# GÜVENLİ İNTERNET KULLANIMI

*İNTERNET ETİĞİ

*SİBER ZORBALIK VE SOSYAL MEDYA

*MEB'İN SİBER ZORBALIĞA DAİR YAPTIRIMLARI

*E-GÜVENLİK

*10 MADDEDE GÜVENLİ İNTERNET KULLANIMI

# İNTERNET ETİĞİ

İnternet etiği, internet üzerinde iletişimde bulunurken doğru ve ahlaki olan davranışlar ile yanlış ve ahlaki olmayan davranışları belirleyen kurallar bütünüdür

# SİBER ZORBALIK

- Siber zorbalık ,dijital teknolojiler kullanılarak geliştirilen zorbalık davranışlarındandır
- Hakaret
- Lakap
- trollemek
- Kötü söz kullanmak
- Tehtit etmek
- Yalan haber yaymak
- ===özellikle lise çağı en çok karşılaşan grup

# Okula yansıyan siber zorbalık

- Siber zorbalığın en tehlikeli sonuçlarından birisi de intihar vakalarıdır.
- Siber zorbalığa uğrayan ve bununla baş edemeyen, yardım istemekten çekinen çocuk yada ergenlerin intihar vakaları, konunun ciddi bir sorun olarak idarak edilmesine yol açmıştır.
- Çoğunlukla şaka, eğlenceli vakit geçirmek, intikam almak, arkadaşlık ilişki-lerini yönetememek, yalnızlık duygusu, depresyon gibi psiko-sosyal faktörler nedeniyle başlayan rahatsız edici, hakaret ve tehdit içeren davranışlar, gerek zorba gerekse kurban açısından başlangıçta önemli görülmeyebilmektedir.
- Zamanla olumsuz sonuçlar doğurarak siber zorba-lığa dönüşmektedir. Siber zorbalığı önlemede öğrenciyi bilinçlendirmek, sağlıklı, etik ve bilinçli internet kullanımını öğretmek önemli yer tutmaktadır

# MEB'İN SİBER ZORBALIĞA DAİR YAPTIRIMLARI

- Siber zorbalık durumunda okulda uygulanacak idari tedbirler MEB in yönetmeliklerinde düzen-lenmiştir.
- Ortaöğretim öğrencileri için 2013 tarihli Millî Eğitim Bakanlığı Ortaöğretim Kurumları Yönetmeliği'nin 163. ve 164. maddelerinde "Disiplin cezasını gerektiren davranış ve fiiller" başlığı altında açıklanmaktadır. Ortaöğretim kurumlarında;
- bilişim araçlarını amacı dışında kullanmak
- kınama;
- bilişim araçları veya sosyal medya yoluyla eğitim ve öğretim faliyetlerine ve kişilere zarar vermek
- Kısa süreli uzaklaştırma

- ; bilişim araçları veya sosyal medya yoluyla eğitim ve öğretimi engellemek, kişilere ağır derecede maddi ve manevi zarar vermek ve kişilere, ar-kadaşlarına ve okul çalışanlarına; söz ve davranışlarla sarkıntılık yapmak, iftira etmek, başkalarını bu davranışlara kışkırtmak veya zorlamak, yapılan bu filleri sosyal medya yoluyla paylaşmak, yaymak
- okul değiştirme
- ; bilişim araçları yoluyla bölücü, yıkıcı, ahlak dışı ve şiddeti özendiren sesli, sözlü, yazılı ve görüntülü içerikler oluşturmak, bunları çoğaltmak, yaymak ve ticaretini yapmak
- örgün eğitim dışına çıkarma cezası kapsamındaki davranışlardır.
- Bu noktada sadece okul içinde değil; okul dışında da öğrencilerin yazılı, görsel ve dijital medya ile ilişkilerinin sağlıklı bir zemine oturtulabilmesi için çalışmalar yapmak, konu adli ve cezai  işlem noktasına gelmeden önlem alınması anlamında yarar sağlayacaktır

# SİBER ZORBALIK İLE KARŞILAŞIRSAK NE YAPMALIYIZ

- Görmezden gelmeyin, ailenize öğretmeninize veya güvendiğiniz bir yetişkine söyleyiniz.
- Uygunsuz davranış sergileyen kişileri şikayet ediniz.
- Siber zorbalıkta bulunan kişileri engelleyin.
- Siber zorbalar tarafından gelen mesajlara cevap vermeyin.

# E - GÜVENLİK

***Mark Zuckerberg bizi annemizden daha***
***İyi tanıyor olabilir mi?***

- Güçlü şifre oluşturun (en az 8 karekter,farklı karekterler kullanın,farklı üyelikleri farklı şifrelerle kullanın.
- Sosyal medya paylaşımlarınız hayatınızı karartmasın, suç teşkil etmesin.
- Bilgi kirliliğine kapılmayıp doğru bilgiye ulaşın.
- Bilgi gizliliği ,ve güvenlik ÇOK  önemli

.(Kişisel veri ve bilgiler gizli kalmalı ,sosyal medyada kimlik gizliliği İÇİN kısıtlama uygulamaSINIZ …adres,tel,diğer bilgler gizli olmalıdır.

# 10 MADDEDE GÜVENLİ İNTERNET KULLANIMI

- 1.Kişisel bilgileri profesyonel ve sınırlı tutun.(Şahsi bilgilerinizi milyonlarca kişiye kendi ellerinizle teslim etmeyin.
- 2.Gizlilik ayarlarınızı açık bırakın.

(Pazarlamacılar sizin hakkınızda her şeyi bilmek isterler Hacerlar da tabi.)Her ikisi de sosyal medya paylaşımlarından çok şey öğrenebilir bunu engellemek ancak gizlilik ayarlarınızı maksimum seviyeye çıkarmakla olur.

- 3.Gördüğünüz her linke tıklamayın.(Kendinizce şüpheli gördüğünüz linklerden uzak durup tıklamamanız gerek .Bu linkler tıklandığında bazı kişisel bilgileriniz açığa çıkmaktadır ve bu da dolandırıcıların ekmeğine bal sürmektir.
- 4.İnternet bağlantınızın güvenli olduğunuzdan emin olun.(Halka açık olan wi-fi alanlarında artık cihazınızın ve bilgilerinizin tek kontrolunun sizde olmadığından emin olun.

- 5.Ne indirdiğinize dikkat edin.Siber suçların en önemli amacı ,kişisel bilgilerinizi çalmaya çalışan ,bilgisayarınızı kendi kötü amaçları için kullanmaya çalışan yazılımlar indirmenizi sağlamaktır.Bu amaca hizmet eden yazılımlar bir oynun içine saklı olduğu gbi bazen hava durumu gibi basit bir uygulamaya da gizlenmiş olabilir .Şüpheli gördüğünüz uygulamayı indirmeyin
- 6.Güçlü şifre seçin

- 7.Güvenli sitelerden satın alım yapın.Çevrim içi bir ürün satın aldığınızda kredi kartı gibi hayati bilgiler önem taşıyan bilgiler vereceğiniz için sitenin güvenli olması çok önemlidir .Burada web sitesinin hptts ile başlayan linki olması sadece hptt olmaması çok önemlidir.Linkin sonundaki ’S’harfi güvenli anlamında olan secure demektir.AMAN DİKKAT S ÇOK ŞEY DEMEK.
- 8. Ne yazdığınıza dikkat edin .İnternette silme anahtarı yoktur yani sildiğiniz tüm yorum, resim,içerik internet üzerinde sonsuza dek kalabilmektedir.

9.Kiminle tanıştığınıza dikkat edin.AS ınfo Word ün raporuna göre sahte sosyal medya hesapları çoğunluka hackerların, insanların hesaplarını çalma yöntemidir

10.Virüs tarama programınızı güncel tutun.Bu programları güncel tutmanız sizi birçokvirüsten koruyacak daha bilgisayarınızdaki bilgilerinize erişmeden bloklayacaktır.

Hazırlayan:Hale Nur ÖZTÜRK

ULUBATLI HASAN ANADOLU LİSESİ