Dijital Göçmenler için Dijital Yetkinlik: Anlama ve Öğrenme Çerçeveleri Toolkiti

Digital Competence for Digital Immigrants:
A Toolkit for Understanding and Learning Frameworks

Co-funded by the
Erasmus+ Programme
of the European Union

DigiComp

Co-funded by the
Erasmus+ Programme
of the European Union

Hazırlayanlar | Prepared by

Hülya Öztekin
Assoc. Prof. Dr., Erciyes University, Faculty of Communicaton
hoztekin@erciyes.edu.tr

Burak Ünlü
Res. Asst. Ph.D., Erciyes University, Faculty of Communication
burakunlu@erciyes.edu.tr

Danışman | Advisor

Metin Eken
Assoc. Prof. Dr., Erciyes University, Faculty of Communicaton
metineken@erciyes.edu.tr

Yürütücü | Coordinator

Hakan Aydın
Prof. Dr., Erciyes University, Faculty of Communication
haydin@erciyes.edu.tr

This intellectual output has been produced under the “Improving Digital Competencies for Digital Immigrants: Tackling with Digital Divide and Digital Social Inequality” Project. The Project titled Improving Digital Competencies for Digital Immigrants: Tackling with Digital Divide and Digital Social Inequality funded by the Erasmus+ Program of the European Union. However, European Commission and Turkish National Agency cannot be held responsible for any use which may be made of the information contained therein.

Bu entelektüel çıktı “Dijital Göçmenler için Dijital Yeterlilikleri Artırma: Dijital Bölünme ve Dijital Sosyal Eşitsizlikle Mücadele” Projesi kapsamında üretilmiştir. “Dijital Göçmenler için Dijital Yeterlilikleri Artırma: Dijital Bölünme ve Dijital Sosyal Eşitsizlikle Mücadele” Projesi Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

https://digicomp.erciyes.edu.tr/

İÇİNDEKİLER

ÖZET

Dijital teknoloji ve internet kullanımı tecrübelerinin yetersizliği sebebiyle dijital göçmenler ağ toplumunun dezavantajlı bir kesimini oluşturmaktadır. Bu toolkit, dijital göçmenlerin tecrübe ve bilgi eksikliklerini giderilmesinde temel bir başlangıç noktası olarak kullanılması için oluşturulmuştur. Toolkit beş ana bölümden oluşmaktadır. Başlangıç bölümünde, dijital hizmetlerin ve internetin günlük kullanımında sıklıkla karşılaşılabilecek olan kavram ve hizmetler açıklanmıştır. E-posta, web tarayıcı, çevrim içi alışveriş ve sosyal medya gibi konu ve hizmetleri içeren bölüm aynı zamanda kamu hizmeti uygulamalarının kapsamı ve kullanımı hakkında temel düzeyde bilgiler de sunar. 3D Secure, SSL sertifikası ve HTTPS gibi çevrim içi alışveriş ve bankacılık işlemlerinin güvenliğine ilişkin kavramlar da bu bölümde ele alınmıştır. Toolkitin ikinci bölümünde, dijital teknolojilerin ve internetin sunduğu olanaklara ilişkin farkındalığın arttırılması hedeflenmektedir. Bölümde, internetin sağladığı ağ toplumuna entegrasyon, hayat boyu öğrenme, bilgiye erişimi kolaylaştırma, sosyalleşme, hızlı ve anlık kişilerarası iletişim ve veri yedekleme gibi olanaklar kısaca açıklanmıştır. Dijital Teknolojilerin ve İnternetin Taşıdığı Riskler başlıklı üçüncü bölümde ise okuyucunun, bir önceki bölümde açıklanan imkân ve hizmetlerin beraberinde getirdiği risklere ilişkin sahip olduğu bilgi birikiminin artırılması amaçlanmıştır. Bölümde ciddiye alınması ve dikkat edilmesi gereken kişisel veri güvenliği, çevrim içi dolandırıcılık ve kimlik hırsızlığı, oltalama (yemleme), siber zorbalık, kötü amaçlı yazılımlar (virüsler), düşük özsaygı, kendini ifade etme ve sosyalleşme yetersizlikleri ve bağımlılık gibi risklere değinilmiştir. Çalışmanın dördüncü bölümü, dijital dünyanın uçsuz bucaksız olanaklarından yararlanmak ve bu olanakların arasına ustalıkla gizlenen risklerinden kaçınmak için dikkat edilmesi gereken dijital sorumluluklara ayrılmıştır. Çevrim dışı dünyada bir vatandaş olarak yerine getirilen sorumluluklar gibi çevrim içi ortamlarda da dijital vatandaşlık sorumluluklarına sahip olduğumuz farkındalığını oluşturmak için telif haklarına dikkat etme, kişisel veri paylaşımı konusunda dikkatli olma, lisanslı yazılım kullanma, kullanılan yazılımları ve antivirüs programlarını güncel tutma ve sosyal medyada aldatıcı kimlik kullanmama gibi konulara kısaca değinilmiştir. Bir diğer dijital sorumluluk olan dijital ebeveynlik konusu ise ayrı bir alt bölümde detaylı olarak ele alınmıştır. Bu kısımda, dijital bir ebeveyn olarak dikkat edilmesi gereken; çocuklarının internet kullanımlarını ebeveyn kontrol programları ile takip etme, oynadıkları oyunları, ziyaret ettikleri siteleri suçlayıcı değil keşfedici bir tavırla anlamaya çalışma, kişisel bilgi, fotoğraf ve videoları sosyal medya ve çevrim içi oyunlarda paylaşmaması konusunda çocuklarını bilinçlendirme, sosyal medya aracılığı ile herkesle iletişim kurulmaması gerektiği hakkında çocuklarında farkındalık oluşturma gibi hususlar listelenmiştir. Toolkitin ilk dört bölümünün her birinin sonunda okuyuculara ilgili bölüm hakkındaki bilgi ve farkındalıklarını test etme şansı veren kısa anketler bulunmaktadır. Bu kısa ölçekler, okuyuculara dijital olanaklar, riskler ve sorumluluklar hakkında kendilerini test etme ve geliştirme imkânı sunmaktadır. Toolkitin son bölümünde ise daha iyi ve güvenli bir dijital hayat için kimi öneriler listelenmiştir. Bu başlıkta özellikle çevrim içi ortamda bırakılan dijital ayak izlerinin çevrim dışı hayatı etkileyecek kadar önemli bir parçası olduğunun altı çizilerek paylaşım farkındalığı, şifre güvenliği, kullanılan yazılımları güncel tutma ve uygulama izinlerini yönetme konularında basit ve uygulanabilir öneriler sunulmuştur. Çalışmanın sonuna faydalı olabilecek diğer rehber ve kılavuzların linkleri eklenmiştir.

ABSTRACT

Due to the lack of experience in using digital technology and Internet, digital immigrants constitute a disadvantaged segment of the network society. This toolkit was created for the use of digital migrants as a basic starting point for eliminating their lack of experience and knowledge. The toolkit consists of five main sections. In the initial section, the concepts and services that can often be encountered in the daily use of digital services and Internet are described. The section, which includes topics and services such as e-mail, web browser, online shopping and social media, also provides basic information about the scope and use of public service applications. Concepts related to the security of online shopping and banking transactions such as 3D Secure, SSL certificate and HTTPS are also discussed in this section. In the second part of the toolkit, it is aimed to increase awareness of digital technologies and the possibilities offered by Internet. In the section, the possibilities such as integration into the network society provided by Internet, lifelong learning, facilitating access to information, socialization, fast and instant interpersonal communication and data backup are briefly explained. The third section titled Risks Posed by Digital Technologies and Internet is aimed at increasing the knowledge of the reader about the risks posed by the facilities and services described in the previous section. In the section, risks such as personal data security, online fraud and identity theft, phishing, cyberbullying, malware (viruses), low self-esteem, lack of self-expression and socialization, and addiction, which should be taken seriously and be considered, are mentioned. The fourth part of the study is related to digital responsibilities that need to be taken into account in order to take advantage of the vast possibilities of the digital world and avoid the risks that are decently hidden among these possibilities. Issues such as non-use are briefly mentioned like paying attention to copyrights, being careful about sharing personal data, using licensed software, keeping up-to-date software and antivirus programs, and deceptive identity on social media to create awareness that we have digital citizenship responsibilities in online environments, just like the responsibilities fulfilled as a citizen in the offline world. Another digital responsibility, the issue of digital parenting, is discussed in detail in a separate subsection. This section lists issues as follows: as a digital parent, attention should be paid to monitoring their children's internet use with parental control programs, trying to understand the games they play and websites they visit in an exploratory manner-not accusing, raising awareness of their children about not sharing personal information, photos and videos on social media and online games, not communicating with everyone through social media. At the end of each of the first four sections of the toolkit, there are short questionnaires that enables readers to test their knowledge and awareness of the relevant section. These short scales provide readers with the opportunity to test and develop themselves about digital possibilities, risks and responsibilities. In the last section of the toolkit, some suggestions for a better and safer digital life are listed. Under this title, it is emphasized that digital footprints left on the internet are an important part of online life that will affect offline life, and simple and applicable suggestions are presented on sharing awareness, password security, keeping the software used up-to-date, and managing application permissions. Links to other useful guides and manuals have been added to the end of the study.

ZUSAMMENFASSUNG

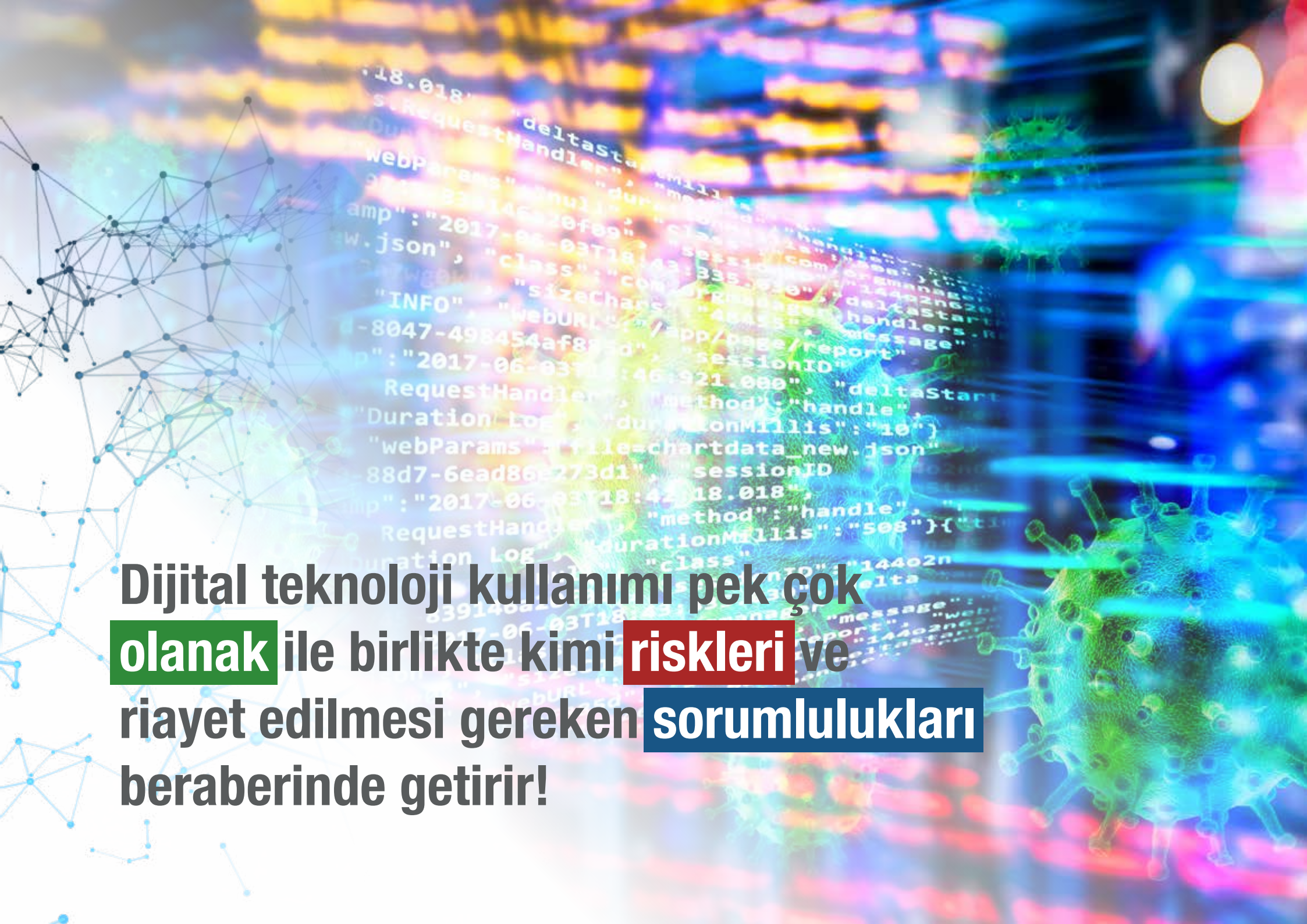
Aufgrund fehlender Erfahrung im Umgang mit Digitaltechnik und dem Internet sind „Digitale Immigranten“ in der Netzwerkgesellschaft benachteiligt. Dieser Werkzeugkasten soll grundlegend dazu beitragen, „digitalen Immigranten“ dabei zu helfen, fehlendes Wissen und Erfahrung zu überwinden. Der Werkzeugkasten besteht aus fünf Hauptabschnitten. Im ersten Abschnitt werden die Konzepte und Dienste beschrieben, die in der täglichen Nutzung von digitalen Diensten und im Internet häufig anzutreffen sind.

In diesem Abschnitt geht es um den Umgang mit E-Mails, Webbrowsern, das Online-Shopping und Social Media sowie grundlegende Informationen zu Umfang und Nutzung öffentlich-rechtlicher Anwendungen. Es werden darüber hinaus Konzepte im Zusammenhang mit der Sicherheit von Online-Einkäufen und Bankgeschäften wie 3D Secure, SSL-Zertifikat und HTTPS behandelt. Im zweiten Teil des Werkzeugkastens soll das Bewusstsein für digitale Technologien und die Möglichkeiten des Internets geschärft werden. In diesem Abschnitt geht es um Themen wie: Integration in die Netzwerkgesellschaft des Internets, lebenslanges Lernen, Erleichterung des Zugangs zu Informationen, Sozialisation, schnelle und unmittelbare zwischenmenschliche Kommunikation und Datensicherung. Der dritte Abschnitt mit dem „Titel Risiken durch digitale Technologien und das Internet“ soll das Wissen des Lesers über die Risiken erweitern, die von den im vorherigen Abschnitt beschriebenen Einrichtungen und Diensten ausgehen.

Im diesem Abschnitt werden Risiken wie Sicherheit personenbezogener Daten, Online-Betrug und Identitätsdiebstahl, Phishing, Cybermobbing, Malware (Viren), geringes Selbstwertgefühl, mangelnde Selbstdarstellung und Sozialisation sowie Sucht, die ernst genommen und berücksichtigt werden sollten , adressiert. Der vierte Teil der Studie bezieht sich auf digitale Verantwortlichkeiten, die berücksichtigt werden müssen, um die enormen Möglichkeiten der digitalen Welt zu nutzen und die in diesem Zusammenhang entstehenden Risiken zu vermeiden. Hierbei geht es um Themen wie die Nichtnutzung, die Beachtung von Urheberrechten, die sorgfältige Weitergabe personenbezogener Daten, die Verwendung lizenzierter Software, die Aktualisierung von Software und Antivirenprogrammen sowie die Identitätstäuschung in sozialen Medien, um ein Bewusstsein dafür zu schaffen, dass in der digitalen Welt genau wie in der Offline-Welt rechtliche Pflichten zu beachten sind. In einem weiteren Unterkapitel geht es um die digitale Verantwortung der Eltern im Hinblick auf ihre das Internet nutzenden Kinder. Dieser Abschnitt befasst sich mit folgenden Problemen: Eltern sollten darauf achten, die Internetnutzung ihrer Kinder mit Kindersicherungsprogrammen zu überwachen und zu versuchen, die Spiele, die sie spielen, und die Websites, die sie besuchen, zu verstehen – ihnen keine Vorhalte zu machen, sondern das Bewusstsein ihrer Kinder für die Gefahren des Netzes zu schärfen und ihre Kinder dafür zu sensibilisieren, keine persönlichen Informationen, Fotos und Videos in sozialen Medien und Online-Spielen zu teilen und nicht unvorsichtig über soziale Medien zu kommunizieren. Am Ende jedes der ersten vier Abschnitte des Werkzeugkastens gibt es kurze Fragebögen, die es den Lesern ermöglichen, ihr Wissen und ihre Kenntnis des jeweiligen Abschnitts zu testen.

RESUMEN

Debido a la falta de experiencia en el uso de las tecnologías digitales e Internet, los inmigrantes digitales constituyen un segmento vulnerable de la sociedad en red. Esta caja de herramientas se creó para ser utilizada por los migrantes digitales como un punto de partida para eliminar su falta de experiencia y conocimiento. La caja de herramientas consta de cinco secciones principales. En la sección inicial se describen los conceptos y servicios que pueden encontrarse en la utilización diaria de los servicios digitales e Internet. La sección, que incluye temas como el correo electrónico, navegación web, compras electrónicas y social media, incluyendo también información básica sobre el abasto y utilización de aplicaciones de servicios públicos. En esta sección también se discuten conceptos relacionados con la seguridad de las compras online y las transacciones bancarias, como el 3D Secure, los certificados SSL y la HTTPS. La segunda parte de esta caja de herramientas se propone aumentar el conocimiento de las tecnologías digitales. Se explican brevemente las posibilidades que ofrece Internet, el aprendizaje a lo largo de la vida, la facilidad de acceso a la información, la socialización, así como las comunicaciones rápidas e instantáneas y la copia de seguridad de los datos. La tercera sección, que lleva el nombre de “Riesgos planteados por las tecnologías digitales e Internet” se dirige a mejorar el conocimiento del lector sobre los riesgos de los servicios descritos en la sección anterior. Se mencionan riesgos que hay que tomar seriamente, como la seguridad de los datos personales, el fraude online y el robo de identidad, el phishing, cyberbullying, los virus y el malware, la baja autoestima, la falta de expresión y socialización en esos medios y la adicción. La cuarta parte del estudio se refiere a las responsabilidades digitales que hay que tener en cuenta para conseguir disfrutar de los beneficios del mundo digital y al mismo tiempo evitar los riesgos que se esconden tras dichas posibilidades. Se tratan temas referidos a prestar atención a los derechos de propiedad, ser cuidadoso con la información personal que se comparte, el uso de las licencias de software, así como su actualización, los programas antivirus y la suplantación de identidad en los medios sociales; todo ello para establecer que tenemos unas responsabilidades de ciudadanía digital, igual que las tenemos como ciudadanos en el mundo offline. Otra responsabilidad digital ser refiere a la crianza digital, que se desarrolla en una subsección separada. En ese apartado se trabajan temas como que deberíamos prestar atención y monitorizar el uso de Internet de nuestros hijos, utilizando programas de control parenteral, a intentar comprender los juegos a los que juegan y las webs que visitan, de una manera exploratoria, sin acusaciones, concienciando a nuestros hijos a no compartir información personal, fotos y vídeos en medios sociales o juegos online, ni a comunicarse con todo el mundo. Al final de cada una de esas cuatro secciones de la caja de herramientas hay unos breves cuestionarios que permiten al lector poner a prueba su conocimiento y concienciación. Estas breves escalas ofrecen al lector la oportunidad de probar y desarrollarse en función de las posibilidades, riesgos y responsabilidades digitales. En la última sección de la caja de herramientas se ofrecen algunas sugerencias para una mejor y más segura vida digital. Se enfatizan las huellas digitales que se dejan en Internet son una parte importante de la vida online que afectará la vida offline. Para ello se ofrecen sugerencias sencillas y aplicables sobre el compartir información, la seguridad de contraseñas, la actualización de los programas y la gestión de permisos de aplicación. En el final del estudio se han añadido referencias a otras guías y manuales útiles aplicables.


Dijital teknoloji kullanımı pek çok
olanak ile birlikte kimi riskleri ve
riayet edilmesi gereken sorumlulukları
beraberinde getirir!

SUNUŞ

Dijital teknolojilerin sürekli geliştiği, değiştiği ve yaşamın her alanını içine alarak yaygınlaştığı günümüzde bu teknolojileri tanımak, kullanabilmek ve gündelik hayata adapte edebilmek son derece önem kazandı. Dijital teknolojiler ve internet, gündelik hayatta bize pek çok fırsat ve olanak sunuyor. Haberleşmek, iletişim kurmak, bankacılık işlemlerimizi gerçekleştirmek, fatura ve vergilerimizi ödemek, hastane randevusu almak, tıbbi kayıtlarımıza ulaşmak, alışveriş yapmak, video izlemek, müzik dinlemek, oyun oynamak, arkadaşlarımızla sohbet etmek, yeni insanlar tanımak, yeni şeyler öğrenmek gibi sayısız şeyi dijital teknolojiler aracılığıyla gerçekleştirmek mümkün. Bununla birlikte dijital teknolojiler pek çok riski de barındırıyor. Dijital teknolojilerin sunduğu fırsat ve olanaklardan yararlanırken bu yeni dünyanın taşıdığı risklerin farkına varmak ve bu risklere bağlı olarak ortaya çıkan sorumlulukları öğrenmek de gerekiyor.

Bu bilgi, beceri ve edinimler konusunda, dijital teknolojinin içerisinde doğan ve 'dijital yerli' olarak adlandırılan çocukların ve gençlerin daha avantajlı oldukları bilinen bir gerçek. Ancak özellikle 1980 öncesinde dünyaya gelmiş olan ve 'dijital göçmen' olarak tanımlanan yetişkin bireyler, hayatlarının ilerleyen yaşlarında dijital teknolojilerle tanıştıkları için bu sürece uyum sağlama konusunda birtakım sorunlar yaşayabiliyorlar.

Dijital Göçmenler için Dijital Yeterlilikler Rehberi'nin amacı dijital göçmenlerin dijital teknolojilere erişme, kullanma, dijital içerikleri seçme ve değerlendirme, içerik üretme, güvenlik, problem çözme gibi konularda bilinçli farkındalık kazanmalarını ve farkındalıklarının artırılmasını sağlamak; dijital yeteneklerinin gelişimine katkıda bulunmaktır.

- Dijital teknolojileri kendi ihtiyaçlarımı ve çocuklarımın ihtiyaçlarını karşılayacak düzeyde kullanabiliyor muyum?
- Bu teknolojilerin sunduğu olanaklardan ve fırsatlardan yeterince yararlanabiliyor muyum?
- Bu teknolojilerin taşıdığı risklerin farkında mıyım?
- Dijital vatandaş olarak sorumluluklarım neler?

Dijital Göçmenler için Dijital Yeterlilikler Rehberi, bu soruların cevaplarını bulmada sizlere yardımcı olacak bir kaynaktır. Rehberin birinci bölümünde gündelik hayatta en çok ihtiyaç duyulan ve en sık kullanılan kavram ve uygulamalar hakkında kısa bilgiler verilecek. Başlangıç düzeyindeki bu bilgiler sizlere dijital dünyanın kapılarını aralama fırsatı sunacak. "Dijital Teknolojilerin ve İnternetin Sunduğu Olanaklar" başlıklı ikinci bölümde dijital teknolojilerin ve internetin sunduğu, gündelik hayatı kolaylaştıran ve zenginleştiren olanaklar anlatılacak. "Dijital Teknolojilerin ve İnternetin Taşıdığı Riskler" isimli üçüncü bölümde dijital teknolojilerin ve internetin barındırdığı olası riskler ve tehlikeler açıklanacak. "Dijital Teknolojilerin ve İnternetin Gerektirdiği Sorumluluklar" başlıklı dördüncü bölümde dijital teknolojileri ve interneti kullanmanın gerektirdiği sorumluluklar anlatılacak. Son bölümde ise dijital hayatta size yol gösterecek ve birtakım temel beceriler kazandıracak pratik öneriler sunulacak.

BAŞLARKEN...

Web Tarayıcı

Gündelik hayatın vazgeçilmezlerinden biri olan internetten yararlanabilmek için bir web tarayıcı kullanmanız gerekmektedir. Web tarayıcı, bilgisayarlar ve mobil cihazlarda (akıllı telefon, tablet gibi) internet sitelerinin ziyaret edilmesine aracılık eden bir ara yüzdür. Yani internet sayfalarını görüntülemeyi sağlayan bir programdır. Web tarayıcısında yer alan adres çubuğuna bir internet sitesinin adresini (URL) yazarak o siteye erişim sağlayabilirsiniz.

Bugün en çok kullanılan web tarayıcıları Google Chrome, Firefox, Mozilla Microsoft Edge ve Opera; en yaygın kullanılan arama motorları ise Google, Yandex, Yahoo ve Bing'tir.

Arama Motoru

Ziyaret etmek istediğiniz bütün internet sitelerinin adreslerini bilemeyebilirsiniz ya da merak ettiğiniz herhangi bir konuda internetten bilgi edinmek isteyebilirsiniz. Bu noktada ihtiyaç duyduğunuz şey bir arama motoru. Arama motoru, internet üzerinde bulunan içeriği aramak için kullanılan bir mekanizmadır. Bir internet kullanıcısı arama motorunda arama yaptığında, kullanıcının aradığı şey ile en iyi eşleşen sonuçlar en kısa zamanda listelenir.

Arama motorları internet kullanıcıları tarafından çok sık kullanılırlar. Çünkü arama motoru sonuçlarını görmeden bir siteye doğrudan tıklayabilmek için o sitenin adresini bilmek ve adresi adres çubuğuna doğru yazmak gerekir. Oysa arama motoruna sitenin kısa adını yazsanız bile siteye kolaylıkla ulaşabilirsiniz. Ayrıca merak ettiğiniz, öğrenmek istediğiniz herhangi bir konuyla ilgili bir ya da birkaç anahtar sözcük yazıp arama motorunda arattığınızda konuyla ilgili sayısız bilgi ve içeriğe ulaşabilirsiniz.

E-Posta

E-mail ya da elektronik posta olarak da bilinen e-posta, internet üzerinden gönderilen dijital mektuptur. Diğer bir ifadeyle internet üzerinden bir kişiye veya bir grup kişiye gönderilen; metin, dosya, resim içerebilen bir mesajdır. Günümüzde geleneksel mektubun yerini alan e-posta, modern hayatın en çok kullanılan haberleşme yöntemlerinden biri olmuştur. Sadece elektronik posta göndermek için değil örneğin alışveriş sitelerine, sosyal medya sitelerine üye olmak, dijital bankacılık hizmetlerinden yararlanmak, internetten uçak bileti satın almak için de bir e-posta adresinizin olması gerekir.

E-postalar, bir e-posta adresinden başka bir e-posta adresine gönderilir. Bu nedenle birine e-posta gönderebilmek veya almak için bir e-posta adresinizin olması gerekir. E-posta adresi genellikle bir kişinin telefon numarası ya da açık ev adresi gibi internet üzerinde bulunan adresini ifade eder. Bu nedenle kişiye özeldir.

E-posta adresini bir e-posta servis sağlayıcısı üzerinden alabilirsiniz. Bunlar Gmail, Outlook, Yahoo Mail, Yandex Mail gibi ticari bir e-posta servisi olabileceği gibi, bir üniversitenin, kamu kurumunun, şirketin de kendi üyelerine sunduğu e-posta servisi olabilir.

E-posta adreslerinin başında kullanıcı adı bulunur, ardından e-posta servis sağlayıcının adı gelir. Örneğin isim.soyisim@gmail.com ya da soyisim@erciyes.edu.tr. Bir e-posta adresi almak için öncelikle bir e-posta servisinin internet sitesine girmeniz gerekiyor. “Hesap Oluştur” bölümünü tıklayarak açılan sayfada istenen bilgilerinizi girerek e-posta hesabı açabilirsiniz. Hesap açarken kendinize bir kullanıcı adı ve şifre belirlemeniz gerekiyor. Kullanıcı adı seçmekte özgürsünüz; ancak adınız ve soyadınız, adınızın baş harfi ve soyadınız, sadece soyadınız gibi sizin kimliğinizi yansıtan bir kullanıcı adı seçmeniz daha doğru olur. Ayrıca kolay tahmin edilemeyecek, büyük ve küçük harf, rakam ve sembollerden oluşan güçlü bir şifre belirlemeniz de hesap güvenliğiniz açısından faydalı olacaktır.

türkiye.gov.tr
"Devletin Kısayolu"

DEVLETİN KISA YOLU
e-Devlet KAPISI

e-Devlet

Elektronik devlet ya da kısa adıyla e-devlet, devlet kurumları tarafından vatandaşlara verilen kamu hizmetlerinin elektronik ortamda sunulmasıdır. e-Devlet uygulamasının amacı bilgi ve iletişim teknolojilerini kullanarak kamu hizmetlerinin vatandaşlara kolay ve etkin yoldan, kaliteli, hızlı ve güvenli bir şekilde ulaştırılmasıdır. Ayrıca devlet yönetiminin ve kamu hizmetlerinin şeffaf bir şekilde yürütülmesi, vatandaşların yönetime katılabilmeleri de olanak sağlar.

e-Devlet uygulamasının başarılı olabilmesinin temel koşullarından biri, vatandaşların bilgi ve iletişim teknolojileri yoluyla sunulan hizmetlere erişilebilmesidir. Bunun için internet ve internete bağlanabilecek bir cihaza sahip olmanın yanı sıra belirli düzeyde dijital beceriye sahip olmak da gerekmektedir.

e-Devlet uygulamasıyla kamu kurumları, belediyeler, üniversiteler ve firmalar tarafından sunulan yüzlerce hizmetten yararlanmak mümkün. Bu hizmetlerden bazıları şunlar;

- Mahkeme dava dosyası sorgulama
- Adli sicil kaydı sorgulama ve belge doğrulama
- Vergi borcu sorgulama ve ödeme
- Araç sorgulama
- Sürücü belgesi ceza puanı sorgulama
- TÜVTÜRK araç muayenesi randevusu alma
- Maaş ve emeklilik bilgileri sorgulama
- Askerlik bilgileri sorgulama
- HES kodu alma
- Mobil hat sorgulama
- Mezuniyet belgesi sorgulama ve doğrulama
- Öğrenci belgesi ve transkript belgesi sorgulama
- Elektrik, su, telefon ve doğalgaz faturası sorgulama

e-Devlet sistemine giriş yapabilmek için e-devlet şifresine sahip olmanız gerekmektedir. e-Devlet şifrenizi PTT Merkez Müdürlüklerinden şahsen başvuruyla, üzerinde T.C. Kimlik numaranızın bulunduğu kimliğinizi ibraz ederek temin edebilirsiniz. e-Devlet üzerinden verilen hizmetler yüksek güvenlik seviyesi gerektirdiğinden, şifreler başvuru sahipleri için özel olarak oluşturulmaktadır. Bu nedenle ancak kimlik ibrazı ve şahsen başvuru ile şifreler verilmektedir. e-Devlet şifresinin yanı sıra mobil imza, e-imza, internet bankacılığı ve T.C. kimlik kartı uygulamasıyla da e-Devlet sistemine girmek mümkün.

e-Devlet'e **www.turkiye.gov.tr** internet sitesi ile giriş yapabilirsiniz. Girdiğiniz internet adresinin başında mutlaka "asma kilit" simgesinin ya da "https" ifadesinin yer aldığından emin olmalısınız. www.turkiye.gov.tr internet sitesine girdikten sonra açılan ekranda "Giriş Yap" butonuna tıklayıp giriş seçeneklerinden hangisini (e-Devlet şifresi, mobil imza, vb.) kullanacaksanız onu seçerek sisteme giriş yapabilirsiniz. Giriş yaptıktan sonra ekranda yer alan menüyü ya da arama kutucuğunu kullanarak istediğiniz işleme erişim sağlayabilirsiniz.

www.turkiye.gov.tr adresinin yanı sıra akıllı telefonunuza veya tabletinize e-Devlet uygulamasını indirerek de sisteme girebilirsiniz. Mobil e-Devlet uygulamasına da e-Devlet şifreniz ya da mobil imzanız ile giriş yapabilirsiniz.

e-nabız
Kişisel Sağlık Sistemi

e-Nabız

e-Nabız sağlık kuruluşlarından toplanan sağlık verilerine vatandaşların ve sağlık profesyonellerinin internet ve mobil cihazlar üzerinden erişebilecekleri bir uygulamadır. Muayene, tetkik ve tedavilerinizin nerede yapıldığına bakılmaksızın, tüm sağlık bilgilerinizi yönetebildiğiniz, tıbbi özgeçmişinize tek bir yerden ulaşabildiğiniz bir kişisel sağlık kaydı sistemidir. Bizzat sizin verdiğiniz, süresi ve sınırı belirlenmiş yetki çerçevesinde sağlık kayıtlarınızın hekimlerce değerlendirilebildiği, böylelikle teşhis ve tedavi sürecinin kalitesini ve hızını artıran, sizinle hekiminiz arasında güçlü bir iletişim ağının kurulmasını sağlayan, internet üzerinden güvenli bir şekilde erişebildiğiniz bir sağlık bilişim alt yapısıdır.

e-Nabız sistemine e-Devlet üzerinden e-Devlet şifresi, e-imza veya mobil imzanızı kullanarak T.C. numaranızla giriş yapabilirsiniz. e-Devlet şifreniz yoksa Sağlık Bakanlığı'na kayıtlı aile hekiminize cep telefonu numaranızın kaydını yaptırarak, telefonunuza gelecek kısa mesaj (SMS) ile size iletilen tek kullanımlık erişim kodunu kullanarak sisteme giriş yapabilirsiniz.

e-Nabız sistemiyle online hastane randevusu alabilir, hem kendinizin hem de çocuklarınızın geçmiş muayene bilgilerine, reçetelerinize, ilaçlarınıza, raporlarınıza, tahlil ve tıbbi görüntüleme sonuçlarınıza ulaşabilir; size ait sağlık bilgilerinin aile hekiminiz ve diğer hekimler tarafından görülüp görülemeyeceğine karar verebilirsiniz. Ayrıca gittiğiniz sağlık tesisini ve hekimi hizmet kalitesi açısından değerlendirilebilir ve yorum yapabilirsiniz.

İnternet Bankacılığı (Dijital Bankacılık)

Dijital teknolojilerin ve internetin yaygın kullanımıyla birlikte en çok tercih edilen dijital hizmetlerden biri de internet bankacılığıdır. Banka müşterilerinin para transferi, kredi kullanma, yatırım işlemleri, kredi kartı işlemleri, fatura ve vergi tahsilatı gibi bankacılık hizmetlerini internet üzerinden gerçekleştirmesine imkân tanıyan internet bankacığı hem bankalar hem de müşteriler açısından büyük kolaylıklar sağlamaktadır.

https (http secure): Secure Hyper Text Transfer Protocol kelimelerinin baş harflerinden oluşan "https" Türkçe Güvenli Hiper Metin Aktarım İletişim Protokolü anlamına gelmektedir. İsminin başında "https" bulunan web siteleri, güvenlik sertifikasına sahip olduğu için bu sitelerde bilgileriniz olası güvenlik sorunlarına karşı korunmaktadır.

Adres satırının yanında asma kilit simgesi olmayan sitelere herhangi bir hassas bilgi (banka bilgileri, kredi kartı bilgileri, T.C. kimlik numarası gibi) girmeyin.

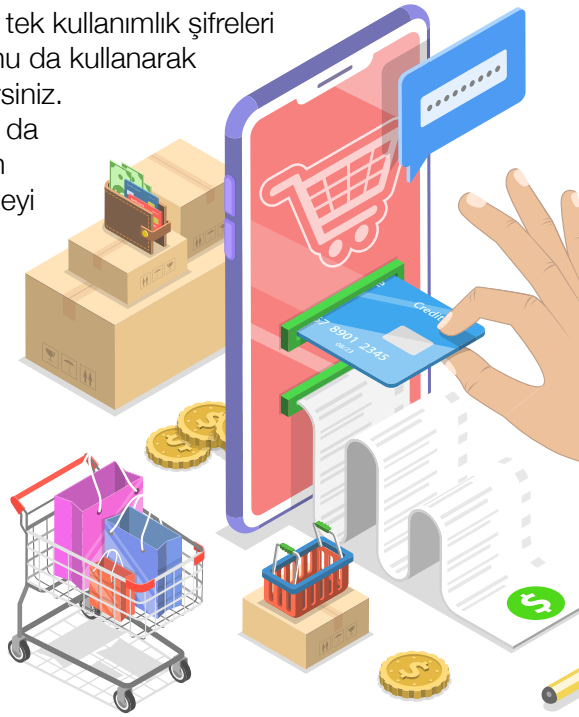
Güvenli

Bilgi veya Güvenli değil

Güvenli değil veya Tehlikeli

Hesabınızın olduğu bankanın internet sitesine ya da mobil uygulamasına girerek size sunulan hizmetlerden yararlanabilirsiniz. Bunun için öncelikle internet bankacılığı şifrenizin olması gerekmektedir. İnternet bankacılığı şifresini banka şubesinden, bankanın internet sitesinden, mobil uygulamasından, çağrı merkezinden ya da ATM'den alabilirsiniz.

İnternet bankacılığının sunduğu kolaylıkların yanı sıra birtakım riskleri de bulunmaktadır. Yetersiz güvenlik önlemleri nedeniyle hesap ve kredi kartı bilgilerinin çalınması sonucunda maddi kayıplar yaşanabilmektedir. Bu durumu önlemek için bankaya ait internet sitesi adresinin doğru olduğundan ve girdiğiniz internet adresinin başında mutlaka asma kilit simgesinin ya da "https" ifadesinin yer aldığından emin olmalısınız. Eğer mobil cihazınızdan bankacılık işlemlerinizi gerçekleştireceksiniz bankanızın kendi uygulamasını cihazınıza indirerek mobil uygulama üzerinden giriş yapmanız çok daha güvenli olacaktır. Bankanızın internet sitesine ve mobil uygulamasına giriş yaparken kullanmak üzere kolay tahmin edilemeyecek, güçlü bir şifre belirlemeli; şifrenizi başka sitelerde kullanmamalı, kimseyle paylaşmamalısınız. Bankanız tarafından kısa mesajla gönderilen tek kullanımlık şifreleri ya da doğrulama kodunu da kullanarak güvenliğinizi sağlayabilirsiniz. İşleminiz bittikten sonra da "Hesabım" bölümünden güvenli çıkış yaparak siteyi ya da uygulamayı kapatmalısınız. Bunların yanı sıra cihazınızın virüslere ve kötücül yazılımlara karşı korunması için antivirüs programı kullanmalı, tarayıcınızın ve işletim sisteminizin güncellemelerini zamanında yapmalısınız.



Çevrim İçi Alışveriş

İnternetle birlikte kullanıcılara sunulan önemli bir hizmet de çevrim içi alışveriştir. E-ticaret siteleri üzerinden her türlü ürün ve hizmetin satışı yapılabilmekte, müşteriler bu ürün ve hizmetleri kredi kartı, havale, EFT ve kapıda ödeme gibi yöntemlerle satın alabilmektedirler. Ürünlerin müşterilere kargo ile gönderildiği bu sistemin hem satıcılar hem de alıcılar açısından sunduğu pek çok kolaylık ve avantaj bulunmaktadır. Özellikle Covid-19 pandemisinde marketleri ve alışveriş merkezlerini virüs açısından güvenli bulmayan milyonlarca insan giyimden temizlik ürünlerine, yemekten teknolojik cihazlara kadar birçok ürünü internetten ve mobil uygulamalardan sipariş vermiştir.

Kullanıcılara alışveriş için zaman harcamadan, dilediği saatte, oturduğu yerden alışveriş yapma imkânı sunan çevrim içi alışverişin de birtakım riskleri vardır. Banka ve kredi kartı bilgilerinin çalınması, sahte ya da yanlış ürün gönderilmesi bu risklerden bazıları. Güvenli bir çevrim içi alışveriş gerçekleştirebilmek için öncelikle cihazınızın virüslere ve kötücül yazılımlara karşı korunması adına antivirüs programı kullanmalı, tarayıcınızın ve işletim sisteminizin güncellemelerini zamanında yapmalısınız. Güvenilir e-ticaret sitelerinden alışveriş yapmalı, sitenin SSL sertifikası olup olmadığını kontrol etmelisiniz. Hakkında bilgi sahibi olmadığınız veya daha önce alışveriş yapmadığınız alışveriş siteleriyle ilgili arama motorlarında ön araştırma yapabilir, site ve ürün hakkında kullanıcı yorumlarını okuyabilirsiniz. İnternet adresinin başında asma kilit simgesinin ya da "https" ifadesinin yer alıp almadığını kontrol etmelisiniz. Eğer alışveriş sitesinin mobil uygulaması varsa bu uygulamayı Google Play Store, App Store gibi uygulama mağazalarından cihazınıza indirerek mobil uygulama üzerinden daha güvenli bir alışveriş yapabilirsiniz. Ödeme aşamasında kredi kartıyla ödeme yapmak yerine havale, EFT ya da kapıda ödeme seçeneklerinden birini tercih edebilirsiniz. Kredi kartıyla yaptığınız alışverişlerde varsa 3D Secure (güvenli ödeme) ile ödemeyi tercih etmeli, kredi kartı bilgilerinizin site tarafından kaydedilmediğinden emin olmalısınız.

SSL Sertifikası: SSL sertifikası bir web sitesinin kimliğini doğrulayan ve şifreli bir bağlantı sağlayan dijital bir sertifikadır. SSL sertifikaları kredi kartı bilgilerinizi e-ticaret sitesinin ödeme sayfasına yazdığınızda, bilgilerinizin özel bir şifreleme yöntemi kullanılarak bankanıza gönderilmesini sağlar.

3D Secure: 3 boyutlu güvenlik anlamına gelen 3D Secure banka ve kredi kartı bilgilerinin kopyalanması, çalıntı kart kullanımı gibi internet alışverişlerinde sıklıkla karşılaşılan dolandırıcılık yöntemlerinin engellenmesi amacıyla geliştirilmiş güvenli ödeme sistemidir. Çevrim içi alışverişlerde ödeme aşamasında kart bilgileri girildikten sonra 3D Secure ekranına yönlendirilirsiniz. Burada kart sahibinin cep telefonuna kısa mesaj yoluyla banka tarafından tek kullanımlık bir şifre gönderilir. Kısa bir süre için geçerli olan bu şifre, kart sahibinin dışında başka bir kişiye gönderilemez. Bu sayede kartın, kart sahibinin rızası olmadan kullanılması engellenir. Gelen şifre 3D Secure işlem ekranında istenen alana girilir, böylece kart sahibi kimliğini doğrulamış olur. Şifre zamanında ve doğru girilip onay verilmediği taktirde ödeme gerçekleşmez. Yani kart sahibi dışında kimse ilgili ödemeyi gerçekleştiremez.

Sosyal Medya

Sosyal medya, kullanıcıların kendi ürettikleri içerikleri yayınladıkları ve paylaştıkları online bir ağdır. Sosyal medya siteleri, kullanıcılarına diğer kullanıcılar ile iletişim ve mesajlaşma, resim, video, haber, ses, yorum vb. içerik paylaşma; paylaşılan içeriği hem izleyebilme hem de hızlı bir şekilde içeriğe yorum yapma imkânı sunarlar. Bugün geldiğimiz noktada sosyal medya, sosyalleşme ve paylaşımın yanı sıra reklamcılık, halka ilişkiler, pazarlama, alışveriş, habercilik, sivil toplum hareketleri gibi çeşitli alanlarda da etkin olarak kullanılmaktadır. Facebook, YouTube, Instagram, TikTok, Twitter Türkiye'de ve dünyada en çok kullanıcısı olan sosyal medya sitelerinden bazılarıdır.

Sosyal medya sitelerine girerek veya sosyal medya uygulamalarını mobil cihazınıza indirerek bir sosyal medya hesabı açabilirsiniz. Açılan sayfa ya da uygulamada "Kaydol"u tıkladıktan sonra sizden istenen isim soyisim, doğum tarihi, cep telefonu numarası gibi bilgileri girerek kayıt yaptırabilirsiniz. Bu aşamada ya da bir sonraki adımda sizden bir şifre belirlemeniz istenecektir. e-Devlet, internet bankası gibi yüksek güvenlik gerektiren site ve uygulamalarda kullandığınız şifreleri sosyal medya hesaplarınızda kullanmamalı, hatta her hesabınız için farklı şifreler belirlemelisiniz.

Dijital Teknolojiler ve İnternetle İlgili Temel Bilgi ve Beceri Düzeyinizi Test Edin!

Bir dijital cihazı (bilgisayar, tablet, akıllı telefon, vb.) ihtiyaçlarım doğrultusunda rahatlıkla kullanabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

Bir cihaza program veya uygulama yükleyebilirim.

☐ Evet ☐ Hayır ☐ Kısmen

Cihazımı güvenli bir wi-fi ağına bağlayabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

İnternet sitelerini bulmak ve kullanmak için bir web tarayıcı açabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

Arama motorlarını kullanarak internette çeşitli bilgilere ulaşabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

Cihazımla ve internetle ilgili basit teknik sorunları kendim çözebilirim.

☐ Evet ☐ Hayır ☐ Kısmen

Bir e-posta hesabı açabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

E-posta, Whatsapp, Telegram gibi mesajlaşma uygulamalarını kullanarak başkalarıyla dijital olarak iletişim kurabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

Bir sosyal medya platformunda hesap açabilirim ve hesabımı yönetebilirim.

☐ Evet ☐ Hayır ☐ Kısmen

Sosyal medya platformlarında paylaşım yapabilirim (mesaj, fotoğraf, video gibi).

☐ Evet ☐ Hayır ☐ Kısmen

Bir ebeveyn olarak çocuğuma internet ve dijital cihazlarla ilgili konularda yardımcı olabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

"Evet" cevabı 2 puan, "Kısmen" cevabı 1 puan, "Hayır" cevabı 0 puan.

Verdiğiniz cevapların puanlarını toplayın. Toplam puanınız **0-7** arasındaysa dijital teknolojiler ve internetle ilgili temel bilgi ve beceri düzeyiniz düşük. Toplam puanınız **8-15** arasındaysa dijital teknolojiler ve internetle ilgili temel bilgi ve becerileriniz orta düzeyde. Toplam puanınız **16-22** arasındaysa tebrikler! Dijital teknolojiler ve internetle ilgili temel düzeyde bilgi ve beceriye sahipsiniz.

DİJİTAL TEKNOLOJİLERİN VE İNTERNETİN SUNDUĞU OLANAKLAR

Hayat Boyu Öğrenme ve Bireysel Gelişim

Dijital teknolojiler ve internet, kendinizi sürekli geliştirmenizi sağlayacak bilgilere hızlı bir erişim imkânı sağlar. Dijital teknolojiler sayesinde kişisel gelişim, yabancı dil, meslek hayatı gibi pek çok alanda yazılı ve görsel bilgiye ulaşabilir ve kendinizi geliştirebilirsiniz.

Bilgiye Erişim ve İşlevselleştirme

Dijital teknolojiler ve internet bilgiye erişiminizi hızlandırmakla kalmaz, ulaştığınız bilgileri günlük hayatınızda kullanabilmenizi de destekler. Haberlerden yemek tariflerine kadar geniş bir çerçevedeki bilgiye internet sayesinde hızlıca erişebilir ve bu bilgileri günlük hayatınızda işlevsel bir şekilde kullanabilirsiniz.

Ağ Toplumuna Entegrasyon

İnternet kullanımının yaygınlaşması ile tüm dünya toplumları birer ağ toplumuna dönüşüyor. Kısacası, internet ve ağa bağlı olmak bir çeşit kimlik kartı gibi artık. Bağlı değilseniz yoksunuz. Bu sebeple, internet ağ toplumuna entegrasyon olanağı da sunuyor hepimize. Tabii, yetkin bir şekilde kullanabilirsek…

İletişim ve Paylaşım

Covid-19 salgını sürecinde gördük ki, internet güçlü ve çeşitli iletişim olanakları sunuyor. Artık çok kolay bir şekilde, kilometrelerce uzakta olan torunlarınızla, çocuklarınızla görüntülü görüşmeler yapabilir, hatta aynı evin salonundaymışçasına eşzamanlı olarak televizyon izleyebilirsiniz. Uzakta olan sevdiklerinizle durumunuzu kolayca paylaşabilirsiniz.

Anlık Mesajlaşma Uygulamaları: Kullanıcılarının birbirlerine herhangi bir gecikme olmadan, anlık olarak mesaj gönderebildikleri uygulamalardır. Günümüzde en yaygın kullanılan anlık mesajlaşma uygulamalarından bazıları WhatsApp, Telegram ve BİP'tir.

Sosyalleşme

Dijital teknolojiler ve internet sayesinde gerçek hayatta tanıdığınız ya da tanımadığınız insanlarla ve gruplarla iletişim kurabilir, sosyal çevrenizi genişletebilirsiniz. Sosyal medya, anlık mesajlaşma programları, internet forumları gibi ortamlarda akrabalarınızla etkileşim kurabilir, yıllardır görmediğiniz çocukluk arkadaşınıza ulaşabilir, sizinle ortak zevk ve ilgi alanlarına sahip yeni insanlarla tanışabilirsiniz.

İnternet Forumları: Forumlar, web sayfaları halinde kullanıcıların herhangi bir konuda tartıştığı, soru sorduğu, çözüm aradığı veya bilgilendirmelerde bulunduğu bir tartışma platformu olarak tanımlanabilir. Bu sitelerde kullanıcılar, daha önce açılan konu başlıklarında yorumlar yapabilir ya da kendileri yeni başlıklar oluşturarak forumdaki diğer kullanıcıların bilgi ve deneyimlerine başvurabilirler.

İçerik Üretme ve Yayma

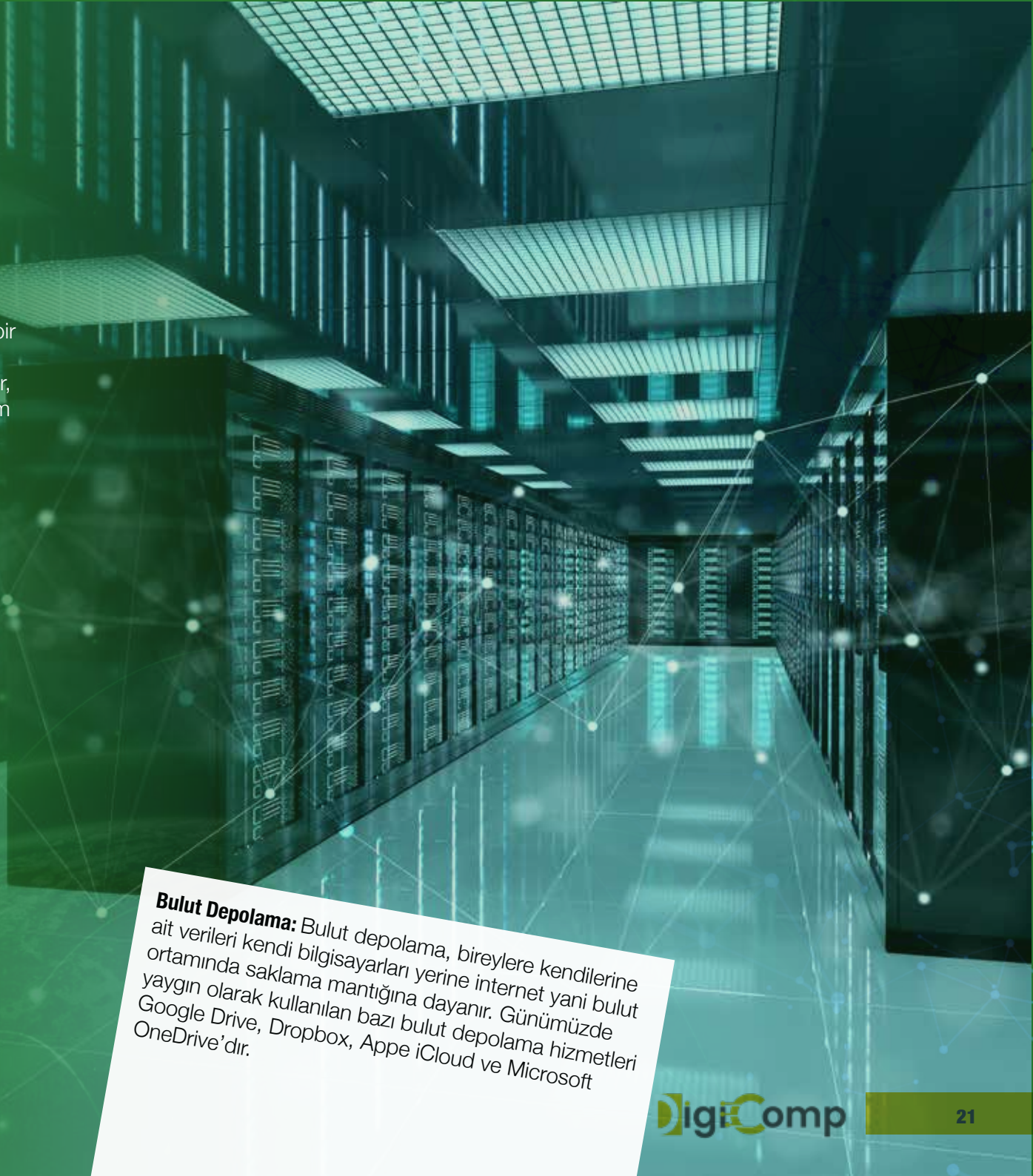
Gazete, televizyon ve radyodan farklı olarak internette siz de içerik üretebilirsiniz. Örneğin evinizdeki kırılan masanın ayağını tamir ettiğiniz videoyu ya da yaptığınız bir yemeğin videosunu internette paylaşabilirsiniz. Böylece hem yaptığınız şeyle başkalarına fikir ve ilham vermiş olur, hem de internette yer alan bu tip içeriklere ulaşarak ilham alabilirsiniz.

Veri Yedekleme

Artık anılarımızı salondaki vitrinin alt raflarından birinde duran, tozlu fotoğraf albümlerinde değil, dijital olarak bilgisayarlarda ve harici disklerde saklıyoruz. Anılarımızın dijitalleşmesi, onları daha sağlıklı saklama imkânı tanısa da depolanan cihazda yaşanacak herhangi bir aksaklık tüm fotoğraflarımızı kaybetme riski doğuruyor. İnternet, sağladığı bulut depolama hizmetleri sayesinde bu gibi önemli verilerimizi yedeklememizi ve onları korumamızı kolaylaştırıyor.

Kamu ve Özel Sektörün İnternet Temelli Hizmetlerinden Yararlanabilme

Adli sicil kaydı, vergi borcu ödeme, fatura ödeme, emeklilik işlemleri, market alışverişi… Yaklaşık 10-15 yıl önce bu işlemlerin hepsi, ayrı ayrı kurumlara giderek ve dakikalarca sıra bekleyerek gerçekleştiriliyordu. Günümüzde dijital teknolojiler ve internet sayesinde bu işlemlerin hepsini evinizin salonunda otururken gerçekleştirebilirsiniz.



Bulut Depolama: Bulut depolama, bireylere kendilerine ait verileri kendi bilgisayarları yerine internet yani bulut ortamında saklama mantığına dayanır. Günümüzde yaygın olarak kullanılan bazı bulut depolama hizmetleri Google Drive, Dropbox, Appe iCloud ve Microsoft OneDrive'dır.

Dijital Teknolojilerin ve İnternetin Sunduğu Olanaklardan Ne Kadar Yararlanıyorsunuz? Test Edin!

Yeni şeyler öğrenmek, araştırma yapmak ve gündemi takip etmek için internet kullanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Sosyal medya platformlarının en az bir tanesinde hesabım var.

☐ Evet ☐ Hayır ☐ Kısmen

Anlık mesajlaşma programlarını kullanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

İstediğim kişilerle görüntülü görüşme yapıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

e-Devlet sisteminde sunulan hizmetlerden yararlanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

e-Nabız sisteminde sunulan hizmetlerden yararlanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Kamu kuruluşlarının ve firmaların sunduğu elektronik hizmetlerden yararlanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

İnternet bankacılığını kullanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi alışveriş yapıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Bilgi ve belgelerimi cihazımda veya bulut depolama alanlarında saklayabileceğimi biliyorum.

☐ Evet ☐ Hayır ☐ Kısmen

"Evet" cevabı 2 puan, "Kısmen" cevabı 1 puan, "Hayır" cevabı 0 puan.

Verdiğiniz cevapların puanlarını toplayın. Toplam puanınız **0-6** arasındaysa dijital teknolojiler ve internetin sunduğu olanaklardan yeterince yararlanamıyorsunuz. Toplam puanınız **7-13** arasındaysa dijital teknolojiler ve internetin sunduğu olanaklardan orta düzeyde yararlanıyorsunuz. Toplam puanınız **14-20** arasındaysa dijital teknolojiler ve internetin sunduğu olanaklardan oldukça yararlanıyorsunuz.


Dijital teknolojilerin
sunduğu olanaklar
mesafeleri ortadan
kaldırır!

DİJİTAL TEKNOLOJİLERİN VE İNTERNETİN TAŞIDIĞI RİSKLER

İnternetin sunduğu olanaklar maalesef içerisinde birtakım riskleri de barındırıyor, hem de ciddiye alınması ve dikkatli olunmasını gerektirecek boyutta riskleri.

Temel Ağ Güvenliğini İlgilendiren Sorunlar

İnternet büyük bir ağ. Bu ağ aslında milyonlarca farklı ağın birleşiminden oluşuyor. Üstelik bu ağlar her yerdeler. Evinizde bir kablosuz modem kullanıyorsanız sizin de bir ağınız var demektir ve bu ağın güvenliğini sağlamamak ciddi riskler ortaya çıkarıyor. Örneğin, evinizde kullandığınız kablosuz modem üzerinden internete bağlanmak için kullandığınız şifre zayıf ya da kolay tahmin edilebilir bir şifreyse ağınız güvende değil demektir. Bu şifrenin başkaları tarafından bilinmesi, sizin internet hesabınız üzerinden, sizin modeminiz üzerinden alınan IP adresi ile bir siber suç işlenmesine, en iyi ihtimalle sizin internet kotanızın dolmasına neden olabilir.

IP Adresi: İnternete bağlanan her cihaz, belirli bir matematiksel sistem çerçevesinde kendine has bir numaralandırma sistemi olan IP adresi (Internet Protocol Address) alır. Bu adres bir bakıma internette gezinirken kullandığımız cihazların plakası olarak değerlendirilebilir. Bu adres, çoğu durumda değişkendir, ancak cihazınızın internete bağlanmak için kullandığı her bir IP adresi, internet servis sağlayıcılar tarafından kaydedilmektedir.

Profil: Sosyal medya siteleri üzerinde, bireylerin çoğunlukla kişisel bilgilerini kullanarak oluşturdukları, arkadaşlarının ya da sosyal çevrelerinin onlara ulaşmasını sağlayan kişisel sayfalardır. Örneğin Facebook profili, kullanıcılara isim, soyisim, fotoğraf, ilgi alanları, siyasi görüşü, cinsiyeti, politik görüşü, ilişki durumu gibi pek çok bilgiyi paylaşma şansı tanır.

Kişisel Verilerin Kötüye Kullanımı

Gerek sosyal medya profillerimiz için gerekse çevrim içi alışveriş siteleri için pek çok kişisel bilgiyi internet aracılığıyla paylaşıyoruz. Paylaşılan bu bilgiler veri tabanlarında toplanıyor, işleniyor ve kimi durumlarda da bu bilgiler başka birilerine satılıyor. Bu veriler çoğu zaman reklam ve tüketici profili oluşturulmak için kullanılsa da verilerin başka kişilerin eline geçmesi ve kötüye kullanılması riski de bulunuyor.

Online Dolandırıcılık ve Kimlik Hırsızlığı

Kişisel verilerin kötüye kullanılması ile ilişkili bir diğer konu da kimlik hırsızlığı ve online dolandırıcılık. Örneğin, sosyal medyada paylaştığınız fotoğraflara ve kişisel bilgilerinize ulaşan biri, size aitmiş gibi bir profil oluşturabilir ve sizmiş gibi davranmaya çalışabilir. Hatta kimi durumlarda kimliği çalınan bir kişi değil bir kurum da olabilir. Örneğin kötü niyetli kişi ya da kişiler bir bankanın internet sitesini kopyalayıp o bankanın internet şubesi izlenimi yaratarak banka hesap bilgilerinizi ele geçirebilir.

Hacklenme (Bilgisayar ya da Hesapların Başkaları Tarafından Ele Geçirilmesi)

Hacklenme, en açık ifade ile cihazınızın kontrolünü kaybetmeniz ya da cihazınızdaki verilerin kötü niyetli bir kişinin eline geçmesi olarak tanımlanabilir. “Hacker” olarak nitelendirilen kötü niyetli kullanıcılar çoğu zaman bu işi kullanıcıların dikkatsizliği ve bilinçsizliğinden faydalanarak gerçekleştirirler. Antivirüs yazılımları, hacklenme riskine karşı koruma sağlar. Bu programların yanı sıra bilinçli kullanım ve kolay tahmin edilemeyecek şifreler tercih etmek de gerekmektedir.

Oltalama (Yemleme)

Oldukça yaygın olan bir çevrim içi dolandırıcılık biçimi olan oltalama yönteminde, kötü niyetli kişiler size ödül, hediye gibi bir şey vaat ederek ya da sizi tehdit ederek bilgilerinizi ele geçirmeye çalışırlar. Örneğin e-posta adresinize gelen bir postada, cevap vermediğiniz takdirde e-posta hesabınızın kullanılamaz hale geleceği belirtilir ve bununla ilgili işlem yapmanız için sizinle bir link paylaşılır. Aynı yöntem cep telefonlarına gelen kısa mesajlarda da kullanılmaktadır. Bir teknoloji firmasından kazandığınız hediye cep telefonunu alabilmek için bir linke tıklamanız istenebilir. Bu linkleri açtığınızda ya da açılan sayfaya bilgilerinizi girdiğinizde kişisel bilgileriniz veya hesabınız çalınabilir, cihazınız kullanılamaz hale gelebilir.

Link: Bağlantı anlamına gelen link, internet sayfalarında kullanıcının başka bir web sayfasına, içeriğe ya da uygulamaya yönlenmesini sağlayan tıklanabilir köprü metni veya resimdir.

Siber Zorbalık

Siber zorbalık bireylerin başka bireyler tarafından dijital teknolojiler aracılığıyla eziyet, tehdit, taciz, hakaret, küçük düşürülme, utandırılma ve benzeri şekillerde hedef alınması durumunu ifade eden bir kavramdır. Siber zorbalığın pek çok görülme biçimi vardır: Mobil cihazlar aracılığıyla bireylerin görüntülerini izinleri olmaksızın çekip paylaşmak; diğer kullanıcılara sosyal medya ya da sohbet odaları gibi çevrim içi ortamlarda aşağılayıcı, alay edici, öfke dolu, kaba, cinsel taciz veya şiddet içeren mesajlar göndermek; birinin kişisel bilgilerini rızası ve haberi olmadan internet ortamında paylaşmak; sosyal ağlarda birisi hakkında dedikodu yaymak ya da özel hayatıyla ilgili konuları açık etmek; başkası adına sahte hesap açıp, onun kimliğine bürünmek; bir kişinin sosyal medyadaki paylaşımlarına sürekli olumsuz yorumlar yapmak... Kavram sıklıkla çocuklar ve ergenlerin internet kullanımlarındaki riskleri ortaya koymak için kullanılsa da yeterli bilince ve dijital beceriye sahip olmayan yetişkinler de siber zorbalığa maruz kalabilirler.

Siber zorbalık bir şiddet türüdür. Sanal ortamda gerçekleşmiş olması, ‘gerçek’ olmadığı anlamına gelmemelidir.

Kötücül Yazılımlar

Covid-19 salgınından korunmak için nasıl ki maske kullanıyor ve aşılarımızı yaptırıyorsak benzer şekilde internetteki kötücül yazılımlardan korunmak için de dijital ortamda bir maske ile dolaşmamız gerekiyor. Çünkü diğer risklerden farklı olarak bu riski fark etmek çok daha güç. Bilgisayarımıza ya da cep telefonumuza giren bir virüs, biz onu fark edene kadar bize ait pek çok bilgiye erişebilir ya da cihazımızı kullanılamaz hale getirebilir. Bu riske karşı en büyük silahımız ise bilinçli internet kullanımı ve antivirüs yazılımlarıdır.

Kötücül Yazılım: Bilgisayar yazılımları, kullanıcılara kimi işleri daha kolay yapma şansı tanıyan ve programcılar tarafından geliştirilen uygulamalardır. Kötücül yazılımlar ise kullanıcılara doğrudan ya da dolaylı yoldan zarar vermek için geliştirilen uygulamalardır. Kötücül yazılımlar çoğu zaman siz farkında olmadan bilgisayarlarınıza ya da cep telefonlarınıza yerleşirler. İnternette çok yaygın olan kötücül yazılımlar virüs, truva atı ya da solucan olarak adlandırılırlar. Kullanıcıların bu kötücül yazılımlardan kendilerini koruması için hem dikkatli olmaları hem de bu yazılımları fark edip engelleyecek programlar kullanmaları gerekmektedir.

Antivirüs Yazılımı: İnternette pek çok site, cihazlarınıza size fark ettirmeden yerleşebilecek kötücül yazılımlarla doludur. Bunu engellemek ve kullanıcıları korumak için antivirüs yazılımları geliştirilmiştir. Bu yazılımlar, virüslerin cihazlarınıza sızmasını engeller. Bu programlar, genellikle cihazdaki zararlı ya da zararlı olabilecek, bilgisayarınızdan sizin izniniz dışında bilgi sızdırabilecek yazılımları bulup yok etmekle görevlidirler.

Entelektüel Mülklere Karşı Suç İşleme

Sevdiğimiz eski bir Türk filmine ya da sevdiğimiz bir şarkıya kolayca erişebildiğimiz ya da onu indirip kendi cihazlarımızda saklayabildiğimiz bir çağdayız. Ancak bunu yaparken o filmi çekenlerin ve o şarkıyı üretenlerin haklarını ihlal etme ihtimalimiz çok yüksek. Üstelik bu ihlalin hukuki bir karşılığı da var. Yani bu konuda yeterince dikkat etmezsek ve hak sahipleri tarafından bir şikâyet gerçekleşirse ceza alabiliriz. Madalyonun diğer yüzü ise bizim özgün olarak ürettiğiniz içeriklerin kopyalanıp izinsiz bir şekilde çoğaltılması, dağıtılmasıdır. Bu nedenle internet üzerinde özgün bir içerik (örneğin yazdığımız bir şiir) paylaşırken çok dikkatli olmalıyız. Takma isim kullanmadan paylaşmalı ve olası bir hak ihlali durumu için ilk paylaşım yaptığımız tarihi not etmeliyiz. Çünkü özgün içeriğin bize ait olduğunu kanıtlamak zorunda kaldığımızda bu bilgilere ihtiyaç duyabiliriz.

Online Yırtıcılar/Avcılar

Bu risk başlığı, özellikle internet kullanmaya başlayan çocuklarımızı ilgilendiriyor. Online yırtıcılar, asıl amaçları başta küçük çocuklar ve gençler olmak üzere internet kullanıcılarını bir şekilde tuzağa düşürerek onları cinsel açıdan istismar etmeye çalışan kişilerdir. Sohbet odaları, anlık mesajlaşma uygulamaları, internet forumları, sosyal medya, cep telefonları ve hatta dijital oyunlar online yırtıcıların sahte hesaplar açarak diğer kullanıcılarla etkileşim kurdukları ortamlardır. Bu ortamlarda dikkat çekmeden kurbanlarıyla iletişime geçen online yırtıcılar; internet yoluyla özel ve mahrem fotoğrafların ve video görüntülerinin elde edilmesi, bunların yine internet ortamında yayınlanması, pornografik amaçla kullanılması, çocuklarla cinsel içerikli iletişim kurulması, çocuğun kamera karşısında cinsel içerikli davranışlarda bulunmaya ikna edilmesi gibi taciz ve istismar yöntemlerini kullanmaktadırlar.

Kendini İfade Etmede ve Sosyalleşmede Yetersizlik

Özellikle dijital dünyanın içine doğan çocuklar ve gençler çoğu zaman sadece çevrim içi araçlar ile sosyalleşiyor ve iletişim kuruyorlar. Ancak bu sosyalleşme biçimine yatkınlık kimi zaman çevrim dışı dünyada kendini ifade etme ve sosyalleşme güçlükleri ile sonuçlanabiliyor. Sosyal medyada iletişim kurmakta zorluk çekmeyen bireyler, yüz yüze iletişimde kendilerini ifade etmede yetersizlik hissedebiliyorlar. Sadece çevrim içi olarak sosyalleşebilen bireyler, yüz yüze iletişimde zorlanabiliyorlar. Hatta kimi durumlarda, düşük özsaygıları nedeniyle çevrim içi ortamda da yeterince sosyallik sağlayamıyor hem çevrim içi hem de yüz yüze iletişimde içine kapanık bireylere dönüşebiliyorlar.

Bilgisayar, cep telefonu ve internet tabanlı hizmetlerin aşırı kullanımı, çevrim dışı sosyalleşme faaliyetlerine zaman ayırmayı da zorlaştırabiliyor. Başka bir ifadeyle, bu teknolojilerin aşırı kullanımı bir süre sonra kendini ifade etme ve sosyalleşme güçlükleri yaratabiliyor.

Düşük Özsaygı

İnternet özellikle de sosyal medya, kullanıcıların gerçekte oldukları gibi değil "olmak istedikleri" gibi bir kimlik yaratmalarına ve sunmalarına imkân tanıyor. Sosyal medya fiziksel olarak kusursuz, özel ve iş hayatında başarılı, mutlu insanların, zengin hayatların, lüks ev ve arabaların gösterildiği sahte bir imaj dünyası aslında. Ancak çoğu insan bu dünyanın gerçek olduğunu zannediyor, başkalarının yaşadığı mükemmel hayatlar karşısında kendi hayatını sorguluyor ve mutsuz oluyor. Bu durum bireylerin kendilerini yetersiz hissetmelerine ve düşük özsaygıya yol açabiliyor. Ayrıca sosyal medyada çok takipçiye sahip olmak, beğeni (like) ve olumlu yorum almak da bireysel başarının bir parçası olarak görüldüğü için bunlara sahip olamamak da yetersizlik duygusunu ve düşük özsaygıyı pekiştiriyor.

Bağımlılık

İnternet ve ona bağlı diğer aktiviteler, farkında olmadan bireyleri bağımlı haline getirebilir. Bu bağımlılık, internete erişimin herhangi bir sebepten dolayı sınırlandığı ya da kesildiği bir anda kendini gösterir. İnternete bağlı olduğunuz zamanın kontrolünü kaybetme, günlük işleri ve sorumlulukları yerine getirmede zorlanmaya başlama, sosyal çevreden kopya ve sosyal izolasyon gibi durumlar internet bağımlılığının belirtileridir.

Doğru Bilgiye Erişememe

Günümüzde internet en önemli bilgi kaynaklarından biri haline geldi. Güncel haberleri, hava durumunu, hastalıkların tedavi yöntemlerini, çocuğumuzun ödev konusunu ve daha birçok bilgiyi internetten öğrenebiliyoruz. Ancak internet dünyası, bütün kullanıcıların içerik üretebildiği ve bu içeriklerin de denetlenmediği bir ortam olduğu için burada yer alan bilgi ve haberlerin bir kısmı maalesef doğru ve güvenilir değil. Ayrıca her gün internette onlarca bilgi ve habere maruz kalıyoruz ve bu bilgi yoğunluğu da neyin doğru neyin yanlış olduğu konusunda kafa karışıklığına neden oluyor. Bunun sonucunda ideolojik ve siyasi açıdan yanlış yönlendirilme, yanlış tedavi yöntemlerine başvurma, kaygı bozukluğu, güvensizlik duygusu gibi olumsuzluklar ortaya çıkabiliyor.

Dijital Teknoloji ve İnternet Kullanımıyla İlgili Risk Düzeyinizi Test Edin!

Çevrim içi ortamlarda tanımadığım insanlarla iletişim kurmakta sakınca görmem.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda tanımadığım insanlarla kişisel bilgilerimi paylaşmakta sakınca görmem.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda herkesin görebileceği şekilde fotoğraf ve video paylaşmakta sakınca görmem.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda kimliğimi gizleyerek/sahte kimlikle hareket etmeyi tercih ederim.

☐ Evet ☐ Hayır ☐ Kısmen

Gerçek hayatta benimsemediğim davranışları (küfür, hakaret, taciz, vb.) çevrim içi ortamlarda sergilemekten kaçınmam.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda gördüğüm tüm bilgileri ve içeriği, doğruluğunu sorgulamadan kabul ederim.

☐ Evet ☐ Hayır ☐ Kısmen

E-posta, SMS veya sosyal medya mesajlarıyla gönderilen linkleri hemen açarım.

☐ Evet ☐ Hayır ☐ Kısmen

Dijital cihazlarda ihtiyaç duyduğum program ve uygulamaları güvenli olup olmadığına bakmadan indiririm.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda kolay hatırlanabilir, basit şifreler kullanırım.

☐ Evet ☐ Hayır ☐ Kısmen

Farklı çevrim içi ortamlarda aynı şifreleri kullanırım.

☐ Evet ☐ Hayır ☐ Kısmen

Dijital cihazlarımda antivirüs program kullanma ihtiyacı duymam.

☐ Evet ☐ Hayır ☐ Kısmen

Başkalarına ait içerikleri çevrim içi ortamlarda kaynak göstermeden ve izinsiz kullanmakta sakınca görmem.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda yer alan film, müzik, kitap gibi içeriklere, yasal olmayan platformlardan ücretsiz erişirim.

☐ Evet ☐ Hayır ☐ Kısmen

Dijital cihazları ve interneti kullanım düzeyim sosyal ilişkilerimi olumsuz yönde etkiler.

☐ Evet ☐ Hayır ☐ Kısmen

Dijital cihazlar ve internet olmadan gündelik hayatıma devam edemem.

☐ Evet ☐ Hayır ☐ Kısmen

"Evet" cevabı 2 puan, "Kısmen" cevabı 1 puan, "Hayır" cevabı 0 puan.

Verdiğiniz cevapların puanlarını toplayın. Toplam puanınız **0-10** arasındaysa dijital teknoloji ve internet kullanımıyla ilgili risk düzeyiniz düşük. Toplam puanınız **11-20** arasındaysa dijital teknoloji ve internet kullanımıyla ilgili kısmen risk altındasınız. Toplam puanınız **21-30** arasındaysa dijital teknoloji ve internet kullanımıyla ilgili risk düzeyiniz oldukça yüksek!

DİJİTAL TEKNOLOJİLERİN VE İNTERNETİN GEREKTİRDİĞİ SORUMLULUKLAR

Dijital dünyanın bize sunduğu uçsuz bucaksız olanaklar ve bu olanakların arasına ustalıkla gizlenmiş olan risklere değindik. Dijital dünyadan sorun yaşamadan faydalanmak ve risklerden kaçınmak için kimi sorumluluklarımız bulunuyor. Gerçek hayatta vatandaş olarak devlete ve topluma karşı sorumluluklarımız olduğu gibi dijital dünyada da dijital vatandaşlığın getirdiği birtakım sorumluluklarımız var.

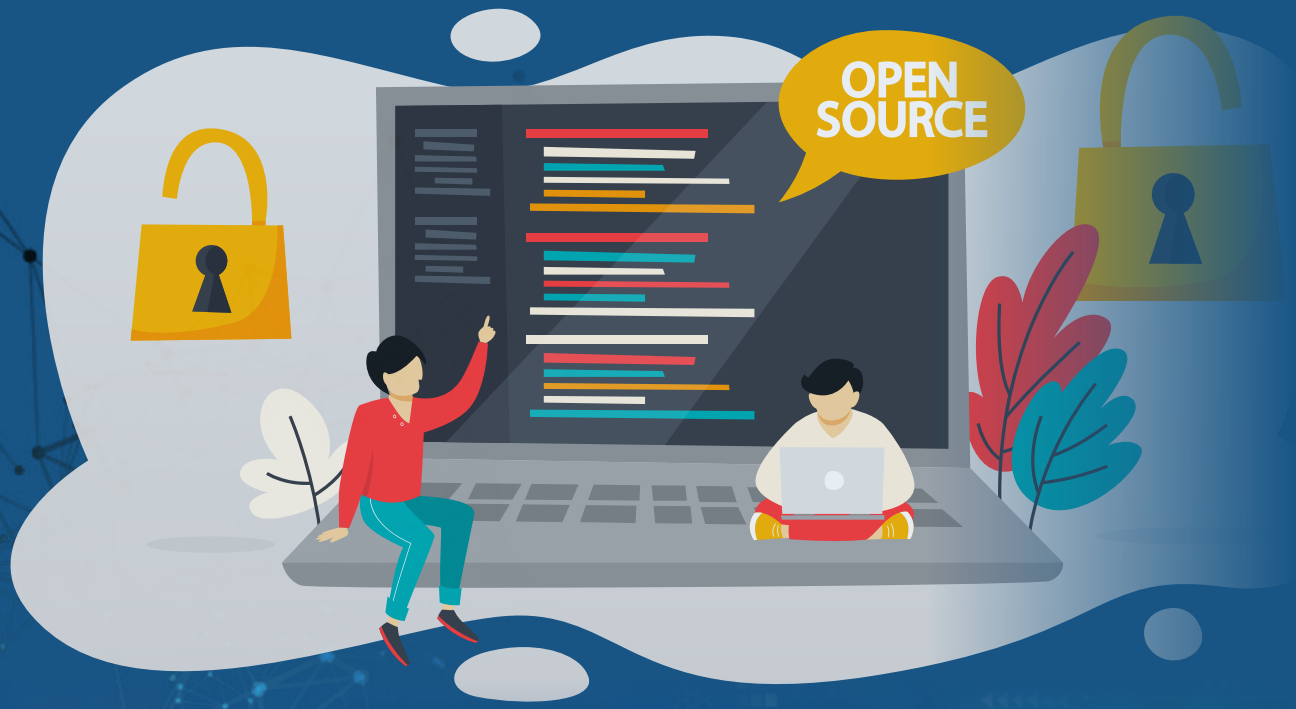
Kişisel Bilgileri Paylaşma Konusunda Bilinçli Olma

Sosyal medyada profil oluşturmak, bir alışveriş sitesinden bir şeyler almak ya da bir e-posta listesine kaydolmak için kimi kişisel bilgilerimizi internette paylaşırız. Bilgileri paylaştığımız siteler ya da kurumlar oldukça uzun bir gizlilik sözleşmesi ile bilgilerimizle neler yapacaklarını ya da yapamayacaklarını anlatırlar. Bu uzun metinleri okumak oldukça zahmetlidir ve çoğu zaman bu sözleşmelerle karşı tarafa bilgilerimizi işleme ve kimi durumda da başka kurumlarla paylaşma yetkisini veririz. Yeni yasal düzenlemeler (Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu), bu konuda doğabilecek hak ihlallerini önlemek için atılmış önemli bir adım olsa da kullanıcı olarak bizlere halen büyük sorumluluk düşmektedir. Güvenmediğimiz sitelere ve uygulamalara kişisel bilgilerimizi (isim soyadı, doğum tarihi, anne kızlık soyadı, TC kimlik numarası gibi) vermemek; sosyal medyada tanımadığımız kişilerle adres, telefon numarası gibi özel bilgilerimizi, görüntü ya da videolarımızı paylaşmamak bizim sorumluluğumuzdadır.

Telif Haklarına Riayet Etme

Bir filmi internetten ücretsiz izlemek ya da bir kitabı para vermeden bilgisayarımıza indirmek her ne kadar kulağa hoş gelse de bu eserlerin telif haklarına riayet etmek dijital vatandaş olarak bizlerin sorumluluğudur. Bin bir emekle ekip biçtiğimiz tarlamızdan bizim iznimiz olmadan birilerinin mahsullerimizi toplayıp tüketmesi hoşumuza gitmeyeceği gibi film, dizi, müzik, kitap gibi fikir eserlerinin herhangi bir bedel ödemeden izinsiz kullanılması da eser sahibinin hoşuna gitmeyecektir. Bu nedenle sahibi ya da üreticisi tarafından ücretsiz olarak herkesin kullanımına sunulmamış filmleri, dizileri, müzikleri, kitapları eser sahibine gerekli ödemeleri yapan yasal platformlardan izlemeli, dinlemeli, okumalı ya da indirmeliyiz. Ayrıca dijital ortamlarda başkaları tarafından paylaşılan ve bize ait olmayan video, fotoğraf, metin gibi içerikleri de izinsiz ve kaynak göstermeden bize aitmiş gibi kullanmamalı ya da paylaşmamalıyız.

Telif Hakkı: Bir fikir veya sanat eserini ya da bir bilgisayar yazılımını üreten kişinin ya da kurumun, bu eserden doğan haklarının hepsine telif hakkı denir.



Lisanslı Yazılım Kullanma

Telif hakları konusu sadece film, müzik, dizi gibi sanatsal üretimler için değil, dijital dünyanın bir parçası olan yazılımlar ve cep telefonu uygulamaları için de geçerli. Bu sebeple, o ürünü ortaya koyan, geliştiren kişilerin haklarını yememek için lisanslı yazılım kullanma sorumluluğumuz var. Lisanslı yazılımlara ödeme yapmak istemiyorsanız ya da buna ayıracak bir bütçeniz yoksa bile o yazılımları korsan bir şekilde kullanmak yerine ücretsiz açık kaynak kodlu alternatiflerini kullanmanız hem telif hakları açısından hem de cihazlarınızın güvenliği açısından daha doğru olur.

Açık Kaynaklı (Açık Kaynak Kodlu) Yazılım: Bilgisayar yazılımlarını basitçe yemek tariflerine benzetebiliriz. Açık kaynak kodlu yazılımlarda bu tarifler herkes ile paylaşılmakta ve herkesin katkı sağlamasına, değiştirmesine izin verilmektedir. Örneğin bir kek tarifindeki şeker miktarı, o tarifi kullanarak kek yapan kişiler tarafından kendi damak tatlarına ya da diyet durumlarına göre değiştirilebilir. Bu açıdan bakıldığında, açık kaynak kodlu yazılım, iş birliğine dayanır ve kaynak kodunu kullanmanın, değiştirmenin ve başkaları ile paylaşmanın esas alındığı bir program geliştirme yöntemidir.

Lisanslı Yazılım: Lisanslı yazılımlar ya da kapalı kaynak kodlu yazılımlar ise adından da anlaşılacağı gibi kaynak kodlarının ya da kendi örneğimizde olduğu gibi yemek tariflerinin kullanıcılarla paylaşılmadığı, özel mülkiyetli yazılımlardır. Bu yazılımları üreten programcılar ya da kurumlar bu programdan oluşan telif haklarına sahiptirler ve bu yazılımları kullanmak için satın almak ya da kiralamak, abone olmak gerekmektedir.

Siber Güvenliği Koruma Bilincine Sahip Olma

İnternet birbirine bağlı milyonlarca, hatta milyarlarca ağdan oluşmaktadır. Tüm gezegene yayılmış olan bu ağda yer alan tüm bireyler bu ağın güvenliği ile ilgili sorumluluklara sahiptir. Bizler, parçası olduğumuz ağın kırılganlığının bilincinde olarak, yapacağımız işlemler ile ilgili siber güvenliği koruma bilinciyle hareket etmek zorundayız. Siber güvenliğimizi sağlamak adına ziyaret ettiğimiz sitelerin ve yüklediğimiz uygulamaların güvenli olup olmadığını kontrol etmek, antivirüs programı kullanmak, dijital dolandırıcılık ve oltama amaçlı içerikler konusunda dikkatli ve bilinçli olmak, dijital ortamlardaki belge, fotoğraf ve videolarımızı güvenli bir ortamda yedeklemek; internete bağlandığımız cihazlara şifre koyarak yabancıların girişini engellemek, şifrelerimizi kimseyle paylaşmamak öncelikli olarak bizim sorumluluğumuzdadır.

Kullanılan Yazılım ve Antivirüs Programlarını Güncel Tutma

Kullandığımız otomobilleri belirli aralıklarla muayeneden geçirir ve durumlarını kontrol ettiririz. Muayeneden geçemeyen araçlar trafiğe çıkamazlar veya muayenesiz yakalandıklarında cezalandırılırlar. İnterneti de bu şekilde düşünebiliriz. İnternete bağlanmak için kullandığımız cihazları ve yazılımları da sürekli muayeneden geçirmeliyiz. Bunlar için yapılabilecek en kolay muayene ise bu cihaz ve yazılımları güncel tutmaktır. Özellikle antivirüs uygulamaları ortalama haftada bir güncellenme gereği duyarlar. Benzer şekilde, cep telefonu uygulamaları da fark edilen hatalar ya da kimi geliştirmeler için güncellenirler. Kullanıcılar olarak bizler, bu yazılımları sürekli güncel tutmakla sorumluyuz. Hem kendi siber güvenliğimiz için hem de çevremizdekilerin güvenliği için…

Dijital Ortamda Aldatıcı Bir Kimlik Kullanmama

Dijital ortamlarda gerçek kimliğimizin dışında başka bir isimle ve rumuzla hesap açmak, profil oluşturmak ve paylaşım yapmak mümkün. Kimi zaman internette özgürce dolaşabilmek ve istediğimizi yapabilmek adına başvurduğumuz bu yöntem, dijital dünyanın güvenliğini tehlikeye atan ve burada ortaya çıkabilecek olumsuzluklara zemin hazırlayan bir durum. Çünkü online dolandırıcılık ve hırsızlık, siber zorbalık, çocuk istismarı gibi eylemler çoğunlukla bu sahte kimlikler ve sahte hesaplar aracılığıyla gerçekleştirilmektedir. Dijital dünyanın daha güvenli ve şeffaf bir yer olabilmesi için burada aldatıcı kimlik kullanmamak, gerçek hayatta olduğu gibi kendi kimliğimizle yer almak hepimizin sorumluluğudur. Tabii bu durum, tüm mahremiyetimizden vazgeçip kişisel bilgilerimizi internette paylaşabileceğimiz anlamına gelmemeli.

Sosyal Medya ve Paylaşım Sitelerinde Başkalarına Karşı Sorumluluklar

Arkadaşlarımızla bir sohbet ortamında olduğumuzu varsayalım. O mekânda bulunan, tanımadığımız bir kişinin giydiği kıyafet ya da çay içme şekliyle ilgili iyi ya da kötü düşüncelerimizi onun duyabileceği bir şekilde ifade etmeyiz. Hatta çoğu durumda onu rahatsız etmemek için o tarafa bakmamayı tercih ederiz. Sosyal medyadaki etkileşimlerimizi de bu çerçevede düşünebiliriz. Sosyal medyada yüz yüze bir temasın olmaması ya da o kişinin bizi tanımaması, istediğimiz her şeyi özgürce söyleyebileceğimiz; kırıcı, yıpratıcı hatta siber zorbalığa varan boyutlarda yorumlar, mesajlar gönderebileceğimiz anlamına gelmez. Sosyal medyada da gerçek hayattaki gibi nezaket kurallarına uymalı, başkalarına karşı saygılı ve kibar davranmalı, iletişim kurduğumuz insanlarla empati yapmalıyız. Ayrıca ister tanımadığımız birisi isterse bir arkadaşımız ya da akrabamız olsun onlardan izin almadan fotoğraflarını, videolarını ve kişisel bilgilerini sosyal medyada paylaşmamalıyız.

Dijital Ebeveynlik

Dijital ebeveyn; dijital çağın gereksinimlerine göre hareket eden, temel düzeyde dijital araçlara hâkim, dijital ortamlardaki olanakların farkında olan ve çocuğunu bu ortamlardaki risklere karşı koruyabilen, kişi haklarına gerçek hayatta saygı duyulması gerektiği gibi sanal ortamda da aynı şekilde davranılması gerektiğini çocuğuna aşılayan ve teknolojik gelişmelere kendini kapatmayan bireydir. Dijital ebeveynlik çocukları ve gençleri dijital dünyada tamamen özgür bırakmak ya da tamamen kısıtlamak yerine onlara rehberlik etmek, yol göstermektir. Bunun için önce kendimizi bu alanda geliştirmeli, en az çocuğumuza yardımcı olacak ve yol gösterecek kadar dijital beceriye sahip olmalıyız. Okuma yazmayı bilmeden çocuğumuza okuma yazma öğretemeyeceğimiz gibi dijital okuryazar olmadan çocuğumuza dijital becerileri kazandıramayız.

Ayrıca birer dijital ebeveyn olarak her şeyden önce yukarıda anlatılan diğer sorumluluk alanlarının hepsinde temel düzeyde farkındalığa sahip olmalı ve bu bilinçle kendi çocuklarımızı dijital ortamlarda korumalı, doğru yönlendirmeliyiz. Nasıl ki çocuklarımızı toplumun bir parçası olacak şekilde bilinçli ve sorumlu bireyler olarak yetiştirmek bizlerin sorumluluğunda ise bu yeni ağ toplumu için onları bilinçli ve sorumlu bireyler olarak yetiştirmek de biz dijital ebeveynlerin sorumluluğudur.

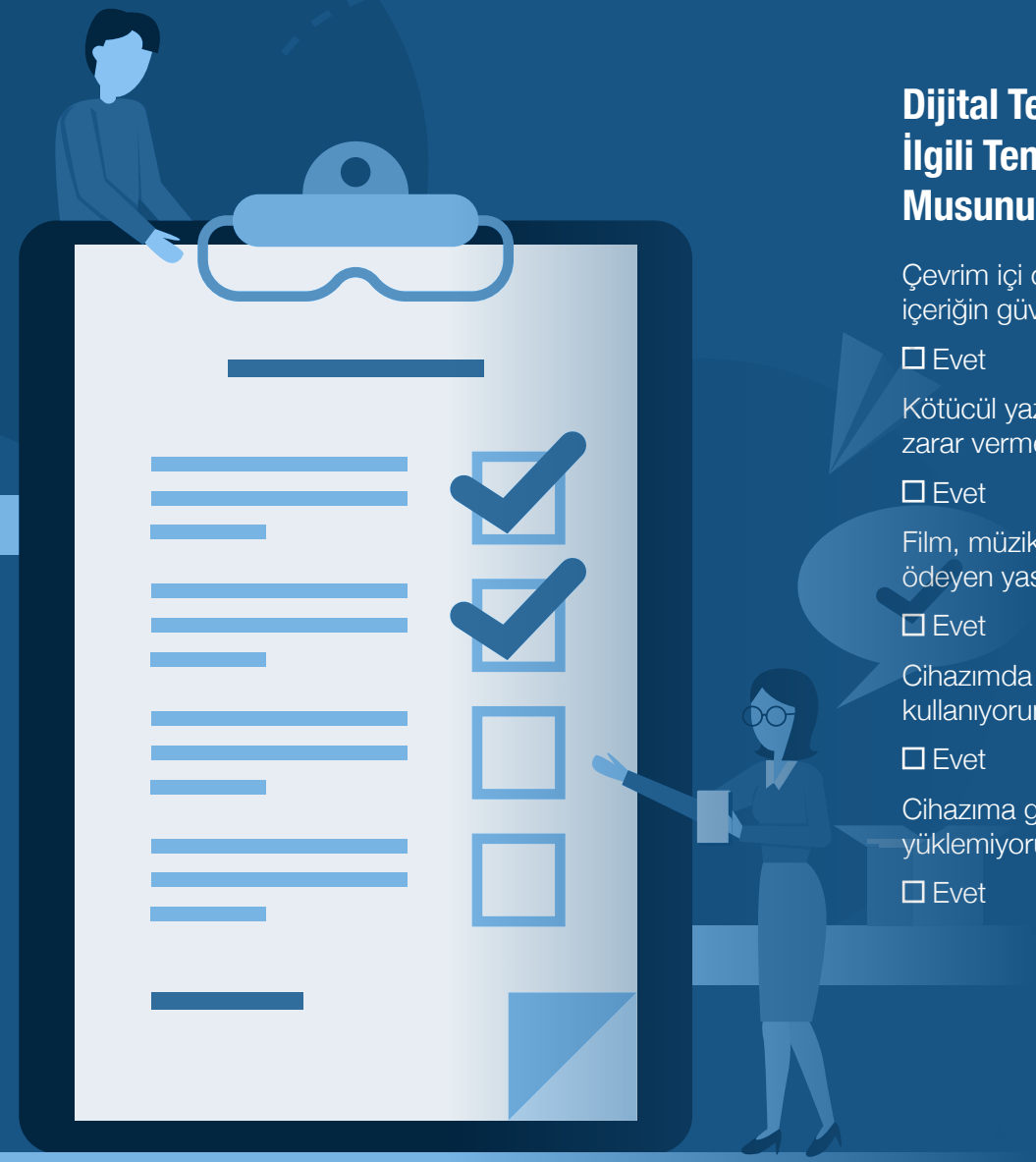
Bilinçli Bir Dijital Ebeveyn Olarak Neler Yapmalıyım?

- En az çocuğunuzu koruyacak kadar internet kullanmayı öğrenin.
- Teknoloji kullanımının olumlu ve olumsuz yanları hakkında bilgi sahibi olun ve bu konularda çocuğunuzda farkındalık oluşturun.
- Çocuğunuzun bilgisayar, cep telefonu, tablet gibi dijital cihazları kullanım kurallarını ve sürelerini onunla birlikte belirleyin.
- Dijital cihazların ve internetin kullanımına ilişkin onaylamadığınız davranışları, nedenleriyle birlikte çocuğunuza açıklayın.
- Çocuğunuzun çevrim içi faaliyetlerini kontrol edin, ne yaptığı ve neden yaptığı konusunda onunla sohbet edin.
- Çocuğunuzun ziyaret ettiği siteler ve oynadığı oyunlar hakkında bilgi edinin. Bunu suçlayıcı bir tavırla değil, keşfetmeye ve öğrenmeye çalışan bir arkadaşıymış gibi yapın.
- Çocuğunuzun ziyaret ettiği siteleri siz de ziyaret edin.
- Çevrim içi ortamlarda kimlerle görüştüğünü ve arkadaşlık ettiğini öğrenin.
- Dijital oyunlarda, sosyal medyada ya da diğer çevrim içi ortamlarda kendisine ve ailenize ait isim, adres, okul adı, telefon numarası, kredi kartı numarası gibi bilgileri paylaşmamasını söyleyin.
- Dijital oyunlarda, sosyal medyada ya da diğer çevrim içi ortamlarda kendisinin ve ailenizin fotoğraf ve video görüntülerini paylaşmaması gerektiğini ona anlatın.
- Çocuğunuzun, sosyal medya kullanıyorsa, profilinde hangi bilgileri paylaştığını kontrol edin.

Güvenli İnternet: İnternet servis sağlayıcıları tarafından ücretsiz olarak sunulan ve internetteki zararlı içeriklerden sizi ve ailenizi büyük oranda koruyan alternatif bir internet erişimidir. Güvenli internet hizmeti ücretsizdir, abonelik bir kısa mesaj (SMS) ile mümkündür ve program kurmaya gerek yoktur. Çocuk profili ve aile profili şeklinde iki farklı seçenek sunulmaktadır.

https://www.guvenlinet.org.tr adresinden bilgi alabilir, güvenli internete geçebilirsiniz

- Sosyal medya platformlarındaki gizlilik ayarlarını siz yapın. Profilini ve paylaşımlarını sadece tanıdığı kişilerin görebileceği şekilde ayarlayın.
- Sosyal medyada çocuğunuzla birbirinizi takip edin.
- Sosyal medyada tanımadığı kişilerin arkadaşlık istediğini kabul etmemesi gerektiğini ifade edin.
- Çocuğunuzun çevrim içi ortamlarda kullandığı şifreleri sizinle paylaşmasını sağlayın.
- Şifrelerini sizin dışınızda kimseyle paylaşmaması gerektiğini ona anlatın.
- Çocuğunuzu ve ailenizi kumar, intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu, sağlık için tehlikeli madde, fuhuş, müstehcenlik, ırkçılık, terör, şiddet gibi içeriklerden, zararlı yazılımlardan ve dolandırıcılık sitelerinden korumak için güvenli internet kullanın.
- Çocuğunuzun kullandığı cihazlara ebeveyn kontrol programı kurun. Bu tür programlar çocuğun cihaz kullanım süresini, etkinliklerini ve uygulamalarını denetlemenize olanak tanır, çocuğunuzun nerede olduğuna dair konum bilgisi sağlar.
- Gerçek hayatta olduğu gibi çevrim içi hayatta onu rahatsız eden, üzen kişileri, yaşadığı olumsuzlukları da sizinle rahatlıkla paylaşabileceği ve yardım alabileceği konusunda ona güven verin.
- Çocuğunuzun internet dışında sizinle ve arkadaşlarıyla zaman geçirmesine ve sosyal aktivitelere katılmasına imkân tanıyın.
- Çocuğunuzun bilgilerini, fotoğraflarını ve video görüntülerini paylaşırken onun mahremiyet ve kendi kaderini tayin hakkına saygı gösterin.



Dijital Teknoloji ve İnternet Kullanımıyla İlgili Temel Sorumluluklarınızı Biliyor Musunuz? Test Edin!

Çevrim içi ortamlarda gördüğüm bütün bilgilerin ve içeriğin güvenilir olmadığını biliyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Kötücül yazılımların (virüs, solucan, truva atı, vb.) cihazıma zarar vermemesi için antivirüs program kullanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Film, müzik, kitap gibi içeriklere, eser sahibine telif bedeli ödeyen yasal platformlardan erişiyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Cihazımda lisanslı programlar ve uygulamalar kullanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Cihazıma güvenilir olmayan program ve uygulamaları yüklemiyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda hangi bilgileri paylaşmam ve paylaşmamam gerektiğini biliyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda siber zorbalık içeren her türlü davranıştan uzak dururum.

☐ Evet ☐ Hayır ☐ Kısmen

Çevrim içi ortamlarda başkalarına ait bilgileri ve içerikleri izinsiz paylaşmam.

☐ Evet ☐ Hayır ☐ Kısmen

Uygunsuz içeriğe sahip (siber zorbalık, pornografi, çocuk istismarı, kumar, vb.) web sitesi ve sosyal medya hesaplarını nereye ve nasıl şikâyet etmem gerektiğini biliyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Web siteleri, uygulamalar ve hesaplar için güvenli ve birbirinden farklı şifreler kullanıyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Şifrelerimi, kredi kartı ve banka bilgilerimi dijital ortamlarda kimseyle paylaşmam.

☐ Evet ☐ Hayır ☐ Kısmen

Bir web sitesinin güvenli olup olmadığını anlayabilirim.

☐ Evet ☐ Hayır ☐ Kısmen

E-posta, SMS veya sosyal medya mesajlarıyla gönderilen ve güvenli olmayan linkleri açmamam gerektiğini biliyorum.

☐ Evet ☐ Hayır ☐ Kısmen

Bir ebeveyn olarak çocuğumu internet ve diğer dijital ortamlardaki tehlikelerden ve risklerden korumam gerektiğini biliyorum.

☐ Evet ☐ Hayır ☐ Kısmen

"Evet" cevabı 2 puan, "Kısmen" cevabı 1 puan, "Hayır" cevabı 0 puan.

Verdiğiniz cevapların puanlarını toplayın. Toplam puanınız **0-9** arasındaysa dijital teknoloji ve internet kullanımıyla ilgili temel sorumluluklarınız hakkında yeterince bilgi sahibi değilsiniz. Toplam puanınız **10-19** arasındaysa dijital teknoloji ve internet kullanımıyla ilgili temel sorumluluklarınız hakkında orta düzeyde bilgi sahibisiniz. Toplam puanınız **20-28** arasındaysa dijital teknoloji ve internet kullanımıyla ilgili temel sorumluluklarınız hakkında yeterli düzeyde bilgiye sahipsiniz.


DAHA İYİ VE GÜVENLİ BİR
DİJİTAL HAYAT İÇİN ÖNERİLER

- İnternette bulduğunuz her bilgiye güvenmeyin. Bilginin kaynağını sorgulayın, doğruluğunu farklı kaynaklardan kontrol edin.
- Çevrim içi ortamda paylaştığınız her şey sizi temsil eder ve gerçek hayatınızın bir parçasıdır.
- Her bir paylaşımınız dijital ayak izleri bırakır ve bu izler başkaları tarafından çeşitli amaçlarla kullanılabilir. Kötüye kullanma potansiyeli olan paylaşımlar yapmaktan kaçının. Gerçek hayatta yapmayacağınız hiçbir şeyi, internetteyken de yapmayın.

Paylaşmadan önce tekrar düşünün!

- Güvenmediğiniz sitelerde ve uygulamalarda kişisel bilgilerinizi (isim soyadı, doğum tarihi, anne kızlık soyadı, TC kimlik numarası gibi) paylaşmayın.
- Kredi kartı ya da banka hesap bilgilerinizi paylaşmayın.
- Şifrelerinizi kimseyle paylaşmayın.
- Hatırlayabileceğiniz güçlü şifreler oluşturun. “12345” gibi şifreler başkaları tarafından kolay tahmin edilebilir. Şifrelerinizde büyük ve küçük harf, rakam ve semboller kullanın.
- Şifreleriniz adınız, soyadınız, doğum tarihiniz gibi kolay tahmin edilebilir kişisel bilgilerinizi içermesin.
- Güvenilir alışveriş sitelerinden alışveriş yapın. Site güvenliğinden emin değilseniz havale, EFT ya da kapıda ödeme seçeneklerinden birini tercih edin.
- Güvenmediğiniz program ya da içerikleri bilgisayarınıza, tabletinize ya da akıllı telefonunuza indirmeyin.

Korsan Yazılım: Lisanslı ve telif hakkına sahip ücretli yazılımların izinsiz olarak, herhangi bir bedel ödemeden kullanılan haline denir. Yasadışı olan korsan yazılımlar güvenlik ve gizlilik riskleri taşımakta, lisanslı yazılımların sunduğu güncelleme ve teknik destek imkanlarından yararlanamamaktadırlar.

- Korsan yazılım kullanmayın.
- Sosyal medyada tanımadığınız kişilerle adres, telefon numarası, kimlik numarası gibi özel bilgilerinizi, görüntü ya da videolarınızı paylaşmayın.
- Başkalarının mahremiyet hakkına saygılı olun. İzni olmadan başkalarıyla ilgili fotoğraf, video gibi paylaşımlar yapmayın.
- Yorum yaparken sakin, saygılı ve kibar olun.
- Başkalarını rencide eden, aşağılayan, hakaret içeren, ırkçılığa ve ayrımcılığa neden olabilecek paylaşımlar yapmayın.
- Herhangi bir şeyi paylaşmadan, beğenmeden, iletmeden ya da yorum yapmadan önce mutlaka bunun gelecekte bir sorun olup olmayacağını düşünün.
- Size ait olmayan şeyleri kaynak göstermeden paylaşmayın.
- Oltalama amaçlı gönderilen e-posta ve mesajlardaki linkleri açmayın. Bunlar virüs, solucan, truva atı gibi kötücül yazılımlar içerebilir, cihazınıza zarar verebilir
- Kişisel fotoğraf, video ve belgelerinizi güvenli bir dijital ortamda yedekleyin ve depolayın.

Wi-Fi (Wireless fidelity): Kablosuz internet anlamına gelen Wi-Fi bilgisayar, tablet, akıllı telefon, akıllı televizyon, oyun konsolu gibi cihazların kablosuz biçimde internete ve birbirlerine bağlanmasını sağlayan teknolojidir.

Bluetooth: Yakın mesafesindeki bilgisayar, tablet, telefon gibi cihazların radyo frekansıyla yani kablosuz olarak birbirlerine bağlanmasını ve veri aktarımı yapabilmelerini sağlayan teknolojidir.

- İhtiyaç duymadığınız zamanlarda Wi-Fi ve Bluetooth uygulamasını devre dışı bırakın.
- Herkese açık ve güvenilir olmayan kablosuz internet (Wi-Fi) kaynaklarını kullanmamaya özen gösterin.
- Herkese açık ve güvenilir olmayan kablosuz ağlarda internet alışverişi ve bankacılık işlemleri yapmayın.
- Sosyal medya, WhatsApp gibi çevrim içi araçlardaki kişisel bilgileriniz için gizlilik ve güvenlik ayarları yapın.
- Cihazlarınızda lisanslı antivirüs programı kullanın.
- USB ve benzeri haricî cihazları antivirüs programında taramadan kullanmayın.
- Önemli ve kişisel bilgilerinizi girdiğiniz e-Devlet, e-Nabız, internet bankacılığı, alışveriş sitesi gibi sitelerde bilgilerin şifrelenerek gönderildiğini ifade eden “https” ifadesinin ve asma kilit simgesinin internet adresinin başında olduğundan emin olun.
- Tablet ve akıllı telefonlarınızda ekran kilidi kullanın.
- Farklı site ve uygulamalarda aynı şifreyi kullanmayın.
- Tablet ve akıllı telefonlarınıza sadece güvenilir uygulamaları indirin.
- Tablet ve akıllı telefonlarınızın yazılım güncellemelerini yapın.

ALO 141
GÜVENLİ İNTERNET BİLGİ DESTEK HATTI

- İndirdiğiniz uygulamaların istediği izinleri (kamera, mikrofon, fotoğraflar, rehbere erişim gibi) okumadan onaylamayın.
- Sosyal medya ve diğer çevrim içi ortamlarda sahte ve yanıltıcı kimlik kullanmayın.
- Sosyal medya platformlarında gizlilik ayarları ile profilinizin ve paylaşımlarınızın kimler tarafından görüleceğini belirleyebilirsiniz. Zorunlu değilse profilinizi ve paylaşımlarınızı herkese açmayın.
- Sosyal medya profilinize telefon numarası, ev ve iş adresi gibi kişisel bilgilerinizi koymayın.
- Sosyal medya ve diğer çevrim içi ortamlarda size ve ailenize ait fotoğraf ve video görüntülerini tanımadığınız kişilere göndermeyin.
- Tanımadığınız insanlarla bilgisayar ya da cep telefonu kamerası kullanarak görüşme yapmayın.
- Sosyal medya ve diğer çevrim içi ortamlarda sizi rahatsız eden hesapları engelleyin ve şikâyet edin.
- İnternette karşılaştığınız yasadışı içerikleri İnternet Bilgi İhbar Merkezi'ne (İhbar Web) bildirin.
https://www.ihbarweb.org.tr/
- İnternet ortamında karşılaştığınız sorunlar ve çözüm bulmakta zorlandığınız konular hakkında, **ALO 141 Güvenli İnternet Bilgi Destek Hattı**'nı arayın.

İLERİ OKUMALAR

Rehberler

iOS Cihazlar için Güvende Kalma Rehberi, Siberay

Android Cihazlar için Güvende Kalma Rehberi, Siberay

Ebeveynler ve Eğitimciler İçin Çevrim İçi Çocuk Koruma Kılavuzları, ITU

Dijital Oyunlarda Mahremiyet Rehberi, BTK

Güvenli İnternet Kullanımı Kılavuzu, MEB

Siber Zorbalık Kılavuzu, MEB

Ebeveynler için Dijital Mahremiyet Rehberi, BTK

Sosyal Medya Rehberi, Cumhurbaşkanlığı İletişim Başkanlığı

Dijital Mahremiyet Rehberi, BTK

Android ve iOS için Uygulama İzinlerini Kontrol Etme, B

YouTube Kısıtlı Mod, BTK

Google Etkinlik Kontrolleri, BTK

Digital Citizenship Education Handbook, Council of Europe

Digital Skills Toolkit, ITU

Internet Literacy Handbook, Council of Europe

Literatür ve Sahanın Kesişiminde Dijital Göçmenler İçin Dijital Yetkinlikler

Dijital bölünme sosyal, ekonomik ve politik alanları kuşatan bir kamu politikası terimi olarak yeni bilgi teknolojilerine erişimi olanlarla olmayanları ayıran boşluğa referansla 1990'lı yılların ortalarında gündeme gelmiştir (Srinuan & Bohlin, 2011). "Bilgisayar ve internet teknolojilerine eşitsiz erişim başta olmak üzere farklı nedenlerle bu teknolojilerin eşitsiz kullanımı ve bu kullanımından elde edilen avantajların farklılaşması sonucu oluşan ve çeşitlenen eşitsizliklere işaret eden dijital bölünme kavramı" sonraları çok yönlü araştırmaların konusu haline getirilmiştir (Özsoy, 2020, s. 11).

Makalenin devamını okumak için tıklayınız ya da yandaki QR kodu taratınız.

Teknoloji Bağımlılığının Önlenmesinde Dijital Ebeveynliğin Rolü

Teknoloji, hızlı bir şekilde kontrolsüzce gelişmekte ve gündelik yaşantının önemli bir rutini haline gelmekte, toplumsal ve bireysel roller üzerinde birtakım köklü değişiklikler meydana getirmektedir. Bu dönüşümün yaşandığı en önemli alanların başında ise aile kurumu gelmektedir. Günümüz dijital dünyasında aile yapısı pek çok yönüyle farklılaşmaya başlamış, aile bireylerinin etkileşim biçimleri yeni bir boyut kazanmış, aile çocuk ilişkileriyle ile ilgili önemli sorunlar ortaya çıkmıştır. Teknolojinin çocukların yaşamında vazgeçilmez unsur haline gelmesi, ebeveynlerin görev ve sorumluluk alanlarının da yeniden belirlenmesini zorunlu kılmıştır.

Makalenin devamını okumak için tıklayınız ya da yandaki QR kodu taratınız.

Yararlanılan Kaynaklar

Baştürk Akca, E. Siber Zorbalık Nedir? Nasıl Mücadele Edilir? Rehberi.

Bilgi Teknolojileri ve İletişim Kurumu İnternet Daire Başkanlığı, Bilgi Teknolojileri ve İnternet'in Bilinçli, Güvenli Kullanımı Rehberi

Department for Education (2018). Essential Digital Skills: Framework, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/738922/Essential_digital_skills_framework.pdf

Eken, M. (2021). Literatür ve sahanın kesişiminde dijital göçmenler için dijital yetkinlikler. Erciyes İletişim Dergisi, 8(2), 813-846. https://doi.org/10.17680/erciyesiletisim.969495

Hartmann, A., & Piontkowski, G. (2021). Developing digital competence framework for digital immigrants via mapping of perceptions and meanings: Country report for Germany [DigiComp Project Report]. https://digicomp.erciyes.edu.tr/project/Country_Report_for_Germany.pdf

https://tr.wikipedia.org/wiki/İnternet_forumu

https://www.guvenlicocuk.org.tr/siber-cocuk/internet-bagimliliginin-belirtileri-nelerdir

https://www.guvenlinet.org.tr/ailelere-tavsiyeler

https://www.guvenliweb.org.tr/dokuman-detay/kotucul-yazilimlar-virusler-truva-atlari-solucanlar

https://www.guvenliweb.org.tr/dokumanlar/rehberler?page=1

https://www.ibm.com/tr-tr/topics/open-source

https://www.theonespy.com/digital-citizenship-of-teens/#

Kabakçı Yurdakul, I., Dönmez, O., Yaman, F., Ferhan Odabaşı, H. (2013). Dijital Ebeveynlik ve Değişen Roller. Gaziantep University Journal of Social Sciences, 12(4), 883-896

Karakuş Yılmaz, T. (2020). Dijital Haklar ve Sorumluluklar. Dijital Okuryazarlık. Ş. Sağıroğlu, H. İ. Bülbül, A. Kılıç, M. Küçükali (Ed.). Ankara: Nobel, ss.152-161

Kuş, Z., Güneş, E., Başarmak, U., Yakar, H. (2017). Gençlere yönelik dijital vatandaşlık ölçeğinin geliştirilmesi: geçerlik ve güvenirlik çalışması. Journal of Computer and Education Research, 5 (10), 298-316. https://doi.org/10.18009/jcer.335806,

MEB Özel Eğitim ve Rehberlik Hizmetleri Genel Müdürlüğü, Güvenli İnternet Kullanımı Rehberi.

Sancho, J., Lindin, C., Grané, M., & Serrat, N. (2021). Developing digital competence framework for digital immigrants via mapping of perceptions and meanings: Technology in use in COVID's society. Learning from failures [DigiComp Project Report]. https://digicomp.erciyes.edu.tr/project/Technology_in_Use_in_COVIDs_Society.pdf

Uluslararası Telekomünikasyon Birliği (2020). Ebeveynler ve Eğitimciler İçin Çevrim İçi Çocuk Koruma Kılavuzları.

Yıldız, M. (2003). Elektronik E-Devlet Kuram ve Uygulamasına Genel Bir Bakış M. Acar ve H. Özgür (Ed.), e Değerlendirme. Çağdaş Kamu Yönetimi- I. M. Acar ve H. Özgür (Ed.), Ankara: Nobel, ss.305-327.

Görseller ve İllüstrasyonlar

Adobe Stock

Dosya Adı / Filename	Platform	Artist	Stock ID	Sayfalar / Pages
AdobeStock_309291306.ai	Adobe Stock	iuriimotov	#309291306	1
AdobeStock_234316577.ai	Adobe Stock	artinspiring	#234316577	9
AdobeStock_233052868e.ai	Adobe Stock	artinspiring	#233052868	10
AdobeStock_361679709.ai	Adobe Stock	barks	#361679709	10
AdobeStock_114755712.jpeg	Adobe Stock	rawpixel.com	#114755712	11
AdobeStock_307877834.ai	Adobe Stock	Gstudio	#307877834	11
AdobeStock_316626808.jpeg	Adobe Stock	zphoto83	#316626808	11
AdobeStock_309114014.ai	Adobe Stock	vladwel	#309114014	13
AdobeStock_144023579.jpeg	Adobe Stock	jirsak	#144023579	14
AdobeStock_271258646.ai	Adobe Stock	TarikVision	#271258646	14
AdobeStock_222019561.jpeg	Adobe Stock	jirsak	#222019561	15
AdobeStock_365528640.ai	Adobe Stock	ST.art	#365528640	15
AdobeStock_368388603.ai	Adobe Stock	Rogatnev	#368388603	19
AdobeStock_406354846.ai	Adobe Stock	barks	#406354846	20
AdobeStock_295247087.jpeg	Adobe Stock	sdecoret	#295247087	21
AdobeStock_181113647.jpeg	Adobe Stock	Andrey Popov	#181113647	27
AdobeStock_289350232.jpeg	Adobe Stock	LIGHTFIELD STUDIOS	#289350232	28
AdobeStock_319122738.ai	Adobe Stock	pavelvinnik	#319122738	29
AdobeStock_315171457.jpeg	Adobe Stock	LIGHTFIELD STUDIOS	#315171457	30
AdobeStock_390212429.jpeg	Adobe Stock	Song_about_summer	#390212429	30

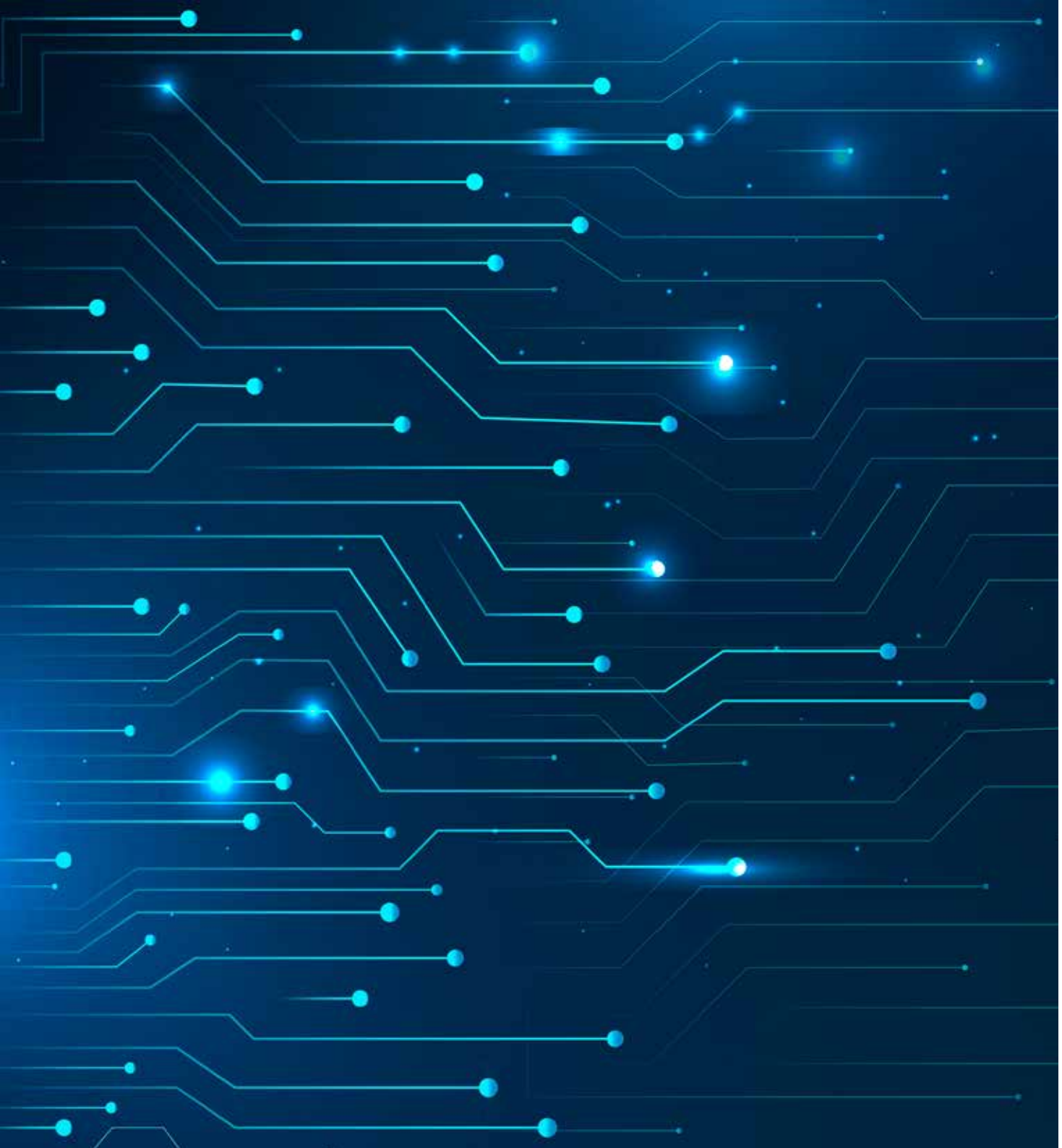
Dosya Adı / Filename	Platform	Artist	Stock ID	Sayfalar / Pages
AdobeStock_259605221.jpeg	Adobe Stock	fizkes	#259605221	31
AdobeStock_333050160.jpeg	Adobe Stock	aerogondo	#333050160	32
AdobeStock_311945974.jpeg	Adobe Stock	Pixel-Shot	#311945974	33
AdobeStock_373145444.jpeg	Adobe Stock	gesrey	#373145444	33
AdobeStock_290346522.ai	Adobe Stock	microstore	#290346522	34
AdobeStock_257923306.jpeg	Adobe Stock	iammotos	#257923306	35
AdobeStock_164606505.ai	Adobe Stock	your123	#164606505	37
AdobeStock_206594846.ai	Adobe Stock	emojoez	#206594846	37
AdobeStock_236977220.ai	Adobe Stock	artinspiring	#236977220	38
AdobeStock_395167439.jpeg	Adobe Stock	Tierney	#395167439	38
AdobeStock_178925715.ai	Adobe Stock	Oleg	#178925715	39
AdobeStock_310522821.ai	Adobe Stock	Ilias	#310522821	39
AdobeStock_257366596.ai	Adobe Stock	TeraVector	#257366596	40
AdobeStock_405731345.ai	Adobe Stock	Good Studio	#405731345	40
AdobeStock_410078480.jpeg	Adobe Stock	NDABCREATIVITY	#410078480	42
AdobeStock_236223547.jpeg	Adobe Stock	VadimGuzhva	#236223547	43
AdobeStock_454471962.jpeg	Adobe Stock	Sophie Alp	#454471962	44
AdobeStock_238333311.ai	Adobe Stock	vladwel	#238333311	48
AdobeStock_315028877.ai	Adobe Stock	Alena	#315028877	49
AdobeStock_327161394.ai	Adobe Stock	TeraVector	#327161394	50
AdobeStock_327451982.jpeg	Adobe Stock	putilov_denis	#327451982	51
AdobeStock_272011127.ai	Adobe Stock	StockVector	#272011127	52
AdobeStock_274539818.ai	Adobe Stock	nisi	#274539818	17, 22, 34, 46

Dosya Adı / Filename	Platform	Artist	Stock ID	Sayfalar / Pages
AdobeStock_332871720.jpeg	Adobe Stock	gopixa	#332871720	2, 8
AdobeStock_194708168.jpeg	Adobe Stock	peshkova	#194708168	23, 59
AdobeStock_370928201.jpeg	Adobe Stock	xiaoliangge	#370928201	47-51
AdobeStock_264712901.ai	Adobe Stock	monkik.	#264712901	47, 49-50
AdobeStock_276792076.jpeg	Adobe Stock	Greyparrot	#276792076	53, 54

Freepik

Dosya Adı / Filename	Platform	Artist	Sayfalar / Pages
5163376.ai	Freepik	Freepik	10
4950546.jpg	Freepik	storyset	16
18307.jpg	Freepik	rawpixel.com	18
Data_security_24.eps	Freepik	jcomp	24
Data_security_26.eps	Freepik	jcomp	25
Data_security_11.eps	Freepik	jcomp	26
2438127.ai	Freepik	Freepik	36
Family using laptops and phone instead of real communication.eps	Freepik	pch.vector	41
Addicted family using digital gadgets.eps	Freepik	pch.vector	44
30756.jpg	Freepik	macrovector	45
2083554.ai	Freepik	Freepik	45
rm373batch2-04.jpg	Freepik	rawpixel.com	18-22
25552.eps	Freepik	starline	3-9, 14-15, 55-58
v617batch2-bb-01-technology.jpg	Freepik	rawpixel.com	59-60


DigiComp



DigiComp

Co-funded by the
Erasmus+ Programme
of the European Union

ERCİYES ÜNİVERSİTESİ
1978
Araştırma Üniversitesi