T.C.

MİLLÎ EĞİTİM BAKANLIĞI

Hayat Boyu Öğrenme Genel Müdürlüğü

BİLİŞİM TEKNOLOJİLERİ ALANI

BİLGİ GÜVENLİĞİ BİLİNÇLENDİRME EĞİTİMİ KURS PROGRAMI

ANKARA, 2016

İÇİNDEKİLER

PROGRAMIN ADI

Bilgi Güvenliği Bilinçlendirme Eğitimi Kurs Programı

PROGRAMIN DAYANAĞI

1. 24.06.1973 tarihli ve 14574 sayılı Resmî Gazete' de Yayımlanan, 1739 sayılı Millî Eğitim Temel Kanunu,
2. 21.5.2010 tarihli ve 27587 sayılı Resmî Gazete' de yayımlanan Yaygın Eğitim Kurumları Yönetmeliği,
3. Talim ve Terbiye Kurulunun 20.04.2016 tarih ve 19 sayılı kararı ile kabul edilen, Yaygın Eğitim Kurumları Çerçeve Kurs Programı,
4. Talim ve Terbiye Kurulu Başkanlığının 27.09.2005 tarih ve 329 sayılı kararı ile onaylanan Bilgi ve İletişim Teknolojisi Dersi Öğretim Programı,
5. Talim ve Terbiye Kurulu Başkanlığının 31.08.2016 tarih ve 65 sayılı kararı ile kabul edilen, Bilgisayar Bilimi Dersi (Kur 1, Kur 2) Öğretim Programı,
6. 23.05.2007 tarihli ve 26530 sayılı Resmî Gazete' de yayımlanan 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
7. 01.11.2007 tarih ve 26687 sayılı Resmî Gazete' de yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik.

PROGRAMIN GİRİŞ KOŞULLARI

1. Okuryazar olmak.
2. 10 yaşını tamamlamış olmak.

EĞİTİMCİLERİN NİTELİĞİ

1. Talim ve Terbiye Kurulu Başkanlığı tarafından yeniden düzenlenen Öğretmenlik Alanları, Atama ve Ders Okutma Esaslarına göre atanan;
   - Bilişim Teknolojileri Meslek Dersleri Öğretmenleri,
   - Elektronik Bölümü Elektronik ve Bilgisayar Öğretmenleri,
   - Elektronik Bölümü Elektronik ve Bilgisayar Eğitimi Öğretmenleri,
2. Bilişim Teknolojileri alanında lisans eğitimi alanlar,
3. Bilişim Teknolojileri alanında ön lisans mezunu olanlar,
4. Bilişim Teknolojileri alanında en az IV. seviye bir eğitimi başarıyla tamamlayanlar,
5. Bilgi güvenliği alanında yüksek lisans/doktora yapmış olanlar

görevlendirilir.

PROGRAMIN AMAÇLARI

Bilgi Güvenliği Bilinçlendirme Eğitimi Kursunu bitiren bireylerin;

1. Bilgi güvenliği kavramını açıklaması,
2. Bilgi güvenliği unsurlarını açıklaması,
3. Kimlerin bilgi güvenliğinden sorumlu olduğunu kavraması,
4. TC Kimlik No, parola gibi kişisel bilgileri başkalarıyla paylaşmaması,
5. Bilinçli kullanıcı olmanın neden önemli olduğunu açıklaması,
6. Bir güvenlik olayı ile karşılaşıldığında ne yapılacağı konusunda işlemleri listelemesi,
7. Bilgisayar açılışında kullanıcı adı ve parola kullanmanın önemini açıklaması,
8. Bilgisayar erişim güvenliğini sağlamak için kullanılan temel yöntemleri listelemesi,
9. Parola güvenliğinin önemini açıklaması,
10. Güçlü parola oluşturma tekniklerini kullanarak güçlü parola oluşturması,
11. Bilgisayarına BIOS şifresi vermesi,
12. İşletim sistemi oturumunu kullanıcı adı ve parola ile açması,
13. Parolalı ekran koruyucusu kullanması,
14. Parolaların korunması için dikkat edilmesi gereken konuları listelemesi,
15. Bilgisayar başından kalkarken bilgisayar oturumunu kilitlemesi,
16. Güvenli olmayan yazılımları açıklaması,
17. Güvenli olmayan yazılımlardan korunma yöntemlerini listelemesi,
18. Internet veya e-posta ile gelebilecek zararlı yazılımlara karşı tedbir alması,
19. Yazılımları güncel tutmanın önemi açıklaması,
20. Yazılımları güncel tutma yöntemlerini sıralaması,
21. Dosya ve veri kaybının nasıl gerçekleştiğini açıklaması,
22. Bilgisayarını yedeklemesi,
23. Zararlı program türlerini listelemesi,
24. Zararlı programların nasıl yayıldıklarını açıklaması,
25. Zararlı programların nasıl anlaşıldığını açıklaması,
26. Zararlı programlardan korunmak için neler yapılabileceğini listelemesi,
27. Anti-virüs yazılımını bilgisayarına kurması,
28. Anti-virüs yazılımı ayarlarını yapması,
29. Anti-virüs yazılımını bilgisayarında güncellemesi,
30. Sosyal mühendislik kavramını açıklaması,
31. Sosyal mühendislikte kullanılan saldırı yöntemlerini listelemesi,
32. Sosyal mühendislik saldırılarından korunması,
33. Güvenlik duvarını kurması,
34. Güvenlik duvarını aktifleştirmesi,

35. Güvenlik duvarını yapılandırması,
36. İnternette gezerken karşılaşılabilecek tehlikeleri açıklaması,
37. İnternette işlem yaparken dikkat edilecek konuları açıklaması,
38. HTTP/FTP/HTTPS protokollerinin farkını açıklaması,
39. HTTP/FTP erişimleri için alınabilecek tedbirleri listelemesi,
40. İşletim sistemi yamalarını yapması,
41. Çocukların güvenliği için neler yapılabileceği konusunda öneriler getirmesi,
42. E-posta saldırılarını listelemesi,
43. İstenmeyen e-postaları tanımlaması,
44. İstenmeyen e-postalara karşı tedbir alması,
45. Taklit e-postaları tanımlaması,
46. Taklit e-postalara karşı tedbir alması,
47. Aldatmaca e-postaları tanımlaması,
48. Aldatmaca e-postalara karşı tedbir alması,
49. E-posta saldırılarına karşı kurumsal olarak alınabilecek tedbirleri listelemesi,
50. ADSL modem ve kablosuz bağlantı konusunda güvenlik tedbirleri almanın önemini açıklaması,
51. ADSL modem ve kablosuz bağlantı konusunda olası tehlikeleri sıralaması,
52. ADSL modem ve kablosuz bağlantı konusunda alınabilecek tedbirleri açıklaması,
53. ADSL modem ve kablosuz internet için güvenlik ayarlarını yapması,
54. Kablosuz modem bağlantısını paylaşmanın olası tehlikelerini listelemesi,
55. Modem ve internet bağlantı güvenliğini sağlamak için alınması gereken temel önlemleri açıklaması,
56. Siber güvenliğin önemini kavraması,
57. Siber güvenlik haberlerini ve duyurularını takip etmesi,
58. Mobil cihazına (akıllı telefon, tablet, vb.) parola korumalı cihaz kilidini ayarlaması,
59. Mobil cihazına Wi-Fi ağını açıp kapatması,
60. İOS işletim sistemli cihazlarda uygulama yetkilerini düzenlemesi,
61. Android işletim sistemli cihazlarda uygulama yükleme sırasında verilecek yetkileri kontrol etmesi,
62. Android işletim sistemli cihazda bilinmeyen kaynaklardan uygulama yüklemeye izin veren “Bilinmeyen Kaynaklar” özelliğini devre dışı bırakması,
63. Mobil cihazlarda güncelleme kontrolünü yapması,
64. Güncelleme yapılması gereken cihazı güncellemesi,
65. Mobil cihaz içeriğini ve ayarlarını sıfırlaması,
66. İnternet’teki aktivitelerin hiçbir zaman silinmediğini kavraması,
67. Tarayıcı ayarlarını mahremiyeti koruyacak şekilde yapılandırması,

68. Sosyal medyada paylaştığınız kişisel verilerin aleyhinizde kullanılabileceğinin farkına varması,
69. Kişisel verilerinin korunması hakkında sahip olunan hakları listelemesi

amaçlanmaktadır.

PROGRAMIN UYGULANMASIYLA İLGİLİ AÇIKLAMALAR

1. İnternetin kullanımının yaygınlaşmasıyla birlikte internet ve ona bağlı sistemler aracılığıyla işlenen suçlar da çoğalmaktadır. Bu suçlar siber suç olarak adlandırılmaktadır. Günümüzde teknolojinin yaygınlaşmasıyla birlikte, gerçek hayatta karşılaşılan suçlar internet aracılığıyla da işlenmektedir. Bu suçlar mevcut hukuk sistemi içerisinde de karşılığı olan suçlardır.
2. Bu programla; internet yoluyla karşılaşılan tehditler, bu tehditlere karşı alınabilecek önlemler hakkında farkındalık oluşturulmaktadır. Bunun yanında, bireylerin bilgisayarlarını ve mobil cihazlarını koruması için neler yapabilecekleri de pratik olarak anlatılmaktadır. Programın sonunda bireyin internet üzerinden işlenen suçların önüne geçilmesi sağlanırken, internetin güvenli bir şekilde kullanılması da sağlanmış olacaktır.
3. Programın uygulanmasında; yaş, cinsiyet, eğitim vb. durumları gözetilerek gruplar oluşturulmalıdır. Oluşturulan grupların özelliklerine göre konular anlatılmalıdır. Yaşanan örnekler, karşılaşılabilecek suç unsurları hedef kitlenin özelliğine göre verilir.
4. Kurs Programı, Millî Eğitim Bakanlığında görevli uzman ve alan öğretmenleri ve alan uzmanları ile iş birliği içinde hazırlanmıştır.
5. Kursun içeriğine göre konular, teorik ve uygulamalı olarak uygun olan yöntem ve teknikler uygulanarak işlenir.
6. Bilgi Güvenliği Bilinçlendirme Eğitimi kurs programının amaçları ve içeriği yoluyla kursa katılan bireylere aşağıda tabloda verilen değerlerin kazandırılması ve geliştirilmesi hedeflenmiştir.

DEĞERLER
Kurallara Uyma
Sabır
Sorumluluk
Duyarlık
Doğruluk ve dürüstlük
Yardımlaşma

7. Programın uygulanmasında hayat boyu rehberlik hizmeti sunan eğiticiler, kursiyerlerin kişisel ve mesleki nedenlerle yeterliliklerinin değişmesi ve gelişmesine katkıda bulunacak bir rehber niteliğinde olmalıdır.

8. Program süresince kursiyerlere program içeriğinin öğretilmesi için ihtiyaç duyduğu araç, gereç ve malzemeler temin edilmeli, donanımlar sağlanmalı ve gerektiğinde bilgisayar destekli öğretim faaliyetlerinden (slaytlar, akıllı tahtalar) faydalanılmalıdır.
9. Program süresince bireylerin merak uyandırma ve planlama, araştırma ve keşfetme, çözümleme ve derinleştirme, paylaşma ve yaşantıya uygulama etkinliklerini gerçekleştirmeleri sağlanarak bireyin öğrenmeye etkin katılımı desteklenmelidir.
10. Kurs dışında bireylerin öğrendiklerini pekiştirmek için kendi kendine öğrenme faaliyetleri yapması teşvik edilmelidir.
11. Program sonunda, bireyin Bilgi Güvenliği Bilinçlendirme Eğitimi kurs düzeyinin ölçülmesi için değerlendirme yapılmalıdır.
12. Uygulama yaptırılırken her bireye bir bilgisayar sağlanır.
13. Uygulamalar mümkünse bilgisayar laboratuvarlarında/sınıflarında veya Kamu İnternet Erişim Merkezleri (KİEM) sınıflarında yaptırılır.
14. Program, yaygın eğitim kurumlarında veya kurumlarca uygun görülen diğer yerlerde uygulanır.

PROGRAMIN KREDİSİ

Genel kurs programında kredilendirme yapılmamaktadır.

PROGRAMIN SÜRESİ VE İÇERİĞİ

Kurs programının süresi; günde en fazla 6 ders saati uygulanacak şekilde toplam 17 ders saatidir. Sürenin konulara göre dağılımı aşağıdaki tabloda verilmiştir.

Konular	Süre (Ders Saati)
Bilgi ve Siber Güvenlik	1
Bilgisayar ve Erişim Güvenliği	2
Tehditler ve Korunma Yöntemleri	4
Internet ve Ağ Güvenliği	6
Mobil Cihazlarda Güvenlik	2
Kişisel Verilerin Korunması ve Mahremiyet	2
Toplam	**17**

1. BİLGİ VE SİBER GÜVENLİK

1.1. Bilgi, Bilginin Sahibi, Bilgiyi Kullanan ve Bilgi Sistemini Yöneten Kavramları,

1.2. Bilgi Güvenliğinin Önemi,

1.3. Bilgileri Yetkisiz Kişilerin Eline Geçen Bireyin Yapması Gerekenler,
    1.3.1. İnternet Bilgi İhbar Merkezi,
    1.3.2. Bilgisayarda Yapılacak Kontroller,
    1.3.3. Bilgi İşlem Personeline Başvuru,
1.4. Bilgi Güvenliğinden Sorumlu olan Kişiler,
1.5. Bilgi Güvenliğinde Kullanıcı Sorumlulukları,
1.6. Siber Güvenlik Kavramı,
1.7. Siber Güvenliğin Önemi,

2. BİLGİSAYAR VE ERİŞİM GÜVENLİĞİ

2.1. Bilgisayara Giriş Güvenliği,
    2.1.1. Bilgisayar BIOS Parolası Koyma,
    2.1.2. Bilgisayarın Kullanıcı Adı ve Parolası Kullanma,
2.2. Parola Güvenliği,
    2.2.1. Parolanın Başkasının Eline Geçtiğinde Yapılacaklar,
    2.2.2. Zayıf Parola Örnekleri,
    2.2.3. Güçlü Parola Oluşturma,
    2.2.4. Parola Koruma Yolları,
2.3. İşletim Sistemi ve Kullanılan Yazılımları Güncel Tutma,
2.4. Güncel Anti-virüs Yazılımı Kullanma,
2.5. Güvenlik Duvarı Kullanma,
2.6. Dosya Erişim ve Paylaşım Güvenliği,
    2.6.1. Paylaştırılmış Klasörlerde Çalışma,
    2.6.2. Dosya ve Klasör Paylaştırırken Dikkat Edilecek Hususlar,
        2.6.2.1. Dosya ve Klasörleri Yetkilendirerek Paylaştırma,
        2.6.2.2. Dosyalara Parola Verme,
2.7. Sistem ve Verilerin Yedeklenmesi,
    2.7.1. Veri Kaybı Nedenleri
        2.7.1.1. İşletim Sistemi Problemleri,
        2.7.1.2. Donanım Hataları,
        2.7.1.3. Kullanıcı Hataları,
        2.7.1.4. Zararlı Program Müdahaleleri,
        2.7.1.5. Saldırgan Kişilerin Müdahalesi,
    2.7.2. İşletim Sisteminin Yedeklenmesi,
    2.7.3. Dosyaların Yedeklenmesi
        2.7.3.1. Yedeklenecek Dosyaların Belirlenmesi,
        2.7.3.2. Yedekleme Zaman Aralıkları,

2.7.3.3. Yedeklerin Tutulacağı Birimler,

2.7.3.4. Yedekleme Dosya İsimleri,

3. TEHDİTLER VE KORUNMA YÖNTEMLERİ

3.1. Zararlı Programlar

3.1.1. Zararlı Program Tanımı,

3.1.2. Zararlı Program Türleri,

3.1.3. Zararlı Programın Bulaşma Yolları,

3.2. Zararlı Programların Oluşturacağı Tehditler

3.2.1. E-posta Hesabı Hırsızlıkları,

3.2.2. Banka Şifreleri ve Diğer Kişisel Bilgi Hırsızlıkları,

3.2.3. İşletim Sistemi ve Programların Çalışmaması veya Yanlış Çalışması,

3.2.4. Dosya/Klasörlerin Göreceği Zararlar,

3.2.5. Bilgisayarda Yapılan İşlemlerin İzlenmesi,

3.2.6. İstek Dışı Kötü Amaçlı Web Sayfalarına Yönlendirme,

3.3. Zararlı Program Bulaşması Durumunda Yapılması Gerekenler,

3.4. Zararlı İnternet Yazılımlarından Korunma

3.4.1. Zararlı Yazılım Türleri,

3.4.1.1. Solucan (Worm),

3.4.1.2. Truva Atı (Trojan),

3.4.1.3. Tuş Kaydedici (Keylogger),

3.4.1.4. Casus Yazılım (Spyware),

3.4.2. Zararlı Yazılım Bulaşma Yolları,

3.4.3. Zararlı Yazılımlardan Korunma Yolları

3.4.3.1. Anti-virüs Yazılımları,

3.4.3.1.1. Kurulumu,

3.4.3.1.2. Ayarları,

3.4.3.1.3. Güncelleştirilmesi,

3.4.3.1.4. Bilgisayarın Taratılması,

3.4.3.2. Anti-Spyware Yazılımları,

3.4.3.2.1. Kurulumu,

3.4.3.2.2. Ayarları,

3.4.3.2.3. Güncelleştirilmesi,

3.4.3.2.4. Yazılım ile Alınabilecek Güvenlik Önlemleri,

3.5. Sosyal Mühendislik

3.5.1. Sosyal Mühendislik Saldırı Yöntemleri,

3.5.1.1. Zararsız Olduğu Düşünülen Bilgiler,

3.5.1.2. Doğrudan Saldırı,
3.5.1.3. Güven Uyandırmak,
3.5.1.4. Yardımcı Olma İsteği,
3.5.1.5. Yardım İsteği,
3.5.1.6. Sahte Web Siteleri,
3.5.1.7. Tehlikeli Program Yamaları,
3.5.2. Sosyal Mühendislik Saldırı Donanımları,
3.5.2.1. Donanımsal Tuş Kaydediciler,
3.5.2.2. Gizlenmiş USB'ler,
3.5.2.3. Gizlenmiş Kameralar,
3.5.3. Şüphe Duyulması Gereken Durumlar,
3.5.4. Sosyal Mühendislik Saldırılarından Korunmak,

4. INTERNET VE AĞ GÜVENLİĞİ

4.1. Güvenlik Duvarı ile Korunma
4.1.1. Güvenlik Duvarı
4.1.1.1. Güvenlik Duvarının Görevleri,
4.1.1.2. Güvenlik Duvarı Programının Kurulumu,
4.1.1.3. Güvenlik Duvarı Ayarları,
4.1.1.4. Güvenlik Duvarı Programının Güncellenmesi,
4.1.1.5. Güvenlik Duvarı Yazılımıyla Alınacak Güvenlik Önlemleri,
4.2. Web Güvenliği
4.2.1. İnternette Güvenli Gezinme Yolları,
4.2.2. HTTP/FTP Erişimlerinde Dikkat Edilmesi Gereken Hususlar,
4.2.2.1. Güvenli İletişim Yolu (HTTPS),
4.2.2.2. Sertifika ve Sertifikanın Geçerliliği,
4.2.2.3. Açılır Pencere Engelleyicisi Kullanımı,
4.2.3. Çocuklar İçin Güvenli İnternet,
4.2.3.1. Ailenin Yapması Gereken Kontroller,
4.2.3.2. Çocuğu Bilinçlendirme,
4.2.3.3. Aile Koruma Yazılımları,
4.2.3.4. Web Sayfası İçerik Filtreleme,
4.2.3.4.1. Uygunsuz İçerik Filtreleme Yazılımı,
4.2.3.4.2. Uygunsuz İçerik Filtreleme Yazılımı Kurulumu,
4.2.3.4.3. Uygunsuz İçerik Filtreleme Yazılımı Ayarları,
4.2.3.4.4. Filtrelemeyle Alınabilecek Önlemler,
4.2.3.5. Konusu Suç Olan İçeriklere Erişimi Önleyici Tedbirler,

4.3. E-posta Güvenliği
4.3.1. İstenmeyen e-posta (Spam)
4.3.1.1. İstenmeyen e-postadan Korunma Yolları,
4.3.1.1.1. Adres Maskeleme,
4.3.1.1.2. Gizli Karbon Kopya (BCC) Kullanımı,
4.3.1.1.3. İstenmeyen e-postaları Cevaplamama,
4.3.1.1.4. Kullanım Amacına Göre Farklı e-Posta Adresi Kullanımı,
4.3.2. Taklit/Oltalama e-postası (Phishing)
4.3.2.1. Taklit/Oltalama e-postasından (Phishing) Korunma Yolları,
4.3.2.1.1. Kişisel Bilgileri e-posta Metnine Yazmamak,
4.3.2.1.2. E-posta Mesajlarındaki İnternet Bağlantılarından Sakınmak,
4.3.2.1.3. Banka Hesaplarını Düzenli Olarak İncelemek,
4.3.3. Aldatmaca e-postası (Hoax)
4.3.4. E-Posta Yazılımları Güvenlik Ayarları,
4.4. ADSL Modem ve Kablosuz İnternet Güvenliği,
4.4.1. Modem ve Kablosuz İnternet Bağlantısını Koruma Yolları,
4.4.1.1. Modem Açma/Kapatma,
4.4.1.2. WEB yönetim Ara Yüzü Parolası,
4.4.1.3. Modem Kablosuz Bağlantı Parolası,
4.4.1.4. İletişim Şifrelemesi (WEP, WPA, WPA2),
4.4.1.5. Kullanılmayan Servisleri (FTP, SNMP, telnet, ICMP vb.) Kapatmak,
4.4.1.6. MAC Adres Filtrelemesi,

5. MOBİL CİHAZLARDA GÜVENLİK

5.1. Güvenlik Konusunda İyi Uygulamalar
5.1.1. Parola ve Cihaz Kilidi,
5.1.2. Kablosuz Ağların Kullanımı,
5.1.3. Uygulama Yükleme,
5.1.4. İşletim Sistemi ve Uygulama Güncelleme,
5.1.5. Cihaz İçeriğinin Temizlenmesi,

6. KİŞİSEL VERİLERİN KORUNMASI VE MAHREMİYET

6.1. İnternet ve İnternette İşlenen Veriler,
6.2. İnternetteki Verilerin Tutulduğu Yerler,
6.3. Paylaşım Yaparken Mahremiyetin Korunması,
6.4. Sosyal Medyada Mahremiyet,

6.5. Mahremiyet, Devlet ve Yasal Haklar,

ÖLÇME DEĞERLENDİRME İLE İLGİLİ ESASLAR

1. Kursiyerin kendi kendine yaptığı tüm öğrenim faaliyetleri,
2. Kurs sonunda yazılı sınavları ve pratik uygulamaları ölçülerek 100 puan üzerinden değerlendirilecektir.

PROGRAMIN UYGULANMASINDA KULLANILACAK ÖĞRETİM ARAÇ GEREÇLERİ

1. Ders kitabı olarak Millî Eğitim Bakanlığının yayınlamış olduğu materyaller kullanılmalıdır.
2. Programın uygulama sürecinde; kaynak ders kitapları, bireysel öğrenme materyalleri ve kaynak ders kitaplarının bulunmaması durumunda öğretmen/öğretici tarafından hazırlanan ders notlarından yararlanılabilir.
3. Programın uygulanabilmesi için bilişim teknolojileri alanı standart donanımları ve programın gerektirdiği diğer donanımlar kullanılacaktır.
4. TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nün bilgi güvenliği farkındalığı konusunda yürütücülüğünü yaptığı internet sitesi olan www.bilgimikoruyorum.org.tr kullanılacaktır.

BELGELENDİRME

Kursu başarı ile tamamlayanlara, kurs bitirme belgesi düzenlenir.