullandığınızdan emin olun

Herkese açık Wi-Fi kullanımı tavsiye edilmese de dışarıdayken bu bazen kaçınılmaz bir durum olabilir. Ancak herkese açık bir yerde çevrimiçi olduğunuzda ve herkese açık bir Wi-Fi bağlantısı kullandığınızda güvenliği üzerinde doğrudan bir kontrolünüz yoktur ve bu da sizi siber saldırılara karşı savunmasız bırakabilir. Yani herkese açık Wi-Fi kullanıyorsanız çevrimiçi bankacılık veya çevrimiçi alışveriş gibi kişisel işlemler yapmaktan kaçının.
Bunlardan herhangi birini yapmanız gerekiyorsa Sanal Özel Ağ veya VPN kullanın. VPN, güvenli olmayan bir ağ üzerinden gönderdiğiniz tüm verileri gerçek zamanlı şifreleme yoluyla korur. VPN kullanmıyorsanız güvenilir bir internet bağlantısı kullanana kadar tüm kişisel işlemlerinizi kaydetmenizi öneririz. VPN'in ne olduğu hakkında daha fazla bilgiyi burada bulabilirsiniz.

2. Güçlü parolalar seçin

Şifreler siber güvenlik söz konusu olduğunda en büyük zayıf noktalardan biridir. İnsanlar genellikle hatırlaması kolay ve bu nedenle bilgisayar korsanlarının korsanlık yazılımlarıyla kırması kolay olan parolalar seçerler. Buna ek olarak, aynı parolayı birden fazla site için kullanmak verilerinizi daha fazla risk altına sokar. Bilgisayar korsanları kimlik bilgilerinizi bir siteden ele geçirirlerse aynı giriş bilgilerini kullanan diğer web sitelerine de erişebilirler.

Siber suçlular için gizliliği ortadan kaldırması daha zor olan güçlü parolalar seçin. Güçlü bir parola:

- Uzundur: En az 12 karakterden (ideal olarak daha fazlasından) oluşur.
- Karakterlerin bir karışımıdır: büyük ve küçük harfler, semboller ve sayılar.
- Bariz bilgiler içermez: sıralı numaralar ("1234") veya sizi tanıyan birinin tahmin edebileceği (veya çevrimiçi ortamlarda bulunabilecek) doğum tarihiniz veya evcil hayvanınızın adı gibi kişisel bilgiler kullanmak gibi.
- Kolay tahmin edilebilir tuş dizilerinden oluşmaz.

Parola yöneticisi kullanmak yardımcı olabilir. Parola yöneticileri, kullanıcıların güçlü parolalar oluşturmasına, bunları dijital bir kasada saklamasına (tek bir ana parola ile korunur) ve çevrimiçi hesaplara giriş yaparken bunları geri almasına yardımcı olur.

3. Mümkün olan yerlerde çok faktörlü kimlik doğrulamayı etkinleştirin

Çok faktörlü kimlik doğrulama (MFA), kullanıcılardan bir çevrimiçi hesaba erişmek için iki veya daha fazla doğrulama yöntemini kullanmalarını gerektiren bir kimlik doğrulama yöntemidir. Yalnızca bir kullanıcı adı veya parola istemek yerine, aşağıdaki gibi ek bilgiler isteyerek güvenlik seviyesini daha da ileriye taşır:

- Web sitesinin kimlik doğrulama sunucularının kullanıcının telefonuna veya e-posta adresine gönderdiği tek seferlik ek bir parola.
- Kişisel güvenlik sorularının yanıtları.
- Parmak izi veya ses veya yüz tanıma gibi diğer biyometrik bilgiler.

Çok faktörlü kimlik doğrulama, bir siber saldırının başarılı olma olasılığını azaltır. Çevrimiçi hesaplarınızı daha güvenli hale getirmek için, mümkün olduğunca çok faktörlü kimlik doğrulaması uygulamak iyi bir uygulamadır. İnternet güvenliğinize yardımcı olmak için Google Authenticator veya Authy gibi üçüncü taraf bir kimlik doğrulayıcı uygulaması kullanmayı da düşünebilirsiniz.

4. Yazılımlarınızı ve işletim sistemlerinizi güncel tutun

Geliştiriciler, ürünleri güvenli hâle getirmek için sürekli çalışıyor, en son tehditleri izliyor ve yazılımlarında güvenlik açıkları olması durumunda güvenlik yamalarını kullanıma sunuyor. İşletim sistemlerinizin ve uygulamalarınızın en son sürümlerini kullanarak en son güvenlik yamalarından yararlanabilirsiniz. Bu, özellikle bir kullanıcı hakkında ödeme, sağlık veya diğer hassas bilgileri içeren uygulamalar için önemlidir.

5. Web sitelerinin güvenilir görünüp görünmediğini kontrol edin

Ziyaret ettiğiniz herhangi bir web sitesi için, özellikle (e-ticaret siteleri gibi) işlem yaptığınız web siteleri için güvenilir olmaları çok önemlidir. Dikkat edilmesi gereken önemli bir unsur SSL/güvenlik sertifikasıdır. Bu, "HTTP" yerine "HTTPS" ile başlayan ("S", "secure" yani "güvenli" anlamını ifade eder) ve adres çubuğunda asma kilit simgesi olan URL'lere dikkat edin anlamına gelir. Diğer güven sinyalleri şunlardır:

- Yazım ve dilbilgisi hatalarından arındırılmış metin – saygın markalar, web sitelerinin iyi yazılmasını ve düzeltilmesini sağlamak için çaba gösterecektir.
- Pikselli olmayan ve ekranın genişliğine doğru şekilde uyan görüntüler.
- Organik hissettiren ve çok güçlü olmayan reklamlar.
- Renk veya temada ani değişiklikler olmaması. Kullanıcıların belirli bir web sitesiyle etkileşime geçtiği ve bir bağlantıdan tanıdık bir sayfaya döndüğü bazı durumlarda, kurnazca yapılan renk veya tasarım değişiklikleri sahteciliğe işaret edebilir.
- Çevrimiçi ödemelerin kabul edilen standartları: Meşru e-ticaret web siteleri, yalnızca kredi veya banka kartı portallarını ya da PayPal'ı kullanır. Bir web sitesi ödemeleri kabul etmek için başka bir dijital para transferi biçimi kullanıyorsa muhtemelen dolandırıcı bir web sitesidir.

6. Gizlilik ayarlarınızı gözden geçirin ve gizlilik ilkelerini anlayın

Pazarlamacılar sizinle ilgili her şeyi bilmek ister. Korsanlar da öyle... İkisi de göz atma geçmişinizden ve sosyal medya kullanımınızdan çok şey öğrenir. Ancak üçüncü tarafların ne kadar bilgiye erişebileceğini siz belirleyebilirsiniz. Hem web tarayıcıları hem de mobil işletim sistemleri, gizliliğinizi çevrimiçi olarak korumak için ayarlara sahiptir. Facebook, Twitter, Instagram, LinkedIn ve bunlara benzer sosyal medya siteleri, etkinleştirebileceğiniz gizlilik artırıcı ayarlara sahiptir. Yönetim kurulundaki gizlilik ayarlarınızı gözden geçirmek ve bu ayarların sizin için uygun bir seviyeye ayarlandığından emin olmak için biraz zaman ayırmanızda fayda var.

Çoğumuz gizlilik ilkelerini okumadan kabul ederiz ancak pazarlama ve reklam (ve bilgisayar korsanlığı) amacıyla kullanılan bu kadar çok veriyle, verilerinizin nasıl toplandığını ve kullanıldığını anlamak için kullandığınız web sitelerinin ve uygulamaların gizlilik ilkelerini gözden geçirmek iyi bir fikirdir. Ancak ayarlarınız özel olarak ayarlanmış olsa bile çevrimiçi ortamlarda çok az verinin tamamen özel olduğunu unutmayın. Korsanlar, web sitesi yöneticileri ve emniyet teşkilatı, özel olduğunu düşündüğünüz bilgilere erişmeye devam edebilir.

7. Şüpheli bağlantılara ve tıkladığınız yerlere dikkat edin

Dikkatsiz bir tıklama, kişisel verilerinizi çevrimiçi olarak açığa çıkarabilir veya cihazınıza zararlı yazılımlar bulaştırabilir. Bu nedenle, güvenilmeyen kaynaklardan gelen bağlantılar ve istenmeyen e-postalar, çevrimiçi testler, tıklama yemi, "ücretsiz" teklifler veya istenmeyen reklamlar gibi belirli çevrimiçi içerik türlerinden bilinçli olarak göz atmak ve kaçınmak önemlidir.
Emin olmadığınız bir e-posta alırsanız içindeki bağlantılara tıklamaktan veya ekleri açmaktan kaçının.

Aslında, güvenilmeyen e - postaları açmaktan kaçınmak en iyisidir. Bir e - postanın yasal olup olmadığından emin değilseniz doğrudan kaynağa gidin. Örneğin, "bankanızdan" şüpheli bir e-posta alırsanız bankanızı arayın ve e-postanın gerçek olup olmadığını sorun.

Bir web sitesine girdiğinizde tıklanan bağlantıların ilgili veya beklenen konulara yönlendirdiğinden emin olun. Örneğin, Afrika'daki safarilerle ilgili olduğunu düşündüğünüz bir bağlantıya tıklarsanız ancak bunun yerine ünlülerin kilo vermesiyle ilgili tıklama tuzağı tarzı bir sayfaya veya "Şimdi ne yapıyorlar?" tarzı bir yazıya yönlendirilirseniz sayfayı hemen kapatın.

8. Cihazlarınızın güvende olduğundan emin olun

İnsanların %60'ının alışveriş yapmak ve çevrimiçi bilgi bulmak için masaüstü yerine mobil cihazları kullandığı düşünüldüğünde bu cihazların doğru şekilde güvenliğinin sağlanması önemlidir. Tüm cihazlarınızda – telefonlar, bilgisayarlar, tabletler, akıllı saatler, akıllı TV'ler vb. – parola veya parola ve parmak izi okuyucular veya yüz tarama teknolojisi gibi diğer güvenlik seçeneklerini kullanmak iyi bir uygulamadır. Bu önlemler, bir siber saldırı veya kişisel verilerinizin bilgisayar korsanları tarafından çalınması olasılığını azaltacaktır.

9. Verilerinizi düzenli olarak yedekleyin

Önemli kişisel bilgileri haricî sabit disklere yedeklemek ve düzenli olarak yeni yedeklemeler oluşturmak önemlidir. Bir tür zararlı yazılım olan Fidye Yazılımı, siber suçluların bilgisayarınızı kilitleyerek değerli dosyalarınıza erişememenize sebep olur. Verilerinizi – ve ailenizin verilerini – yedeklemek, bir fidye yazılımı saldırısının etkisini azaltmaya yardımcı olur. Uygun güvenlik yazılımları ile kendinizi daha fazla koruyabilirsiniz. Diğer zararlı yazılım türleri sisteminizi ele geçirerek veya sadece dosyaları silerek kişisel verilerinize erişiminizi engeller, bu nedenle dikkatli olun.

10. Kullanmadığınız hesapları kapatın

Yıllar geçtikçe, çoğumuz artık kullanmadığımız eski hesapları biriktiririz. Bunlar, interneti kullanırken güvenlik zincirindeki bir zayıf halka olabilir; eski hesapların daha zayıf parolalara sahip olma olasılığının olmasının yanı sıra bu sitelerin bazılarında zayıf veri koruma ilkeleri olabilir. Buna ek olarak siber suçlular, daha sonra ele geçirmek amacıyla kimliğinizin bir resmini oluşturmak için, örneğin doğum tarihiniz veya konumunuz gibi eski sosyal medya profillerinde bıraktığınız bilgileri bir araya getirebilir. Sonuç olarak, eski çevrimiçi hesaplarınızı kapatmanızı ve verilerinizin ilgili üçüncü taraf sunuculardan silinmesini talep etmenizi öneririz.

11. Neyi indirdiğinize dikkat edin

Siber suçluların en önemli hedeflerinden biri, makinenize bir "arka kapı" açmak için kullanılabilecek zararlı yazılımları indirmeniz için sizi kandırmaktır. Zararlı yazılımlar, popüler bir oyundan trafiği veya hava durumunu kontrol eden bir şeye kadar herhangi bir uygulama olarak gizlenmiş olabilir. Ayrıca cihazınıza zararlı yazılımlar yüklemeye çalışan zararlı bir web sitesinde de gizlenmiş olabilir.

Zararlı yazılımlar, cihazınızın çalışma şeklini bozmak, kişisel verilerinizi çalmak veya makinenize yetkisiz erişime izin vermek gibi hasarlara neden olur. Bu, genellikle sizin tarafınızdan bazı eylemler gerektirir ancak bir web sitesinin önce izin istemeden bilgisayarınıza yazılım yüklemeye çalıştığı istemsiz indirmeler de vardır. Yeni bir web sitesini ziyaret etmeden veya cihazınıza herhangi bir şey indirmeden önce dikkatlice düşünün ve yalnızca güvenilir veya resmî kaynaklardan içerik indirin. İndirme klasörlerinizi düzenli olarak kontrol edin ve sisteminizde bilinmeyen dosyalar görünürse (potansiyel olarak bir istemsiz indirmeden) bunları hemen silin.

12. Nerede ne paylaştığınıza dikkat edin

İnternette sil tuşu yoktur. Çevrimiçi olarak yayınladığınız herhangi bir yorum veya resim sonsuza kadar çevrimiçi kalabilir çünkü orijinali kaldırmak diğer kişilerin yapmış olabileceği kopyaları kaldırmaz. Yapmamış olmayı dilediğiniz bir yorumu 'geri almanız' veya yayınladığınız utanç verici bir resmi kaldırmanızın hiçbir yolu yoktur. Dolayısıyla bir ebeveynin veya potansiyel işverenin görmesini istemeyeceğiniz hiçbir şeyi internete koymayın.

Benzer şekilde, çevrimiçi ortamda kendinizle ilgili kişisel bilgileri ifşa ederken de dikkatli olun. Örneğin, sosyal medya biyografilerinde sosyal güvenlik numaranızı, adresinizi veya doğum tarihinizi ifşa etmekten kaçının. Kişisel bilgileri yabancılara bireysel olarak vermezsiniz, bu nedenle çevrimiçi olarak milyonlarca insana vermeyin.

E - posta adresinizi nerede görüntülediğinize veya gönderdiğinize dikkat edin. Yalnızca e-posta kayıt ve abonelikleri için kullandığınız, arkadaşlarınız ve aileniz için kullandığınızdan ayrı ve iş için kullandığınızdan ayrı ikincil ve önemsiz bir e-posta hesabınızın olması iyidir.

13. İnternette tanıştığınız kişilere dikkat edin

İnternette tanıştığınız kişiler her zaman söyledikleri kişiler değildir. Hatta gerçek bile olmayabilirler. Sahte sosyal medya profilleri, bilgisayar korsanlarının dikkatsiz internet kullanıcılarını tımar etmelerinin ve siber ceplerini seçmelerinin popüler bir yoludur. Çevrimiçi sosyal yaşamınızda da, yüz yüze sosyal yaşamınız için uyguladığınız aynı dikkati uygulayın. Bu, özellikle son yıllarda çevrimiçi flört dolandırıcılıklarının artması nedeniyle geçerlidir.

14. Çevrimiçi bilgileri iki kez kontrol edin

Ne yazık ki sahte haberler, yanlış bilgiler ve dezenformasyon internet ortamında karşılaşılan durumlardır. Her gün maruz kaldığımız bilgi seliyle kaybolmuş hissetmek kolay. Emin olmadığınız bir şey okursanız, gerçekleri belirlemek için kendi araştırmanızı yapın. Güvenilir web siteleri, orijinal bilgi kaynağı ve kaynak materyaller ile ilgili referanslara sahip olur. Şüpheli sayfalar hiçbir referans sunmaz. Sahte haberleri tespit etme kılavuzumuzu buradan okuyun.

15. İyi bir anti virüs kullanın ve programınızı güncel tutun

Çevrimiçi davranışlara yönelik güvenlik ipuçlarını uygulamanın yanı sıra kaliteli bir anti virüs sağlayıcısı kullanmak önemlidir. İnternet güvenlik yazılımları cihazlarınızı ve verilerinizi korurken virüsler ve zararlı yazılımlar gibi yaygın tehditleri (ayrıca casus uygulamalar, şifreli kilitleyiciler ve XSS saldırıları gibi karmaşık tehditleri) engeller. Tüm işletim sistemleri ve uygulamalarda olduğu gibi, en son siber tehditler karşısında bir adım önde olmak için anti virüs programınızı güncel tutmak önemlidir.

Çocuklar için 3 çevrimiçi güvenlik kuralı

Çevrimiçi ortamda güvende kalmaya yönelik ipuçlarının çoğu yetişkinler ve çocuklar için aynı olsa da, bunları açıklamak kolay veya anlaşılır değildir. Çocuklar, çoğu zaman yanlışlıkla kötü niyetli aktörlerin dijital sistemlerinize erişim sağlaması için kullandıkları bir geçit olabilir. Bu nedenle, ev ağınızı istenmeyen kazalardan korumak için çocuklarınıza çevrimiçi ortamda güvende kalmanın temellerini öğretmeniz önemlidir. Dikkat etmeniz gereken 3 alan:

Dijital Ayak İzi

Dijital ayak iziniz, yani kullanımdan sonra çevrimiçi ortamda size dair var olan şeyler, çocukların bilmesi gereken önemli bir kavramdır. Çocuklara bu konuda eğitim verirken bilgilerin nasıl kolayca erişilebilir olduğuna ve başkalarının bu verilerle (örneğin, suç faaliyeti için kullanılabilecek kimlik bilgileri içeren e-posta adresleri ve kullanıcı adları) nasıl etkileşime girebileceğine odaklanmak önemlidir. Çevrimiçi içerik paylaşımı (sosyal medya, oyun hesapları ve e-postalar aracılığıyla) gibi daha geniş tartışmalar da bundan kaynaklanabilir. İnternette hangi içeriklere izin verilmediğini açıkça belirttiğinizden emin olun (fotoğraflar, adres, telefon numaraları ve ikinci isimler).

Parolalar

Güçlü parolalar, günümüzde modern siber güvenlik önlemlerinin ayrılmaz bir parçasıdır. Çocuklara küçük yaşlardan itibaren güçlü parolaların (en az 12 karakterden oluşan ve harf, rakam ve sembollerin karışımı olan) ve bunların uygun şekilde saklanmasının önemi hakkında bilgi vermek, interneti aileniz için daha güvenli hâle getirmenin en basit yollarından biridir. Bu nedenle, farklı web siteleri için parola kimlik bilgilerini otomatik olarak doldurabilen bir parola yönetim sistemine sahip olmak çok yararlı olabilir.

İletişim

Her türlü siber suçlunun en çok eriştiği yollardan biri olan çevrimiçi mesajlaşma ve iletişim, çocuklarınızın güvenliği için onları uyarmanız gereken “olmazsa olmaz” bir alandır. Öncelikle, yabancılardan gelen ve çevrimiçi ortamda kimlik bilgilerini isteyen mesajların, şüpheli bağlantıların, indirmelerin veya e-postaların nasıl tespit edileceğini ve bunlardan nasıl kaçınılacağını açıklamak önemlidir. Bu, aynı zamanda kimlik avı dolandırıcılığı ve sahte web sitelerinin nasıl tespit edileceği konusunda daha geniş bir tartışmaya yol açabilir. Güvenli çevrimiçi iletişimin ikinci en önemli parçası, başkalarıyla doğru etkileşim kurmaktır. Gerçek dünyada olduğu gibi, güvende kalmak bazen uyanık kalmaya, kibar bir iletişim kurmaya ve zorbalığı nasıl tespit edeceğinizi ve zorbalıkla nasıl başa çıkacağınızı öğrenmeye bağlı olabilir. Çocuğunuzu siber zorbalığın neye benzediği ve çevrimiçi ortamda başkalarına karşı nasıl nazik davranılacağı konusunda eğitin.