

SİBER GÜVENLİK FARKINDALIK SORULAR

1-)Bir bilgi güvenliği ihlali olduğunu düşündüğünüzde ne yaparsınız?

A-) Kendim çözerim.

B-) Sistemdeki açığın nasıl kullanılabileceğini bulmaya çalışırım.

C-) Kayıtsız kalıp ilgili kişilerin çözmesini beklerim.

D-) İlgili firmanın IT veya güvenlik birimlerine iletirim.

2-)Siber güvenlikte ki en önemli zafiyet nedir?

A-) İnternet erişimi olan her nesne.

B-) Elektrikle çalışan her nesne.

C-) Güvenilmeyen sitelere girmek.

D-) İnsani eylemler.

E-) Kolay parola oluşturmak.

3-)Sosyal Mühendislik nedir?

A-)Maddi kaygı güdülmeyen mühendislik.

B-) Kişisel ağın kullanılması.

C-) Çevresel etkenleri göz önünde bulundurarak yapılan çalışmalar.

D-) Teknik olmayan yollarla istenen sisteme ulaşmak.

E-)Maddi kaygı güdülen mühendislik

5-)Bir firmanın sistemindeki zayıflıklarını tespit etmek için uyguladığı saldırı simülasyonu nedir ?

A-) Sanal saldırı ortamı (VATE)

B-) Bilgisayar korsanlığı

C-) Antivirüs uygulamaları

D-) Penetrasyon testi

E-) Siber saldırı

6-)Bilgilerinizi nasıl daha güvende tutabilirsiniz?

A-)Fiziksel bir not defterine yazarak.

B-) Txt dosyasında tutarak.

C-) Sadece güvendiklerimize vererek.

D-) Şifreleme kullanarak.

E-)Güvende tutmaya değer bilgi yoktur.

7-)Parolalarınızı nasıl oluşturuyorsunuz?

A-) Harf ve rakam kullanarak.

B-) Yalnızca harf ya da rakam kullanarak.

C-) Harf, rakam ve özel karakterler kullanarak.

D-) Büyük küçük harf, rakam ve özel karakter kullanarak.

E-)Sadece harf kullanarak.

8-)Bildiğiniz bir yerden gelen e-posta mesajında bağlantıya (link) tıklayarak bilgilerinizi güncellemeniz istendiğinde, ne yaparsınız?

A-) İlgili yerin logosu, adresi ve diğer bilgilerin doğruluğunu teyit edince güncellerim.

B-) Tanıdığım herhangi birinde bu e-maili alıp almadığını kontrol eder ona göre güncellerim.

C-) Linke tıklamadan istenen bilgileri yanıt olarak yollarım.

D-) İlgili kurumu arayarak e-mail konusunda bilgi alırım.

E-)Bağlantı linkine basıp direkt gereken adımları yaparım.

9-)Parolalarınızı kimlerle paylaşırsınız?

A-) Yalnızca güvendiğim arkadaşım ile paylaşırım.

B-) Ailem ile paylaşırım.

C-) Hesap önemli değilse isteyenle paylaşırım.

D-) Paylaşmam.

E-) Hangi sistem parolası olduğuna göre değişir.

10-)Siber güvenlikle ilgili kimler bilgi sahibi olmalı?

A-)Büyük kurumların teknoloji departmanının da çalışanlar.

B-) Bilgisayar kullananlar.

C-) İlgi duyanlar.

D-) Herkes.

E-) Siber güvenliğe ilgisi olanlar.

11-)Aşağıdaki şifrelerden hangisi daha güvenlidir?

A-) Selam123

B-) WTh!5Z7*

C-) kırmızı*48

D-) 123456

E-) 98765abcd

12-)Yol kenarında bulduğunuz bir USB bellek doğrudan cihazınıza takmak güvenli midir?

A-) Her zaman güvenlidir.

B-) Yalnızca sistemin virüsten koruma yazılımı güncellenirse takılabilir.

C-) Kısa sürede tak çıkar yapılabilir.

D-) Hayır, asla güvenli değildir.

E-) Hangi cihaza taktığımıza bağlıdır.

13-)İnternette bir yabancıyla arkadaşlık kurdunuz. Bir süre sonra, kişi kişisel bilgilerinizi istedi siz paylaşıyor mısınız?

A-) Evet, her zaman.

B-) En az birkaç haftadır arkadaşsanız olabilir.

C-) Sesli ve görüntülü görüşüldüyse olabilir.

D-) Hayır, asla güvenli değildir.

E-) Uzun zaman sohbet ettikten sonra paylaşılabilir.

14-)Sosyal medya hesaplarınızı nasıl daha güvende tutabilirsiniz?

A-) İki faktörlü kimlik doğrulamayı etkinleştirme.

B-) Güçlü parola kullanma.

C-) Benzersiz parola kullanma.

D-) Güvenilir mail hesabı kullanma.

E-) Yukarıdakilerin hepsi.

15-)Parolanızı bir iş arkadaşınız ile paylaşmanın kabul edilebilir olduğu durumlar nelerdir?

A-) İzindeyken.

B-) Yöneticiniz tarafından yönlendirildiğinde.

C-) Meslektaş güvenilir olduğunda.

D-) Kabul edilebilir bir durum yoktur.

E-) Molaya çıkıldığı zaman.

16-)Aşağıdakilerden hangisi zayıf bir paroladır?

A-) 123456

B-) P@ssw0rd

C-) seniseviyorum123

D-) Yukarıdakilerin hepsi

E-) 987654selam

17-)Bir web sitesinin veri ihlali öğrenildikten sonra ne yapılmalıdır?

A-) Hiçbir şey değil.

B-) Bu web sitesi için hesabın profil fotoğrafını değiştir.

C-) Bu web sitesi için hesabın şifresini değiştir.

D-) Bu web sitesi ve aynı parolayı kullanılan diğer tüm web sitelerinin hesaplarının parolasını değiştir.

E-) Bu web sitesi için hesabın mailini değiştir.

18-)Güçlü bir parolanın özellikleri nelerdir?

A-) Uzun

B-) Uzun, rastgele ve benzersiz

C-) Uzun, benzersiz

D-) Uzun, rastgele

E-) Kısa, rastgele

19-)Birisiyle bir parola paylaşmak istiyorsanız, en iyi seçenek nedir?

A-) E-posta ile gönder.

B-) Kısa mesaj gönder.

C-) Telefonla söyle.

D-) Hiçbiri.

E-) Görüntülü sohbette söyle.

20-) "Bill Gates'ten 5 milyon dolarlık bağış" konulu bir e-posta alıyorsunuz ve e-postada sizden parayı talep etmek için telefon numaranızı ve tam posta adresinizi vermenizi istiyorlar. En iyi eylem nedir?

A-)Telefon numaram ve posta adresimle cevap veririm.

B-) E-postayı açar paylaşılan ekleri inceler, bakarım.

C-)E-postayı arkadaşlarıma iletirim çünkü paylaşmak önemlidir.

D-)E-postayı spam olarak bildiririm ve silerim.

E-) E-postayı herkese iletirim.

21-)Oltalama (phishing) nedir?

A-) Yasal bir e-posta gibi görünen ve kişisel bilgilerinizi talep eden bir e-posta mesajıdır.

B-) İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik metodudur.

C-) Kimlik hırsızlığıdır.

D-) Veri hırsızlığıdır.

E-) Yukarıdakilerin hepsidir.

22-)İnternet alışverişlerinizde sitelerin orijinal ürün sattığını nasıl anlıyorsunuz?

A-) Ürünü sipariş ettikten sonra gelen qr kodunu okutarak.

B-) İnternet sitesi hakkındaki yorumları okuyarak.

C-) Ürünün fiyatlarını inceleyerek.

D-) Hiçbiri , ürünü direk satın alırım.

E-) Ürünü kontrol etmeye gerek yok.

23-)Bilgisayarınızdan kalkmanız gerektiğinde aşağıdakilerden hangisini yapılmalıdır?

A-) Bilgisayarımı kilitlerim.

B-) Bir şey yapmam ekranı açık bırakır giderim.

C-) Tüm uygulamaları kapatır masaüstünü açık bırakırım.

D-) Bilgisayar ekranımı kapatırım.

E-) Sekmeleri kapatır masaüstünü açık bırakırım.

24-)Herhangi bir sosyal medya hesabından veya smsten size gelen bir mesajda altın bulduğunu, para bulduğunu söyleyerek altını,parayı paylaşmak için numarayı aramanızı isteyen mesajlarda ne yapılmalıdır ?

A-) Numarayı aramak.

B-) Mesajın geldiği yeri engellemek

C-) Numarayı görüntülü aramak.

D-) Mesajla geri dönüş sağlamak.

E-) Numarayı herkese dağıtmak.

25-)Verilerin sağlıklı bir şekilde yedeklenmesi için aşağıdakilerden hangisi önemli değildir? A-

)Yedeklerin nerede ve hangi isimde saklanacağını belirlenmesi.

B-)Hangi bilgilerin yedekleneceğinin belirlenmesi.

C-)Hangi zamanlarda yedek almak gerektiği.

D-)Yedeği alınacak bilginin ne kadar sık aralıklarda değiştiğinin bilinmesi.

E-)Yedeklemenin kim tarafından yapılacağı.

26-)Aşağıdaki parolalardan hangisi diğerlerinden daha güçlüdür?

A-) ornekParola

B-) ornekBirParola

C-) ornekParola1

D-) ornek1Parola\$

E-) örnekparola

27-)Aşağıdakilerden hangi URL'e basmanız sakıncalıdır?

A-)https[:]//www.karabuk[.]edu.tr

B-)https[:]//www.turkiye[.]gov.tr

C-)https[:]//www.turkiye50bintl[.]tr.gg

D-)https[:]//www.cimer[.]gov.tr

E-) https[:]//www.siber[.]com..tr

28-)Kişisel bilgisayar güvenliği ile alınabilecek önlem ile ilgili hangileri doğrudur?

I-Şifre paylaşımında dikkatli olmak

II-Önemli bilgilerin parola ile korunması

III-E-posta ile gelen verilere dikkat etmek

A-)I,II,III

B-)Hepsi

C-)Yalnız I

D-)II,III

E-) Yalnız II

29-)İnternet alışverişlerinde kredi kartınızdan ödemeyi gerçekleştirirken site üzerinde nelere dikkat edilmelidir?

A-) Hepsine

B-)2 faktörlü olarak ödemenin gerçekleştiğine.

C-)Bilgilerinizin şifrelendiğine dair açık rıza metni olup olmadığına.

D-)Bilgilerinizin kaydedilip kaydedilmediğine dair açık rıza metni olup olmadığına.

E-) Çok faktörlü olarak güvenliğin gerçekleştiğine.

30-) “Bilgi Güvenliđi Yönetim Standardı” na göre aşağıdakilerden hangisi bilgi güvenliđinin temel unsurları arasında değildir?

A-) Bütünlük

B-) İnkâr etme

C-) Kimlik doğrulama

D-) Sorumluluk

E-) Erişim denetimi

31-)ZeroDay Nedir?

A-) Sıfırın cı Gün saldırısı.

B-) Sistemi sıfırlama saldırısı.

C-) Daha önce fark edilmemiş açıkların sömürülmesi ile oluşan saldırılar.

D-) 1 ve 0 ların hepsinin 0 olması.

E-)1 ve 0 ların hepsinin 1 olması.

32-) Tehdit Aktörü kimdir?

A-) Siyah Şapkalı Hacker

B-) Hacktivist

C-) Hepsi

D-) Gri Şapkalı Hacker

E-) Hacker

33-) Dijital Ayak izi Nedir?

A-) İnternet ortamında gezinmelerin bıraktığı izler.

B-) İnternet ortamındaki paylaşımlar.

C-) Hepsi

D-) İnternette yapılan yorumlar.

E-) İnternette paylaşılan fotoğraflar.

34-)

- 1.Telefon çeviriciler (dialer)
2. Arka kapılar (backdoor)
- 3.Mesaj sađanıkları (spam)
- 4.Kök kullanıcı takımları (rootkit)

Yukarıdakilerden hangisi veya hangileri en genel kötücül yazılımlardandır?

A-) Yalnız 3

B-)Hepsi

C-) 3 ve 4

D-) 1 ve 4

E-) 1 ve 2

35-) Aşağıdakilerden hangisi bir virüs türü değildir?

A) Boot virüsleri

B) Dosya virüsleri

C) Script virüsleri

D) Klasör virüsleri

E-)Casus virüsleri

36-) Mail içerisinde kötü niyetli bir link ya da doküman barındırır ve kullanıcıların bilgilerini çalmayı hedefler”. Bu cümleyi tanımlayan seçenek hangisidir?

A) Zararlı yazılım

B) DDoS

C) Parola saldırıları

D) Phishing

E-) Dos

37-) Aşağıdaki parolalardan hangisi diğerlerinden daha güçlüdür?

A) ornekParola

B) ornekBirParola

C) ornekParola1

D) ornek1Parola\$

E-) ornekparola

38-) Aşağıdaki programlar içinde en güvenli olan hangisidir?

- A) kırılmış (crack) programlar
- B) casus yazılım (spyware)
- C) yazılım yamaları (patch)
- D) solucan (worm)
- E-)virüsler

40-) Bulaşma bölgesine göre virüsler aşağıdakilerden hangisi değildir?

- A) Boot Virüs
- B) Dosya Virüs
- C) Anti Virüs
- D)Karışık Virüs
- E-) Casus virüsleri

41-) Güçlü Parola oluştururken aşağıda verilen kriterlerin hangisine dikkat edilmez?

- A-) En az 8 karakterden oluşmasına
- B-) Doğum tarihi gibi özel bilgilerin kullanılmasına
- C-) Çoğu kişinin kullandığı parolaları kullanmamaya
- D-) Özel karakterlerin kullanılmasına
- E-) Hiçbiri

42-) Aşağıdakilerden hangisi zararlı yazılımlardan korunma yöntemlerinden biri değildir?

- A-) Çok kişinin kullandığı bilgisayarda bankacılık işlemleri yapmak
- B-) İnternet üzerinden alışveriş yapıyorsak sanal kredi kartı kullanmayı tercih etmek
- C-) Neyi nerede aradığımıza dikkat etmek
- D-) Antivirüs ve firewall programı kullanmak, işletim sistemimizi güncel tutmak
- E) Hepsi

43-) Hangisi siber tehditlere karşı bir önlem değildir?

- A-) Kaynağı bilinmeyen e-postaları yok etmek
- B-) Sık sık parola değiştirmek
- C-) Anti-virüs programı kullanmak
- D-) Cep telefonuna gelen mesajlardaki tüm talimatları uygulamak
- E-) Hepsi

44-) Aşağıdakilerden hangisi siber saldırılara örnektir?

- A-) Veri hırsızlığı
- B-) Parolanın çalınması
- C-) Virüs bulaşması
- D-) Hepsi
- E-) Verileri ifşa edilmesi

45-) Sizden banka bilgilerinizi talep eden ve ekinde “ acil_okuyunuz.vbs” adında dosya bulunan e-posta gördüğünüzde ne yapmalısınız?

- A-) Talep edilen bilgileri en kısa zamanda girmek
- B-) E-postanın içerisindeki dosyayı indirmek
- C-) Şüpheli olduğunu anladıktan sonra spam olarak işaretlemek
- D-) Dosyanın içeriğini incelemek
- E-)Maili incelemek dosyayı yüklemek bilgisayara yedeklemek.

46-) Genel olarak tüm kötücül yazılımlar için aşağıdaki ifadelerden hangisi yanlıştır?

- A) kendi kendilerini çoğaltamazlar
- B) özerk bir yapıya sahiptirler
- C) bulaşma mekanizmaları vardır
- D) ayrık veya virüs özelliği taşırlar
- E-)Hepsi

47-) Aşağıdakilerden hangisi kriptografik saldırılardan değildir?

- A) Kaba kuvvet saldırısı (brute force attack)
- B) Ortadaki adam saldırısı (man in the middle attack)
- C) İlişkili anahtar (related key attack)
- D) Uzaktan yönetim aracı (Remote administration tool)
- E-) Hiçbiri

48-)Kişisel bilgisayar güvenliği ile alınabilecek önlem ile ilgili hangileri doğrudur?

- I-Kullanılmadığı zaman internet erişimin kapanması
 - II-Disk paylaşımında dikkatli olmak
 - III-Önemli bilgilerin parola ile korunması
 - IV-E-posta ile gelen verilere dikkat etmek
- A)I,II,III B)Hepsi C)I ve IV D)II,III ve IV E) II,III

49-) Bilgisayar ya da telefonlarımızdaki bilgi güvenliğini nasıl sağlamalıyız?

- A-) Her hafta yedek alarak
- B-) Güvenlik yazılımları kullanarak
- C-) Verileri şifreleyerek
- D-) Bilgisayarımızı açık bırakmayarak
- E) Hepsi

50-) Güncellemeler ile ilgili aşağıdaki ifadelerden hangisi doğru DEĞİLDİR?

- A) Güncellemeler yazılımlardaki güvenlik açıklıklarını kapatmak için gereklidirler.
- B) Sadece işletim sistemini güncel tutmak yetmez. Kullandığımız tüm programların güncelliği önemlidir.
- C) Yayınlandıktan sonra her hangi bir zamanda yapılsa yeterli olur.
- D) Güncellemeler “yeni sürümler”, “yazılım yamaları”, veya “hizmet paketleri” olarak yayınlanabilirler.
- E) Hepsi

51-) Normal ve sistem tarafından olması istenilen bilgi akışına yapılan saldırılar dört değişik karakteristik sergileyebilmektedir. Aşağıdakilerden hangisi bu karakteristik özelliklerden biri değildir?

A) Yarıda kesme (interruption)

B) Gizli dinleme (intercept)

C) Değiştirme (modification)

D) Aldatmaca (hoax)

E) Hepsi

52-) İlgili sistem, ağ, uygulama veya protokolün güvenliğini tehlikeye atan; beklenmeyen ve istenmeyen bir olaya sebep olabilecek bir zayıflığın varlığı, tasarım veya gerçekleştirme hatası olarak tanımlanmaktadır.

Yukarıdaki tanım aşağıdaki kavramlardan hangisine aittir?

A) Korunmasızlık (vulnerability)

B) Aldatmaca (hoax)

C) Kandırıcı (spoofing)

D) Port tarayıcılar (port scanner)

E) Hiçbiri

53-) TSE-17799 “Bilgi Güvenliđi Yönetim Standardı” belgesine göre aşağıdakilerden hangisi bilgi güvenliđinin temel unsurları arasında değildir?

A) Bütünlük

B) İnkâr etme

C) Kimlik dođrulama

D) Sorumluluk

E) Aldatmaca

56-) İş arkadaşınızın adını içeren bir mail adresinden içinde acil bakmanızı istediđi bir dosya olan bir mail aldınız ne yaparsınız?

A-) Dosyayı açıp kontrol ederim.

B-) Arkadaşımı arayıp o mu diye teyit ederim.

C-) Umursamam.

D-) Şüphelenip IT bölümündeki çalışanlara olayı bildiririm.

E-) Maili inceleyerek, dosyayı yedeklerim

57-) Aşağıdakilerden hangisi tehlikeli yazılımlara örnek değildir?

A-) Kayıtlı yazılım güncellemeleri

B-) Korsan yazılımlar

C-) Yama olarak internetten indirilmiř herhangi bir program

D-) Korsan müzik ve film dosyaları

E-) Hepsi

59-) Aşağıdakilerden hangisi bilgi güvenliğinin temel ögesi değildir?

A-)Erişilebilirlik

B-)Bütünlük

C-)Çeşitlilik

D-)Gizlilik

E-)Hepsi

61-) Bilgisayarınızda virüs olduğundan şüpheleniyorsanız, aşağıdakilerden hangisini yapmak hata olabilir?

A-)Anti-virüs programı ile virüs taraması yaptırmak

B-)Tanımadığınız kişilerden gelen e-posta eklerini açmak

C-)Anti-virüs yazılımınızın virüs tanımlamalarını güncellemek

D-)Bilmediğiniz ve şüpheli görünen uygulama (exe uzantılı) dosyalarını araştırıp silmek

E-) Hepsi

62-) Aşağıdakilerden hangisi siber suça örnek teşkil etmez?

A-) Sibirya doğalgaz patlaması

B-) Çernobil Olayı

C-) Mavi Marmara Saldırısı

D-) NATO Kosova krizi

E-) SCADA Sistemi patlaması

63-)Aşağıdakilerden hangisi zararlı yazılımlardan korunmak için alınacak tedbirlerden biri değildir ?

A-)Lisanslı anti-virüs programı kullanmak

B-)Diski düzenli olarak harici bir yere yedeklemek

C-)İşletim sistemini güncel tutmak

D-)Mail adresine gelen mailleri zamanında okumak

E-Hepsi

64-)Bilgisayarda programları ve verileri bozmak amacıyla yazılmış programlara ne ad verilir?

A-) Oyun

B-) Virüs

C-)E-Posta

D-)İnternet

E-) Spam

65-)Aşağıdakilerden hangisi bilgisayara virüs bulaştığının belirtisidir?

A-) Hiç beklenmedik hata mesajları ekranda görüntüleniyorsa

B-) Dosyalar bozuluyor veya aniden siliniyorsa

C-) Ekranda değişik karakterler görünüyor veya kayıyorsa

D-) Hepsi

E-) Hiçbiri

66-)Aşağıdakilerden hangisi zararlı yazılımlar arasında yer almaz?

A-) Truva Atı

B-) Antivirüs

C-) Solucanlar

D-) Ransomware

E-) Spyware

67-) Gereksiz e-posta virüslerine ne denir?

A-)Keylogger

B-)Truva atı

C-)Spam

D-)Solucan

E-) Spyware

68-) Şüpheli bir e-posta geldi ne yaparsınız?

A-) Hiçbir şey yapmam.

B-) E-posta içerisindeki linke tıklarım.

C-) Cevaplarım.

D-) Gelen e-postayı raporlar ilgili birimlere şikâyet ederim.

E-)E postayı inceler mailde yazan yapılması gerekenleri yaparım .

69-)Online alışverişlerde hangisini kullanmak daha güvenilirdir?

A-)Tek kullanımlık kart oluşturmak

B-)Kredi kartı

C-)Banka kartı

D)Telefondan ödeme

E) Hepsi

70-)Örnek Wi-Fi parolası nasıl olmalıdır?

A-) 123456

B-) Bedavamısandın-para verip aldım

C-) 1gb100tl

D-) Tg2#N^bxH

E-)987654

71-)Aşağıdakilerden hangisi zararlı yazılımlardan korunmak için alınacak tedbirlerden biri değildir?

A-) Diski düzenli olarak harici bir yere yedeklemek

B-) İşletim sisteminin güncelleştirmek

C-) Mail adresine gelen mailleri zamanında okumak

D-) Tarayıcıları güncel tutmak

E-) Hiçbiri

72-) Aşağıdakilerden hangisi İşletim sisteminin temel görevlerinden biri değildir?

A-) Hesap Yönetimi

B-) Ağ Yönetimi

C-) Bellek Yönetimi

D-) Giriş Çıkış Birimleri Yönetimi

E-)Hepsi

73-) Aşağıda verilen parola örneklerinden hangisi diğerlerine göre daha güçlü paroladır?

A-) H.34.323

B-) ERTY3456

C-) @_43A-f6

D-) Qwer1234

E-)123456

74-)Aşağıdakilerden hangisi ağ cihazlarından değildir?

A-) Telgraf

B-) Switch

C-) Router

D-) Hub

E-) Repeater

75-)Lamer'lar hakkında aşağıda verilen bilgilerden hangisi yanlıştır?

a) Yeterli hacking bilgisine sahiptirler

b) Phishing yazılımlarla e-posta adresi aralamaya çalışırlar.

c) Trojanlar kullanarak bilgisayarları ele geçirmeye çalışırlar.

d) Hazırlanmış exploit yazılımlar kullanılarak web sunucularında root, ya da admin hakkı elde etmeye kasarlar.

E) Hepsi

76-)Veri bütünlüğünü test etmek için kullanılan, bir şifreleme algoritması hangisidir?

a)Yapay Şifreleme

b)Multi Şifreleme

c)Sezar Şifreleme

d)Md-5

e) Hepsi

77-)Aşağıdakilerden hangisi zararlı yazılımlardan korunma yöntemlerinden biri değildir?

A-)Neyi nerede aradığımıza dikkat etmek,

B-)İnternet üzerinden alışveriş yapıyorsak sanal kredi kartı kullanmayı tercih etmek,

C-)Antivirüs ve firewall programı kullanmak, İşletim Sistemimizi güncel tutmak,

D-)Çok kişinin kullandığı bilgisayarda, bankacılık işlemlerini yapmak

E-) Hiçbiri

78-)Aşağıdakilerden Hangisi zararlı yazılım çeşitlerinden değildir?

A-)Trojan

B-)Router

C-)Spyware

D-)Worm

E-) Hepsi

79-)Bilgi güvenliği üç temel unsurdan oluşur. Bu üç temel unsur nelerdir?

A-)Doğruluk, Bütünlük, Erişebilirlik

B-)Gizlilik, Bütünlük, Kullanılabilirlik

C-)Gizlilik, Öznellik, Erişebilirlik

D-)İlkesellik, Gizlilik, Tekillik

E-)İlkesellik, Gizlilik, Erişebilirlik

80-)Aşağıdakilerden hangisi bir tarayıcı değildir?

A-)Explorer

B-)Excel

C-)Opera

D-)Chrome

E-) Hepsi

81-)Kullanıcı ile bilgisayar sistemini oluşturan tüm yazılım ve donanım birimleri arasından iletişimi sağlayan nedir?

A-)İşletim Sistemi

B-)Sürücüler

C-)Grafik yazılımları

D-)Anti-virüs

E-) Hiçbiri

82-)Aşağıdakilerden hangisi güvenli internet kullanımı doğrultusunda alınması gereken tedbirlerdendir?

A-)Aileler bilinçli internet kullanımı noktasında bilgilenmeli.

B-)İlköğretim müfredatına “Bilişim Şuuru” dersi konulmalı.

C-)Türkiye genelinde bütün okullarda veliler ile birlikte bilinçlendirme faaliyetleri yürütülmeli.

D-) Hepsi

E-) Hiçbiri

83-)Aşağıdakilerden hangisi siber zorbalık kapsamına girer?

A-)Dolandırıcılığa ya da istismara maruz kalarak bilinçsiz veri paylaşımı

B-)Yabancı İnsanlarla tanışmak

C-) Sosyal medya aracılığıyla toplumsal konular üzerine yorumda bulunmak

D-) Sosyal platformlarda paylaşılan gönderilerin beğenilmesi

E-) Hiçbiri

84-)Güvenli internet nedir?

A-) İnternetteki risklerden ve zararlı içeriklerden korunmanızı sağlayan bir servistir.

B-) Belirli saatler içerisinde kullanıma sunulan servistir

C-) Ücretli olarak kullanıma sunulan servistir

D-) Sosyal medya uygulamalarının kullanımını engelleyen bir servistir

E-) Sadece sosyal medya uygulamalarının kullanımını engellemeyen bir servistir

85-)Aşağıdakilerden hangisi siber zorbalıktan korunma yöntemlerinden biridir?

A-)Kişisel Bilgilerin paylaşılması.

B-) Bilinçsiz internet kullanımı.

C-)Kimliği bilinmeyen sahte kullanıcılarla iletişime geçmek.

D-) Güvenlik yazılımları kullanmak.

E-)Her şeyi sosyal medyada paylaşmak.

86-)Bilgi Güvenliğine yönelik saldırı çeşitleri nelerdir ?

A-)Phishing

B-)Zararlı yazılımlar

C-)Yoğun e posta (spam) gönderimi

D-) Hepsi

E-) Hiçbiri

87-)Güvenli bir Bilgi Nedir?

A-) Gizlilik Erişilebilirlik ve Bütünlük ilkelerine sahip bilgi

B-)Kimseyle paylaşılmayan bilgi

C-) Tekrar kullanılabilirliği olmayan bilgi

D-)Sosyal medya üzerinde paylaşılan veriler

E-)Herkesle paylaşılan bilgi.

88-)Aşağıdakilerden hangisi Mobil sistemlerde bulunan bir güvenlik zafiyetidir?

A-) Konum bilgileri kullanılan 3.parti uygulamalar

B-) Geçerli güvenlik sertifikaları tarafından imzalanmış mobil oyunlar

C-) (AppStore,Google Play Store) Uygulamalar tarafından kullanılan servis uygulamaları.

D-)İzin gerektirmeyen ve geçerli bir otorite tarafından kabul edilen uygulamalar

89-)Hangisi Bilgi Güvenliđinin incelendiđi bařlıklar hangisidir ?

A-) Gizlilik

B-) Bütünlölük

C-) Kullanılabilirlik

D-) Hepsi

E-) Hiçbiri