GÜVENDE OL !

Güvenli İnternet Nedir?

Güvenli internet : İşbirliği ağının misyonu ,çocuklara ve gençlere pozitif, güvenli ve etkili, internet, yanı sıra diğer çevrimiçi ve mobil teknolojileri kullanmayı hedeflemektedir.. Eğitimciler, veliler, medya, ve diğer tüm ilgili kişiler tarafından özellikle çocuklar ve gençlerin vatandaşların hak ve ihtiyaçlarının korunması için ortak sorumluluk gerektirir.

Yeni dijital teknolojiler, çocuklar ve gençler için fırsatlar sunar. Bugün Online dünya, çocukların yaşamlarının önemli bir parçası: onlar iş, yaşam ve oyun her yönüyle teknoloji ile iç içe, 'Dijital Çağın' çocukları olarak büyüyorlar.Bu noktada interneti güvenli internet eğitimi verilmelidir.Başta çocuklar ve gençler olmak üzere tüm vatandaşların bilinçli birer 'Dijital Vatandaş' olmalarını sağlamak amacıyla 'Dijital Vatandaşlık algısının oluşturulması, güvenli internet kullanımına teşvik etmektedir.

Güvenli İnternet Günü

Avrupa Komisyonu'nun Güvenli İnternet Programı çerçevesinde, Güvenli internet ağı, 2004 yılından bu yana her Şubat ayında ve eş zamanlı olarak, Avrupa ve dışındaki ülkeleri kapsayarak, Güvenli İnternet Günü, düzenlemektedir.Güvenli İnternet Günü (SID) özellikle dünya çapında çocuk ve gençler arasında online teknoloji ve cep telefonları ile daha güvenli ve sorumlu bir şekilde kullanımını teşvik etmek için her yıl Şubat ayında **insafe** tarafından organize edilmektedir.Insafe 31 ulusal bilinçlendirme merkezinden oluşan, bir Avrupa ağı olan (AB üyesi ülkelerin 27'sinde, ayrıca İzlanda, Norveç, Rusya ve Sırbistan). Her ulusal Merkezi, farkındalık ve eğitim kampanyaları uygulayan bir yardım hattı ve daha iyi bir internet yaratmak için kanıta dayalı, çok paydaşlı bir yaklaşım sağlamak için gençlerle yakından çalışır.

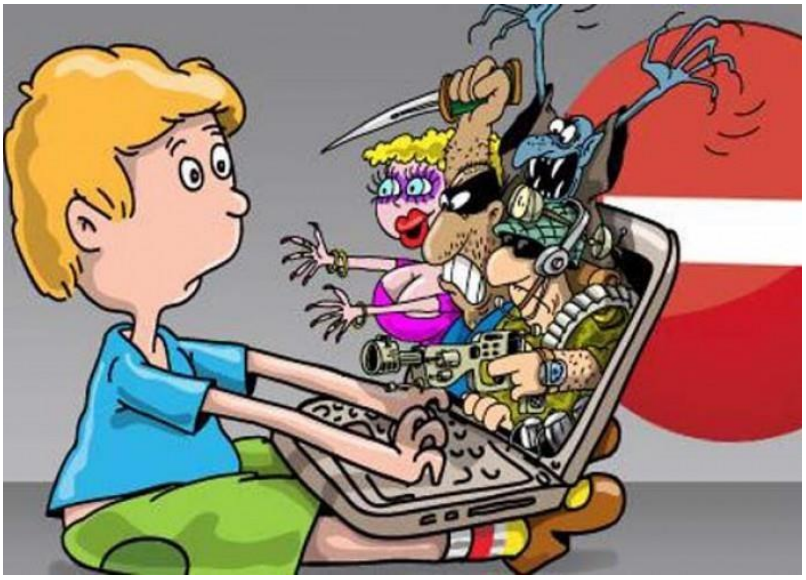
Insafe; internetin ve mobil cihazların gençler tarafından güvenli ve sorumlu kullanımını teşvik eden Avrupa Farkındalık Merkezleri ağıdır. Daha Güvenli İnternet Programı tarafından ortaklaşa finanse edilmektedir. İnternet sitesi: www.saferinternet.org

Görev beyanı

Güvenli internet işbirliği ağının misyonu, çocuklara ve gençlere pozitif, güvenli ve etkili, internet, yanı sıra diğer çevrimiçi ve mobil teknolojileri kullanmayı teşvik etmektir. Ağ hükümet, eğitimciler, veliler, medya, sanayi ve diğer tüm ilgili aktörler tarafından özellikle çocuklar ve gençlerin vatandaşların hak ve ihtiyaçlarının korunması için ortak sorumluluk, gerektirir. Insafe ortakları en iyi uygulama, bilgi ve kaynak paylaşımı için birlikte çalışır. Okullar, ev ve okul arasındaki dijital uçurumu, insanları bilinçlendirme amacı ile aileleriyle etkileşime girer.

Insafe ortakları izlemek ve öğrenmek için bir yer olarak web imajını güçlendirmeyi hedefliyor.. Bunlar zararlı veya yasa dışı içerik ve raporlama hizmetleri konusunda bilinçlendirmek için gayret gösteriyor. Ortakları ve diğer aktörler arasındaki yakın işbirliği sayesinde, Güvenli internet ,internet güvenliği bilinçlendirme standartlarını yükseltmek ve tüm bilgi okuryazarlığı gelişimini desteklemeyi hedefliyor.

e-Güvenlik Etiketi: e-Güvenlik Etiketi; okullara, eğitim ve öğretim deneyiminin parçası olarak çevrimiçi teknolojilere güvenli bir şekilde erişim sağlayarak güvenli ve zenginleştirici bir ortam sağlama görevlerinde yardımcı olmayı amaçlamaktadır. Ayrıca, politikacıların okullarda karşılaşılan e-Güvenlik sorunlarını daha iyi bir şekilde anlamalarını sağlamaktadır. İnternet sitesi: www.esafetylabel.eu



GÜVENLİ İNTERNET KURALLARI

1. İnternet hayatınızın tamamı değil, sadece bir parçası olsun. Çok fazla zamanınızı çalmasına izin vermeyin.
2. İnterneti ailelerinize ve arkadaşlarınıza değişmeyin. Aileleriniz ön koltukta, internet ise arka koltukta otursun.
3. İnternette her bilgi doğru olmayabilir. İnternette elde ettiğiniz bilgiyi en az 3 kaynaktan kontrol edin. Ödevinizde kullanıyorsanız kaynağını belirtin
4. İnternet ortamındaki bedava teklifler büyük ihtimalle gerçek değildir. Tanımadığınız kişi size neden bedava bir şey teklif etsin ki.
5. Adınız, okulunuz, adresiniz, telefon numaranız, aile bireylerinizin adı vb. gibi kişisel bilgilerinizi paylaşmayın. Paylaşılan küçük gibi görünen bilgiler, büyük zararlara sebep olabilir.
6. İnternet ortamında paylaşacağınız resminiz, size ait video gibi paylaşımları önce düşünün, sonra paylaşın. Paylaştıklarınız sizin veya sevdiklerinizin üzülmesine sebep olmasın.
7. Şifreleriniz güçlü olsun. Adınızı ve doğum tarihinizi, ard arda gelen kelimeleri ve sayıları şifre olarak belirlemeyin. Anlamlı bir cümle kurun ve o cümlenin kelimelerinden seçtiğiniz en az 8 karakterden oluşan şifreler oluşturun
8. İyi ve nazik bir kullanıcı olmaya çalışın. Gerçek hayatta Merhaba dediğiniz arkadaşınıza internet ortamında "mrb" değil, yine merhaba deyin. Tamam derken "Ok." veya "Tmm" yerine yine tamam deyin.
9. Gerçek hayatta yüzüne söylemeyeceğiniz ifadeleri internet ortamında da söylemeyin.
10. Gerçek hayatta olduğu gibi, internet ortamında da tanımadıklarınızı arkadaş edinmeyin.
11. İnternet ortamında tanımadıklarınıza cevap vermeyin, tekliflerini reddedin, size gönderdikleri mesajları açmadan silin
12. İnternet ortamında sizi rahatsız edenleri, sizi taciz edenleri ailelerinize söyleyin. Ailelerinizle birlikte emniyete veya savcılığa suç duyurusunda bulunun
13. İnternetin zararlı içeriklerinden korunmak için tamamıyla ücretsiz olan "Güvenli İnternet Hizmeti"nden ailelerinizi haberdar edin.

GÜVENLİ INTERNET

İZİN AL!

İnternete girmeden önce her zaman bir büyüğünden izin al.

PAYLAŞMA!

İnternette isim, adres, fotoğraf, şifre, okulunun ismi gibi kişisel bilgilerini ASLA paylaşma.

BULUŞMA!

İnternette tanıştığın biriyle ASLA yüzyüze buluşma.

AÇMA!

Tanımadığın insanlardan gelen mesajları ASLA açma.

ANLAT!

Hangi sitelerde dolaştın, neler öğrendin, kimlerle konuştun her zaman anne/ babana anlat.

ONLINE ANNE

www.onlineanne.com

HERE ARE THE TOP 10 INTERNET SAfety RUles to follow to HELP yoU AVOİD GETTİnG İnto TROUBle onLİne (AND OFFlİne).

1. Keep Personal Information Professional and Limited

Potential employers or customers don't need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You wouldn't hand purely personal information out to strangers individually—don't hand it out to millions of people online.

2. Keep Your Privacy Settings On

Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. But you can take charge of your information. As noted by Lifehacker, both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like Facebook also have privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy safeguards, and keep them enabled.

3. Practice Safe Browsing

You wouldn't choose to walk through a dangerous neighborhood—don't visit dangerous neighborhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet's demimonde is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge, you don't even give the hackers a chance.

4. Make Sure Your Internet Connection is Secure

When you go online in a public place, for example by using a public Wi-Fi connection,PCMag notes you have no direct control over its security. Corporate cybersecurity experts worry about "endpoints"—the places where a private network connects to the outside world. Your vulnerable endpoint is your local Internet connection. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network) before providing information such as your bank account number.

5. Be Careful What You Download

A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be

disguised as an app: anything from a popular game to something that checks traffic or the weather. As PCWorld advises, don't download apps that look suspicious or come from a site you don't trust.

6. Choose Strong Passwords

Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.

7. Make Online Purchases From Secure Sites

Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. As Boston Universitynotes, you can identify secure sites by looking for an address that starts with *https:* (the S stands for *secure*) rather than simply *http:* They may also be marked by a padlock icon next to the address bar.

8. Be Careful What You Post

The Internet does not have a delete key, as that young candidate in New Hampshire found out. Any comment or image you post online may stay online forever because removing the original (say, from Twitter) does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you hadn't made, or get rid of that embarrassing selfie you took at a party. Don't put anything online that you wouldn't want your mom or a prospective employer to see.

9. Be Careful Who You Meet Online

People you meet online are not always who they claim to be. Indeed, they may not even be real. As InfoWorld reports, fake social media profiles are a popular way for hackers to cozy up to unwary Web users and pick their cyber pockets. Be as cautious and sensible in your online social life as you are in your in-person social life.

10. Keep Your Antivirus Program Up To Date

Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

Keep these 10 basic Internet safety rules in mind and you'll avoid many of the nasty surprises that lurk online for the careless.

Sevgili gocuklar,

- Sizler de biliyorsunuz ki, yayamin her alaninda haklarimiz oldujju gibi, haklarimizi kullanirken uymamiz ve dikkat etmemiz gereken kurallar vardir.
- Iletiyim hak ve ozgurlu§u iginde yer alan Internet kullanlmlnda da dikkat etmemiz gereken kurallar vardir.
- Bu kurallar sizlerin Internet'ten guvenli bir yekilde yararlanmanizi sajjlamak agisindan onem tayimaktadir.

Sizlerin daha bilinçli ve güvenli Internet kullaniciları olmanızı saglayacak bazi oneriler aşagıda sıralanmıştır.

- Her şeyden önce internet ve bilgisayarda çok fazla vakit geçirmeyin. Oyuna, kitap okumaya, spora ve sanata vakit ayirin. Internet ve bilgisayar kullanma surenize aileniz ve öğretmenlerinizle konuşarak karar verin.

- Internet ortaminda, sohbetlerde sizi rahatsiz eden görüntü, ses ve yazilar yer alirsa hemen bulundugunuz Internet ortamindan çıkın ve ailenize haber verin.
- Bir sitede yer alan oyunlara, aktivitelere, yarışmalara katılmadan önce bunların yaşınıza uygun olup olmadıgını mutlaka ailenize ve öğretmeninize danışın. Ailenizin ve ögretmeninizin uyarilarini dikkate alın.

İNTERNETİ OTURMA ODANIZA TAŞIYIN

Bilgisayari mutlaka evinizde ailenizin hep birlikte zaman gecirdigi yasam odaniza tutun. Bu sayede cocugunuzun İnternetle ilişkisini kontrol etmeniz daha kolay olacaktır.

DİKKAT!!

Interneti ASLA bir bebek bakıcısı ya ds çocuk yetistiricisi olarak dusunmeyin.

Size zaman l‹alMasi için, cocugunuzun kendi odasında bilgisayar başında uzun zaman gecirimesine musade ettiginizde cocugunuza iyilik vapmadıgınızı bilin.

İNTERNET KULLANIMI İLE İLGİLİ KURALLAR BELİRLEYİN

Internet l‹ullanimi ile ilgili olatak. belirli ve kesin kurallar koyun ve ba fa l‹endiniz olmal‹ uze‹e oiledeki herl‹esin bu i‹urolJoro uymosi l‹onusundo korarli olun.

AİLE SÖZLEŞMESİ

Aile icerisinde, Internet kullanimiyla iigili belirlediginiz l‹urallar da içeren bir aile sozlesmesi yapın, ailedeki tüm fertler bu Sözleşmeyi imzalasın ve anlaşmayı bilgisayarınızdan görülecek bir vere asın.