e-Güvenlik (e-Safety) POLİTİKASI

MERSİN ZEYNEP TOROĞLU ÇAMLIBEL LİONS ANAOKULU

e-Güvenlik (e-Safety) POLİTİKASI

ve

AMAÇLARI

Milli eğitim bakanlığı destek hizmetleri genel müdürlüğünün 2018/10 nolu "Okullarda Güvenlik Önlemleri Alınması" konulu genelge doğrultusunda MERSİN ZEYNEP TOROĞLU ÇAMLBEL LİONS ANAOKULU olarak; güvenlik politikası dosyası hazırlandı. Okulda can güvenliği, internet güvenliği, kişisel güvenlik temaları baz alınarak okul politikası belirlendi. Okul güvenlik politikası, 2024/2028 stratejik planın gereği olarak değerlendirilip gerekli tüm e-güvenlik tedbirleri alınır.

Teknolojinin hızla gelişmesiyle birlikte her okulun Okul Güvenlik Politikasının olması kaçınılmaz olmuştur. Çünkü paydaşlar günümüzde okul binasından çok çeşitli şekillerde internete erişebilirler. Günlük hayatımızın bir parçası olarak hepimiz dijital teknolojilerle yaşıyoruz. Çocuklarımızın dijital teknolojiler aracılığıyla mevcut olan fırsatları en iyi nasıl kullanacaklarını bilmelerini sağlamak için, artık bunları nasıl kullanacaklarını bilmek ve anlamak gerekiyor. Bunun mümkün olan en güvenli şekilde ve en güvenli ortamda yapılmasını sağlamak için, öğrencilerimizin evde, okulda veya dışarıda ya da arkadaşlarıyla ya da yalnız olduğu zaman, dikkatini çeken açık ve özlü bir Güvenli İnternet Okul Politikasına sahip bir okuluz.

A. ÖZETLE E-GÜVENLİK (E-SAFETY) POLİTİKAMIZ:

1. Okulumuzun internet sitesi, facebook gibi sosyal ağları bulunmaktadır. Bu ağların üzerinde yayınlanan veriler kontrollü olarak paylaşılmaktadır.

2. Okulumuzda cep telefonları ders esnasında kapalı konumda tutulmakta, eTwinning projesi yapan arkadaşlar proje çalışmaları amacıyla gerektiği takdirde kullanmaktadır.

3. Öğretmenlerimiz tarafından, sınıflara düzenli olarak, BİT bağımlılığı, BİT'nin doğru ve güvenli kullanımı, Siber Zorbalık gibi konularda seminerler tertiplenmektedir. Bu konu ile ilgili sertifikası olan öğretmenlerimiz vardır.

4. Okulumuzda BİT doğru ve güvenli kullanımı ile ilgili sabit panolar bulunmaktadır.

5. Okulumuzun bazı öğretmenleri Milli Eğitim Bakanlığı tarafından verilen Siber Zorbalık, BİT 'in doğru ve güvenli kullanımı konularında uzaktan ve yüz yüze eğitimler almıştır.

6. Okulumuzda "Daha Güvenli İnternet Günü" kutlanmaktadır.

7. Okulumuzun internet sitesinde e-güvenlik konusunda, güvenliweb.org.tr. sitesi linki yer almaktadır. Okul paydaşlarımız istedikleri zaman konu ile ilgili bilgi alabilmekteler.

8. Okulumuzda güvenli internet günü kutlamalarında, konu ile ilgili seminerlerde güvenliweb.org.tr. sitesinden alıntılanan bilgi broşürleri dağıtılmaktadır.

9. Sınıf Öğretmenlerimiz internet etiği ve güvenli internet kullanımı konuları hakkında öğrencilerimize bilgilerini aktarmaktadır.

10. Okulumuzda 21.yy iletişim becerileri önemsenmektedir. Bununla ilgili olarak öğrencilerimizin BİT kullanım becerilerini geliştirme çalışılmaları yapılmaktadır.

11. Okulumuzda Dijital vatandaş olma konusunda paydaşlarımızı bilinçlendirme çalışmaları yapılmaktadır.

12. Okuldaki internet sağlayıcısı (MEB) her türlü zararlı içeriklere ulaşımı engellemiştir. Bu sitelere erişim MEB internet filtreleme ağına takılır.

13. Milli Eğitim Bakanlığı Hukuk Hizmetleri Genel Müdürlüğü 07.03.2017 tarihli 2975829 sayılı 2017-12 Sayılı Okullarda Sosyal Medyanın Kullanılması konulu yazı gereği, öğrencilerin, ebeveynlerin, personelin fotoğraflarının çekilmesi ve yayınlanması güvenlik nedeniyle yasaklanmıştır.

14. Tarayıcıların gizlilik ve güvenlik ayarları yapılarak, virüs programı kullanılarak siber zorbalığın önüne geçilmesi sağlanır.

15. Mobil cihazların/cep telefonlarının eğitim amacı dışında kullanılmaması için gerekli önlemler alınır.

B. OKULUMUZDA E-GÜVENLİK POLİTİKASININ AMACI;

- Okulumuz'un tüm üyelerini çevrimiçi olarak korumak ve güvenliğini sağlamak.
- Teknolojinin potansiyel riskleri ve yararları konusunda Mersin Zeynep Toroğlu Çamlbel Lions Anaokulu idareci, öğretmeni öğrenci ve çalışanları için farkındalık yaratmak.
- Tüm personelin güvenli ve sorumlu bir şekilde çalışmasını sağlamak, olumlu davranışları online olarak modellemek ve teknolojiyi kullanırken kendi standartlarını ve uygulamalarını yönetme gereksiniminin farkında olmak.
- Okuldaki tüm üyeler tarafından bilinen çevrimiçi güvenlik endişelerine yanıt verirken açıkça kullanılacak prosedürleri tanımlamak.
- Bu politikanın, yönetim organı, öğretmenler, destek personeli, harici yükleniciler, ziyaretçiler, gönüllüler ve okul adına hizmet veren veya bunları yerine getiren diğer kişiler (toplu olarak bu politikada ´personel´ olarak anılacaktır) dahil olmak üzere tüm personel için geçerlidir) yanı sıra çocuklar ve ebeveynleri kapsamasını sağlamak,

Sonuç olarak ana hedefimiz, internet erişimi ve kişisel cihazlar da dahil olmak üzere bilgi iletişim cihazlarının kullanımı için bu güvenlik politikasının geçerli olmasıdır. Çocuklar, personel ya da diğer kişilere, çalıştıkları dizüstü bilgisayarlar, tabletler veya mobil cihazlar gibi uzaktan kullanım için okul tarafından verilen cihazlar için de geçerlidir.

TÜM ÇALIŞANLARIN KİLİT SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.

- Kabul Edilebilir Kullanım Politikalarını (AUP'lar) okumak ve onlara bağlı kalmak.
- Okul sistemlerinin ve verilerin güvenliğinden sorumlu olmak.
- Bir dizi farklı çevrimiçi güvenlik konusundaki farkındalığa sahip olmak ve onların bakımında çocuklarla nasıl ilişkili olabileceklerini bilmek.
- Yeni ve gelişmekte olan teknolojiler kullanıldığında iyi uygulamaları modelleme
- Mümkün olduğunca müfredat ile çevrimiçi güvenlik eğitimini ilişkilendirme.
- Okul koruma politikalarını ve prosedürlerini takip ederek endişe duyan bireylerin belirlenmesi ve uygun önlem alınması.
- Olumlu öğrenme fırsatlarına vurgu yapmak.
- Bu alanda mesleki gelişim için kişisel sorumluluk almak.

ÇOCUKLARIN VE GENÇLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- Çevrimiçi güvenlik politikalarının geliştirilmesine katkıda bulunmak.
- Okulun Kabul Edilebilir Kullanım Politikalarını okumak ve onlara bağlı kalmak.
- Çevrim içi ve çevrimdışı başkalarının hislerine ve haklarına saygı duymak.
- İşler ters giderse, güvenilir bir yetişkinden yardım istemek ve çevrimiçi güvenlik sorunlarıyla karşılaşan diğer kişileri desteklemek.

Bireysel yaşlarına, yeteneklerine ve zayıf yönlerine uygun bir seviyede:

- Kendilerini ve başkalarını çevrimiçi olarak korumak için sorumluluk almak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.
- Belli bir teknolojiyi kullanmanın kişisel risklerini değerlendirmek ve bu riskleri sınırlamak için güvenli ve sorumluluk sahibi davranmak.
-

EBEVEYNLERİN BAŞLICA SORUMLULUKLARI ŞUNLARDIR:

- Okul Kabul Edilebilir Kullanım Politikalarını okumak, çocuklarını bu politikaya bağlı kalmaya teşvik etmek ve uygun olduğunca kendilerinin de bağlı kalmasını sağlamak.
- Çocuklarıyla çevrimiçi güvenlik konularını tartışmak, okulun çevrimiçi güvenlik yaklaşımlarını desteklemek ve evde uygun güvenli çevrimiçi davranışları pekiştirmek.
- Teknoloji ve sosyal medyanın güvenli ve uygun kullanımını modellemek.
- Davranışlarında, çocuğun çevrimiçi olarak zarar görme tehlikesi altında olduğunu gösteren değişiklikleri belirlemek.
- Okul veya diğer uygun kurumlardan, kendileri ve ya çocukları çevrimiçi problem veya sorunlarla karşılaşırsa yardım veya destek istemek.
- Okulun çevrimiçi güvenlik politikalarının oluşturulmasına katkıda bulunmak.
- Öğrenme platformları ve diğer ağ kaynakları gibi okul sistemlerini güvenli ve uygun bir şekilde kullanmak.
- Yeni ve gelişmekte olan teknolojilerin getirdiği fırsatlar ve risklerle ilgili olarak kendi bilinci ve öğrenimlerinden sorumlu olmak.

C. ÇEVRİMİÇİ İLETİŞİM VE TEKNOLOJİNİN DAHA GÜVENLİ KULLANIMI

Okul / web sitesinin yönetilmesi

- Web sitesinde iletişim bilgileri okul adresi, e-posta ve telefon numarası olacaktır. Personel veya öğrencilerin kişisel bilgileri yayınlanmayacaktır.
- Okul Müdürü yayınlanan çevrimiçi içerik için genel yayın sorumluluğunu alacak ve bilgilerin doğru ve uygun olmasını sağlayacaktır.
- Web sitesi, erişilebilirlik fikri mülkiyet haklarına saygı, gizlilik politikaları ve telif hakkı da dahil olmak üzere okulun yayın yönergelerine uyacaktır.
- Spam maillerden korunmak için e-posta adresleri çevrimiçi olarak dikkatli bir şekilde yayınlanacaktır.
- Öğrenci çalışmaları öğrencilerin izniyle ya da ebeveynlerinin izniyle yayınlanacaktır.
- Okul web sitesinin yönetici hesabı, uygun bir şekilde güçlü şifreyle şifrelenerek korunacaktır.
- Okul, çevrimiçi güvenlik dahil olmak üzere, toplumun üyeleri için okul web sitesinde korunma hakkında bilgi gönderecektir.

Çevrimiçi görüntü ve videolar yayınlama

- Okul, çevrimiçi paylaşılan tüm resimlerin ve videoların okul resim kullanımı politikasına uygun şekilde kullanılmasını sağlayacaktır.
- Okul , resimlerin ve videoların tümünün, veri güvenliği, Kabul Edilebilir Kullanım Politikaları, Davranış Kuralları, sosyal medya, kişisel cihazların ve cep telefonlarının kullanımı gibi diğer politikalar ve prosedürlere uygun şekilde yer almasını sağlayacaktır.
- Görüntü politikasına uygun olarak, öğrencilerin resimlerinin / videolarının elektronik olarak yayınlanmasından önce her zaman ebeveynlerin yazılı izni alınacaktır.

Video Konferans Kuralları

- Öğrenciler, bir video konferans araması veya mesajı hazırlamadan veya cevaplamadan önce bir öğretmenin izin isteyecektir.
- Video konferans, öğrencilerin yaşı ve yeteneği için uygun bir şekilde denetlenecek.
- Velilerin rızası, çocuklar video konferans faaliyetlerine katılmadan önce alınacaktır.
- Video konferans, sağlam bir risk değerlendirmesini takiben, resmi ve onaylanmış iletişim kanalları vasıtasıyla gerçekleşecektir
- Sadece ana yöneticilere video konferans yönetim alanlarına veya uzaktan kumanda sayfalarına erişim hakkı verilecektir.
- Eğitimsel video konferans servisleri için özel oturum açma ve şifre bilgileri yalnızca personellere verilecek ve gizli tutulacak.

Kişisel Cihazların ve Cep Telefonlarının Kullanımı

- Cep telefonlarının ve çocukların, gençlerin ve yetişkinler arasındaki diğer kişisel cihazların yaygın bir şekilde sahiplenilmesi, tüm üyelerin cep telefonlarının ve kişisel cihazların sorumlu bir şekilde kullanılmasını sağlamak için gerekli adımları atmalarını gerektirir .
- Gençlerin ve yetişkinlerin cep telefonlarının ve diğer kişisel cihazların kullanımı, okul tarafından kararlaştırılacak ve okul Kabul Edilebilir Kullanım veya Cep Telefonu Politikası dahil olmak üzere uygun politikalarda yer alacaktır.

- Mersin Zeynep Toroğlu Çamlıbel Lions Anaokulu, mobil teknolojilerle yapılan kişisel iletişimin, çocuklar, personel ve anne-babalar için gündelik yaşamın kabul edilen bir parçası olduğunun farkındadır; ancak, bu tür teknolojilerin okulda güvenli ve uygun bir şekilde kullanılmasını gerektirir.

Öğrencilerin kişisel cihazlarını ve cep telefonlarını kullanımı

- Öğrenciler, kişisel cihazların ve cep telefonlarının güvenli ve uygun kullanımı konusunda eğitim alacaklardır.
- Bilişim araçlarını, okul yönetimi ile öğretmenin bilgisi ve izni dışında konuşma yaparak, ses ve görüntü alarak, mesaj ve e-mail göndererek, bunları arkadaşlarıyla paylaşarak eğitim-öğretimi olumsuz yönde etkileyecek şekilde kullanmak aynı zamanda okul ders saatleri içerisinde telefon bulundurmak kesinlikle yasaktır.
- Öğrenciler ders başlamadan önce telefonlarını okul yönetimi tarafından yaptırılan telefon kutularına koymakla yükümlüdür. Cep telefonunun amacı dışında kullanımı ihlali oluştuğunda, öğrenci, telefondaki özel verilerin korunmasını sağlamak amacıyla telefonunu kapatıp ders öğretmenine verir. Ders öğretmeni öğrenci telefonunu ilgili müdür yardımcısına teslim eder. Cep telefonu öğrenci velisine teslim edilinceye kadar güvenli bir yerde tutulur. Velisi dışında telefon kimseye teslim edilmez.
- Çocukların cep telefonlarının ve kişisel cihazların tüm kullanımları, kabul edilebilir kullanım politikasına uygun olarak gerçekleşecektir.
- Cep telefonları veya kişisel cihazlar, bir öğretmenin onayını alarak onaylanmış ve yönlendirilmiş müfredat tabanlı etkinlik kapsamında olmadıkları sürece dersler veya resmi okul saatlerinde öğrenciler tarafından kullanılamaz.
- Çocukların cep telefonlarını veya kişisel cihazlarını eğitim etkinliğinde kullanımı, okul idaresi tarafından onaylandığında gerçekleşecektir.
- Bir öğrenci ebeveynlerini arama gereği duyduğunda, okul telefonunu kullanmasına izin verilecektir.
- Ebeveynlerin okul saatlerinde cep telefonuyla çocuklarıyla iletişim kurmamaları, okul idaresine başvurmaları önerilir. İstisnai durumlarda öğretmenin onayladığı şekilde istisnalara izin verilebilir.
- Öğrenciler, telefon numaralarını yalnızca güvenilir arkadaşlarına ve aile üyelerine vermelidirler.
- Öğrencilere, cep telefonlarının ve kişisel cihazların güvenli ve uygun bir şekilde kullanımı öğretilecek ve sınırların ve sonuçların farkına varılacaktır.
- Öğrencinin kişisel cihazında veya cep telefonunda bulunan materyalin yasadışı olabileceği veya cezai bir suçla ilgili kanıt sağlayabileceğinden şüpheleniliyorsa, cihaz daha ayrıntılı araştırma için polise teslim edilir.

Ziyaretçiler kişisel cihazların ve cep telefonlarının kullanılması

- Ebeveynler ve ziyaretçiler, okulun kabul edilebilir kullanım politikasına uygun olarak cep telefonlarını ve kişisel cihazları kullanmalıdır.
- Fotoğraflar veya videolar çekmek için ziyaretçiler ve ebeveynler tarafından cep telefonlarının veya kişisel cihazların kullanılması, okul resim kullanımı politikasına uygun olarak gerçekleştirilmelidir.
- Okul, ziyaretçilere kullanım beklentilerini bildirmek için uygun tabela ve bilgileri sağlayacak ve sunacaktır.
- Personelin uygun ve güvenli olduğunda sorunlara karşı çıkması beklenir ve her zaman ziyaretçilerin herhangi bir ihlalini idareye bildirecektir.

Çocukların ve gençlerin katılımı ve eğitimi

- Öğrenciler arasında güvenli ve sorumlu internet kullanımının önemi ile ilgili farkındalık yaratmak için bir çevrimiçi güvenlik (e-Güvenlik) müfredatı oluşturulur ve okulun tamamında yer alır.
- Güvenli ve sorumlu kullanım ile ilgili eğitim internet erişiminden önce yapılacaktır.
- Müfredat geliştirme ve uygulama da dahil olmak üzere okul çevrimiçi güvenlik politikaları ve uygulamaları yazarken ve geliştirirken öğrenci katkıları aranacaktır.
- Öğrenciler, Kabul Edilebilir Kullanım Politikasını, yaşlarına ve yeteneklerine uygun bir şekilde okumak ve anlamak için desteklenecektir.
- Tüm kullanıcılara ağ ve internet kullanımının izleneceği bildirilecektir.
- Kabul Edilebilir Kullanım beklentileri ve Posterler, Internet erişimi olan tüm odalarda yayınlanacaktır.
- İnternetin ve teknolojinin güvenli ve sorumlu kullanımı, müfredatta ve tüm konularda güçlenecektir.
- Dışarıdan destek, okulların dahili çevrimiçi güvenlik (e-Güvenlik) eğitim yaklaşımlarını tamamlamak ve desteklemek için kullanılacaktır.
- Okul, öğrencilerin teknolojiyi olumlu şekilde kullandıklarını ödüllendirecektir.
- Okul, öğrencilerin ihtiyaçlarına uygun olarak çevrimiçi güvenliği geliştirmek için akran eğitimini uygulayacaktır.

Personelin katılımı ve eğitimi

- Çevrimiçi güvenlik (e-Güvenlik) politikası, tüm çalışanların katılımı için resmi olarak sağlanacak ve tartışılacak ve korunma sorumluluğumuzun bir parçası olarak güçlendirilecek ve vurgulanacaktır.
- Personel, İnternet trafiğinin izlenebileceğini ve tek bir kullanıcıya kadar izlenebileceğinin farkında olacak. Okul sistemlerini ve cihazlarını kullanırken takdir yetkisi ve profesyonel davranış gereklidir.
- Personelin tüm üyelerine, profesyonel ve kişisel olarak, güvenli ve sorumlu İnternet kullanımı konusunda güncel ve uygun personel eğitimi, düzenli (en az yıllık) temelde çeşitli şekillerde sağlanacaktır.
- Çalışanların tüm üyeleri, çevrimiçi davranışlarının okuldaki rolü ve itibarını etkileyebileceğinin farkına varacaktır. Mesleği veya kurumu çürüme durumuna düşürdüğü veya profesyonel yeteneklerine güvenini kaybetmiş bir şeyin bulunduğu düşünülürse, kamusal, disiplin veya hukuki önlemler alınabilir.
- Filtreleme sistemlerini yönetme veya BİT kullanımını izleme sorumluluğu taşıyan personelin üyeleri, Liderlik Ekibi tarafından denetlenecek ve sorunları veya endişeleri bildirmek için açık prosedürlere sahip olacaklar.
- Okul, çalışanların öğrencilerin yaşlarına ve yeteneklerine göre kullanması gereken yararlı çevrimiçi araçları vurgulamaktadır.

Ebeveynlerin katılımı ve eğitimi

- Mersin Zeynep Toroğlu Çamlıbel Lions Anaokulu, çocukların internetin ve dijital teknolojinin güvenilir ve sorumlu kullanıcıları olabilmesi için ana-babaların oynayacakları önemli bir role sahip olduklarını kabul eder.
- Ebeveynlerin dikkatleri, okul açıklamaları ve okul web sitesinde okul çevrimiçi güvenlik (e-Güvenlik) politikasına ve beklentilerine yönelecektir.
- Okulumuzun bir parçası olarak ebeveynlerin çevrimiçi güvenlik bilgilerini okumaları istenecektir.
- Ebeveynler, Okula Kabul Edilebilir Kullanım Politikası'nı okumaya ve çocuklarıyla etkilerini tartışmaya teşvik edilecektir.
- Çevrimiçi güvenlik konusundaki ebeveynler için bilgi ve rehberlik, ebeveynlere çeşitli biçimlerde sunulacaktır.
- Ebeveynlerin, çevrimiçi olarak çocukları için olumlu davranışları rol modellemeleri teşvik edilecektir.

Çevrimiçi Olaylara ve Koruma sorunlarına yanıt verme

- Okulun tüm üyeleri, sakıncalı mesajlaşma, çevrimiçi / siber zorbalık vb. dahil olmak üzere karşılaşılabilecek çevrimiçi risklerin çeşitliliğinden haberdar edilecektir. Bu, öğrencilere yönelik personel eğitimi ve eğitim yaklaşımları içerisinde vurgulanacaktır.
- Okulun tüm üyeleri, filtreleme, sakıncalı mesajlaşma, siber zorbalık, yasadışı içerik ihlali vb. gibi çevrimiçi güvenlik (e-Güvenlik) endişelerini bildirme prosedürü hakkında bilgilendirilecektir.
- Dijital Abone Hattı (DSL), daha sonra kaydedilecek olan çocuk koruma endişelerini içeren herhangi bir çevrimiçi güvenlik (e-Güvenlik) olayı hakkında bilgilendirilecektir.
- İnternet´in yanlış kullanımı ile ilgili şikayetler, okulun şikayet prosedürleri kapsamında ele alınacaktır.
- Çevrimiçi / siber zorbalık ile ilgili şikayetler, okulun zorbalık karşıtı politikası ve prosedürü kapsamında ele alınacak
- Personelin yanlış kullanımı ile ilgili herhangi bir şikayet okul müdürüne yönlendirilecektir
- Okul şikayet prosedürü öğrencilere, velilere ve personele bildirilecektir.
- Şikayet ve ihbar prosedürü personele bildirilecektir.
- Okulun tüm üyeleri, gizliliğin öneminden ve endişeleri bildirmek için resmi okul usullerine uyma ihtiyacından haberdar olmalıdırlar.
- Okulun tüm üyeleri, çevrimiçi ortamda güvenli ve uygun davranış hakkında hatırlatılacak ve okul camiasının herhangi bir diğer üyesine zarar vermek, sıkıntı yaşamak veya suç oluşturan herhangi bir içerik, yorum, resim veya video yayımlamamanın önemini hatırlatacaktır.
- Okul, çevrimiçi güvenlik (e-Güvenlik) olaylarını, uygun olduğunda, okul disiplini / davranış politikasına uygun olarak yönetir.
- Okul, ebeveynlere, ihtiyaç duyulduğunda bunlarla ilgili endişeleri bildirir.
- Herhangi bir soruşturma tamamlandıktan sonra okul bilgi alacak, öğrenilen dersleri belirleyecek ve değişiklikleri gerektiği gibi uygulayacaktır.
- Sorunları çözmek için ebeveynlerin ve çocukların okulla ortak çalışması gerekir.

Mustafa TUFAN
Okul Müdürü

10 Maddede Güvenli İnternet Kullanımı

Hayatın neredeyse her alanında evimizde, cebimizde, kafelerde, restoranlarda, AVM'lerde ve aklınıza gelebilecek her türlü ortamda interneti özgürce kullanabiliyoruz. Bu denli büyüyen ve gün geçtikçe gelişmeyi sürdüren internetin, gerek sosyal gerekse iş hayatındaki olumlu katkıları yadsınamaz ancak kimi zaman da pek çok olumsuz durumla da bizi yüz yüze bırakabiliyor. İşte bu noktada olumsuz durumları yaşamamak ya da en azından minimuma indirmek adına birtakım önlemler almak gerekiyor. Peki güvenli internet kullanımı için yapılması gerekenler neler, gelin bir gözden geçirelim...

1. Kişisel Bilgileri Profesyonel ve Sınırlı Tutun

Potansiyel işveren veya müşterilerin kişisel ilişki durumunuzu veya ev adresinizi bilmesine gerek yok. Uzmanlık alanınızı, profesyonel geçmişinizi ve sizinle nasıl iletişim kuracaklarını belirtmiş olmanız yeterlidir. Şahsi bilgilerinizi tanımadığınız milyonlarca yabancı kişiye kendi ellerinizle teslim etmeyin.

2. Gizlilik Ayarlarınızı Açık Tutun

Pazarlamacılar sizin hakkınızda her şeyi bilmek isterler aynı zamanda hackerlar da ister tabii. Her ikisi de internet taramalarınızdan ve sosyal medya kullanımınızdan bir çok şey öğrenebilir. Bunun önlemini alabilmeniz için hem web tarayıcıların hem de mobil işletim sistemlerin gizliliğinizi çevrimiçi korumak için çeşitli ayarlar bulunmaktadır. Ayrıca Facebook, Instagram ve Twitter gibi büyük sosyal medya uygulamalarının da gizlilik artırıcı ayarları mevcut. Bu ayarlar içerisinden aradıklarınıza erişebilmeniz bazen çok zor olabilir. Çünkü şirketler kişisel bilgilerinizi pazarlayıp maddi gelir elde etmek için kullanıyorlar. Dolayısıyla bu bilgileri gizli tutmakta ne kadar zorlanırsanız bu durum onların işlerine gelecektir. Burada sizin yapmanız gereken tüm bu güvenlik ayarlarını detaylı bir şekilde gözden geçirip önemli olanlar başta olmak üzere tüm güvenlik ayarlarınızın açık olduğundan emin olmalısınız.

3. Gördüğünüz Her Linke Tıklamayın

Tehlikeli bir semtte yürümeyi tercih etmezsiniz değil mi? O zaman tehlikeli web sitelerinde de dolaşmamalısınız. Siber suçlular, bu tarz tehlikeli gibi gözükmeyen ancak içerisinde bir çok tuzak barındıran sahte içerikleri birer yem olarak kullanırlar. Siber suçlular bir çok insanın arama yaptıkları esnada buldukları kaynaklar şüpheli dahi olsa merak duygularına yenik düşeceklerini ve içeriklerin cazibelerine kapılıp gardlarını indireceklerini biliyorlar. Bu tarz dikkatsiz tıklamalar sonucunda kişisel verilerinizin açığa çıkabileceği gibi elektronik cihazlarınıza malware diye tabir edilen kötü amaçlı yazılımlarınyüklenmesine de sebebiyet verebilir. Dolayısıyla içinizdeki dürtülere direnerek o şüpheli gördüğünüz içeriklerdeki linklere tıklayıp hackerlara sizi hacklemeleri için fırsat tanımamalısınız.

4. İnternet Bağlantınızın Güvenli Olduğundan Emin Olun

Halka açık bir yerde, örneğin herkese açık bir Wi-Fi bağlantısı kullanarak çevrimiçi olduğunuzda, artık cihazınızın güvenliğinin üzerinde doğrudan kontrolünüz olmadığını bilmelisiniz. Bu sebepten dolayı siber güvenlik uzmanları birliği dış dünya ile bağlantı kurduğunuz halka açık özel ağlar ile ilgili oldukça endişeliler. Onların tavsiyesine göre eğer banka hesap numaranız gibi önemli bilgileri girecekseniz önce cihazınızın bağlandığı ağın güvenli olduğundan emin olmalısınız. Eğer güvenlik ile ilgili herhangi bir şüpheniz varsa, güvenli bir Wi-Fi ağına bağlanana kadar beklemelisiniz.

5. Ne İndirdiğinize Dikkat Edin

Siber suçluların en önemli amacı, kişisel bilgilerinizi çalmaya çalışan veya bilgisayarınızı kendi kötü çıkarları için kullanmaya çalışan kötü amaçlı yazılımları indirmenizi sağlamaktır. Bu kötü amaçlı yazılımlar popüler bir oyunun içerisine saklanabileceği gibi, trafik durumunu veya hava durumunu kontrol eden uygulamanın içerisinde de saklı bulunabilmektedir. Dolayısıyla şüpheli gördüğünüz veya güvenmediğiniz sitelere ait uygulamaları indirmemelisiniz.

6. Güçlü Şifreleri Seçin

Şifreler, tüm internet güvenliği yapısında en büyük zayıf noktalardan biridir. Günümüzde parolalarla ilgili esas problem, insanların siber hırsızların tahmin etmeleri kolay olan şifreler kullanmalarıdır. İnsanlar hatırlanması kolay olan şifreleri seçme eğiliminde olduklarından dolayı şifrelerini basit seçmektedirler. Eğer elektronik aygıtlarınızın ve internet üzerinde bulunan tüm hesaplarınızın güvenliklerini artırmak istiyorsanız siber suçluların tahmin etmesi zor olan güçlü şifreleri seçmeyeözen göstermelisiniz. Güçlü bir parola belirleyebilmek için, benzersiz kelime grupları oluşturmalı ve en az 15 karakter uzunluğunda, harfleri, sayıları ve özel karakterleri barındıran şifreler kullanmalısınız.

7. Güvenli Sitelerden Satın Alım Yapın

Çevrimiçi bir ürün satın aldığınızda, kredi kartı veya banka hesabı bilgilerini kullanmanız gerekmektedir. Dolayısıyla bu bilgileri güvenli, şifreli bağlantılar sağlayan sitelere girmeniz hayati önem taşımaktadır. Ürün satın almadan önce kart bilgilerini gireceğiniz web sitelerinin https: ile başladığından emin olmalısınız. Eğer yalnızca http: ile başlıyorsa o siteden kesinlikle alışveriş yapmamalısınız. Burada sonda bulunan "S" ifadesi secure yani güvenli anlamına gelmektedir.

8. Ne Yazdığınıza Dikkat Edin

İnternette bir silme anahtarı yoktur yani sizin internet üzerinde paylaştığınız tüm yorumlar, resimler ve içerikler silseniz dahi internet üzerinde sonsuza dek kalabilirler. Çevrimiçi gönderdiğiniz herhangi bir yorum veya resim Twitter'dan kaldırılmış olsa dahi, başkalarının sildiğiniz içeriği kendi bilgisayarına kopyalamadığından %100 emin olamazsınız. Dolayısıyla içerik paylaşırken ailenizin, potansiyel işvereninizin ve geri kalan çevrenizin görmesini istemeyeceğinizşeyler paylaşmamaya özen gösterin.

9. Kiminle Tanıştığınıza Dikkat Edin

Çevrimiçi olarak tanıştığınız kişiler, her zaman iddia ettikleri kişiler olmayabilir. Hatta gerçek kişiler bile olmayabilirler. As InfoWorld'ün raporlarına göre, sahte sosyal medya profilleri sıradan sosyal medya kullanıcıların kullandığı bir yöntem olduğu kadar hackerlar için de insanların hesaplarını çalmak amacıyla kullandıkları popüler bir yoldur. O yüzden çevrimiçi sosyal yaşamınızda, kişisel sosyal yaşamınızda olduğunuz kadar dikkatli ve mantıklı olmanızda fayda vardır.

10. Virüs Koruma Programınızı Güncel Tutun

İnternet güvenlik yazılımlarınız sizi her tehdide karşı koruyamayacaktır, ancak bu yazılımları güncel tuttuğunuz müddetçe sizi bir çok malware virüslerinden koruyacaklardır. Dolayısıyla, işletim sisteminizin ve kullandığınız başta güvenlik yazılımlarınız olmak üzere tüm uygulamaların güncellemelerini aksatmadan düzenli bir şekilde yapmalısınız.

Eğer yukarıda bahsettiğimiz bu 10 temel internet güvenliği kuralını aklınızda bulundurup dikkatlice internette dolaşırsanız kötü sürprizlerin çoğunu önleyeceğinizden emin olabilirsiniz.