

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

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

