2022-2023 EĞİTİM-ÖĞRETİM YILI
NURCAN RÜSTEM CÖMERTOĞLU ORTAOKULU
E-GÜVENLİK SWOT ANALİZİ

GÜÇLÜ YÖNLER (G) (STRENGHTS)	ZAYIF YÖNLER (Z) (WEAKNESSES)	FIRSATLAR (F) (OPPORTUNITIES)	TEHDİTLER (T) (THREATS)
1.Bakanlık tarafından tahsis edilen filtreli (korumalı) internet ağından faydalanmamız. 2.Bazı öğretmenlerimizin yardımıyla ve kontrolü altında öğrencilere e-güvenlik kurallarına uygun dijital kaynakları kullandırmamız. 3.Bazı derslerinin müfredat programlarında e-güvenliğe yer verilmiş olması. 4.Rehberlik servisimizin "siber zorbalık ve bilinçli teknoloji kullanımı" ile ilgili öğrenci,öğretmen ve velilere yönelik eğitim çalışmalrını yapması. 5.EBA destek noktası olan okulumuzda güvenli internet kullanımına Milli Eğitim Bakanlığının destek vermesi. 6.Okuluuzun sosyal medya sayfalarında çeşitli filtreleme seçenekleri ile e-güvenliğin en üst seviyede sağlanması. 7.Öğrenciler bilgisayarlarında çalışma yaptıktan sonra herhangi bir zararlı içerik kaydedilmiş dahi olsa bilgisayar kapatılıp açıldığında verilerin silinmesi. 8.Okulda kullanılan dökümanların dijital araçlar içerisinde (usb bellek vb.) korumalı olarak saklanması. 9.e-Güvenlik ile ilgili okulumuzda bir komisyonun bulunması ve güvenlik çalışmalarının yapılması.	1.Öğrencileriizin ve ailelerinin e-güvenlik yönünden yetersiz kalmaları. 2.Covid-19 nedeniyle öğrencilerin uzaktan eğitim görmesi sonucu internet kullanımının denetlenememesi. 3.Açık kaynak kodlu işletim sisteminin kullanılmaması. 4.Okulun çevirim içi politikalarının sürekli gelişen teknoloji ve buna pararlel olarak ilerleyen dijitalleşmeye ayak uydurmakta zorlanması. 5.Okulumuz personelinin bir kısmının yeni teknolojileri ve web 2 araçlarını kullanmakta yetersiz kalmaları. 6.Okulumuzda bulunan etkileşimli tahtaların (akıllı tahta) e-güvenlik tedbirlerinin arttırılması. 7. Okulumuzda bulunan bazı bilgisayarlarda anti-virüs programının bulunmaması.	1.E-güvenlik uzmanlarının çağrılarak eğiti seminerlerinin düzenlendirmesi ve yaygınlaştırılması. 2.Online platformlara ilginin artması bazı durumlarda zorunlu hale gelmesi böylece e-güvenlik konularının ön plana çıkması. 3.Covid-19 süreci sebebiyle öğretmenlerin web2 araçlarını ve diğer dijital platformları kullanmak zorunda kalması ve böylelikle e-güvenlik kurallarını daha iyi öğrenme çabaları. 4.Uzaktan eğitim nedeniyle rehberlik servisinin yapacağı çerçeve programa zorunlu olarak "bilinçli teknoloji kullanımının" genel hedef olarak yer almasının eklenmesi. 5.Öğrencilerin denetlenmesi açısında güvenlik mağduriyeti yaşanmaması için Milli Eğitimin uzaktan eğitim kanallarının(EBA) kullanılması. 6.MEBBİS üzerinden öğretmenler için açılan uzaktan eğitim kurslarının teknoloji kullamına yönelik arttırılması ve faydalandırılması. 7.e-Twinning portalında veya il,ilçe milli eğitim müdürlükleri tarafından uzaktan eğitim ve e-güvenlik eğitimlerinin açılması.	1.Online platformlara yeni dijitalleşme çağında ilginin artması. 2.Velilerin uzaktan eğitim sebebiyle öğrencilerin ekran bağımlılığının artması konusundaki endişelerinin oluşması. 3.Uzaktan eğitim ve dijitalleşme ile birlikte siber tehditlerin artması. 4.Öğrenciler arsında siber akran zorbalığının yaygınlaşması. 5.Uzaktan eğitim araçlarını yeterli düzeyde kullanmayan eğitimcilerin derslerinin sabote edilmeye açık hale gelmesi. 6.Ders sırasında görüntü açma mecburiyeti durumlarında öğretmen ve öğrencilerin siber zorbalığa maruz kalabilesi (sosyal medyada görüntülerin izinsiz paylaşılması gibi). 7.Sosyal medya ağlarının bilinçsiz ve çok kullanılması sebebiyle güvenlik tehditlerinin artması.