BİLGİSAYAR VE AĞ GÜVENLİĞİ

ÖĞR. GÖR. **MUSTAFA ÇETİNKAYA**

DERS 1 > BİLGİSAYAR VE BİLGİ SİSTEMLERİ GÜVENLİĞİ

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYARLARIN FİZİKİ GÜVENLİĞİ
- BİLGİSAYARLARIN VERİ GÜVENLİĞİ
  - POLİTİKA VE PROSEDÜRLER
  - DONANIM VE YAZILIM ARAÇLARI
  - BAĞLAYICI MEVZUAT

BİLGİSAYAR GÜVENLİĞİ.

- GEREKLİ ÖNLEM VE KONTROLLERİN SAĞLANMASI
  - **GİZLİLİK:** ERİŞİM HAKKI, ŞİFRELER GİBİ
  - **BÜTÜNLÜK:** BEKLENMEDİK OLAYLAR SONUCUNDA DEĞİŞTİRİLEMEME, İNSAN HATASI VEYA TAHRİFAT
  - **KULLANILABİLİRLİK:** KULLANILAMAZ HALE GELMEYİ ENGELLENEME

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR
  - VİRÜS, BİLGİSAYAR KURDU, TRUVA ATI, CASUS YAZILIM...
- BİLGİSAYAR KORSANLARI
  - HACKER vs LAMER
  - CRACKER

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **VİRÜSLER**
- BİLGİSAYAR YAZILIMLARI
- HIZLI ŞEKİLDE YAYILIRLAR
- FARKLI ŞEKİLLERDE BULAŞABİLİRLER

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **SOLUCAN-TROJAN**
- AĞ ÜZERİNDEN SIZMA
- İNSAN MÜDAHALESİ OLMADAN KENDİNİ KOPYALAR
- VERİ TOPLAR

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **TRUVA ATI**
- İYİ GÖRÜNÜMLÜ ZARARLI YAZILIM
- BİR PROGRAM GİBİ GÖRÜNEN VEYA ONUNLA GELEN
- E-POSTA ARACILIĞI İLE GELEBİLİR

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **CASUS YAZILIMLAR**
- ETKİLERİ GÖRÜLMEZ
- VERİ TOPLAR
- SİSTEMİ MANİPÜLE EDER

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **ÇÖP E-POSTA-SPAM**
- BİRDEN FAZLA KİŞİYE GÖNDERİLİR
- REKLAM VEYA DOLANDIRICILIK AMAÇLIDIR
- İÇERİĞİNDE ZARARLI YAZILIMLAR BARINABİLİR

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **SQL ENJEKSİYON**
- BİLGİ ELDE ETME/DEĞİŞTİRME
  - VERİTABANLARI
  - BİLGİ SİSTEMLERİ

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **KAYITÇI-KEYLOGGER**
- KLAVYEDEN GİRİLEN HER ŞEYİ KAYDEDER
  - ŞİFRELER VE YAZILIM ANAHTARLARI
  - BİLGİ ELDE ETME-YAZIŞMALAR

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **KİMLİK SAHTECİLİĞİ**
- BAŞKASI GİBİ GÖRÜNÜR/YANILTIR
- GENELLİKLE E-POSTA VE SMS KULLANILIR
- BAŞKA BİR ADRESE YÖNLENDİRİR

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **SNIFFER-PAKET DİNLEYİCİ**
- AĞ ÜZERİNDEKİ VERİ AKIŞINI KONTROL EDER
- ORTAK ALANDA AĞ KULLANIMI
  - BANKACILIK İŞLEMLERİ ÖRNEĞİ

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **HİZMET ENGELLEME**
- **DOS:** AĞ VEYA WEB SUNUCUSUNUN YANLIŞ İLETİŞİM VE HİZMET İSTEĞİYLE YAVAŞLATILMASI/DURDURULMASI
- **DDOS (DAĞITILMIŞ):** BU İŞLEMİN SAYISIZ NOKTADAN GERÇEKLEŞTİRİLMESİ

BİLGİSAYAR GÜVENLİĞİ.

- KÖTÜ NİYETLİ YAZILIMLAR: **ROBOT AĞLAR-BOTLAR**
- BAŞKA BİLGİSAYARLARIN İZİNLİ VEYA İZİNSİZ SALDIRILARA VEYA İŞLEMLERE DAHİL EDİLMESİDİR
- BULAŞTIĞI YERİN TEKNİK İMKANLARINI KULLANIR
  - TWITTER ÖRNEĞİ #TRENDTOPICOLMAK

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇU NEDİR?
  - BİLGİSAYARLARIN SUÇ HEDEFİ OLMASI
  - BİLGİSAYARLARIN SUÇ ARACI OLMASI

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYARLARIN SUÇ HEDEFİ OLMASI
  - VERİ GİZLİLİĞİNİ İHLAL
  - YETKİSİZ ERİŞİM
  - SAHTEKARLIK AMACIYLA ERİŞİM
  - KASTEN DONANIM VE YAZILIMA ZARAR VERME...

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYARLARIN SUÇ ARACI OLMASI
  - TİCARİ SIR HIRSIZLIĞI
  - TELİF ESERLERİ ÇOĞALTMA-P2P YASAL MI?
  - DOLANDIRMA, TEHDİT, TACİZ
  - HESAP ÇALINMASI...

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **KİMLİK HIRSIZLIĞI**
- KİŞİSEL BİLGİLERİ ÇALMAK
- SOSYAL GÜVENLİK, EHLİYET, KREDİ KARTI...

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **YEMLEME-PHISHING**
- SAHTE WEB SİTESİ OLUŞTURMA
- GERÇEK İŞLETMENİN GÖNDERDİĞİNE BENZER E-POSTA VE MESAJLAR GÖNDERME

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **ŞEYTAN İKİZLER**
  - SAHTE WI-FI HİZMETİ SUNMA
- BİLGİSAYAR SUÇLARI: **DNS TABANLI YEMLEME**
  - DOĞRU WEB SAYFASINA GİRİLSE BİLE BAŞKA WEB SAYFASINA YÖNLENDİRME

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **TIKLAMA HİLESİ**
  - FAZLA TIKLAMA ALMAK İÇİN HİLE YAPMAK
- BİLGİSAYAR SUÇLARI: **SİBER TERÖR-SAVAŞ**
  - ÜLKELERİN KORUMACI VE SALDIRGAN POLİTİKALARI

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **İÇ TEHDİTLER**
  - ÇALIŞANLAR SİSTEMDE İZ BIRAKMAZLAR
  - AYRICALIKLI BİLGİ HAKLARI VARDIR
  - İÇ GÜVENLİK KURALLARI ÖZENSİZDİR
  - SOSYAL MÜHENDİSLİĞE AÇIKTIRLAR

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **İÇ TEHDİTLER-SOSYAL MÜH.**
  - SİSTEMİN KULLANICISINI SOSYAL OLARAK ETKİLEYEREK SİSTEMİN İÇERİSİNE GİRMEK
  - KULLANICI İLE YAKIN DİYALOG KURMAK

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **YAZILIM ZAAFİYETLERİ**
  - SAHTE YAZILIM KULLANMAK, CRACKING
  - WINDOWS GÜNCELLEMELERİ
  - AÇILIŞ PROGRAMLARINI DÜZENLEME
  - YAZILIMCININ BİLİNÇLİ AÇIK BIRAKMASI

BİLGİSAYAR GÜVENLİĞİ.

- BİLGİSAYAR SUÇLARI: **YAZILIM ZAAFİYETLERİ**
  - YAZILIM AÇIKLARI
    - KODLAMA HATALARI
    - LOGIC HATALAR
  - PATCH-YAMA YAPMAK

BİLGİSAYAR GÜVENLİĞİ.

- **ÖNLEMLER:** VİRÜSLERE KARŞI ÖNLEMLER
  - ANTİVİRÜSLER
  - INTERNET SECURITY UYGULAMALARI

BİLGİSAYAR GÜVENLİĞİ.

- ANTİVİRÜS VE INTERNET SECURITY UYGULAMALARI
  - FREE VEYA TAM SÜRÜM, CRACK?
    - FREE: AVG, AVIRA…
    - TAM SÜRÜM: KASPERSKY, BITDEFENDER…
    - MISCROSOFT SECURITY ESSENTIAL?

BİLGİSAYAR GÜVENLİĞİ.

- ANTİVİRÜS VE INTERNET SECURITY UYGULAMALARI
  - GÜNCELLİK SORUNU, ANTİVİRÜS BİLİNEN VİRÜSLERİ BULUR
  - SİTESİNDEN İNDİRME
  - ANTİVİRÜSÜN VİRÜS OLMA DURUMU
  - KALDIRMA SORUNU: NORTON VE AVAST VAKALARI

BİLGİSAYAR GÜVENLİĞİ.

- ANTİVİRÜS VE INTERNET SECURITY UYGULAMALARI ÜÇ ŞEKİLDE KONTROL YAPAR
  - PROGRAM KENDİNİ KOPYALAMAYA ÇALIŞIYOR MU?
  - SİSTEMDEKİ HESAPLARA ERİŞMEYE ÇALIŞIYOR MU?
  - REGISTRY DEĞİŞİKLİĞİ YAPIYOR MU?

BİLGİSAYAR GÜVENLİĞİ.

- VİRÜS TARAMA TEKNİKLERİ
  - E-POSTA VE EKLERİNİN TARANMASI
  - İNDİRİLENLERİN TARANMASI
  - DOSYA TARAMASI
  - BULUŞSAL TARAMA: VİRÜS GİBİ DAVRANMA
  - SANDBOX: İZOLE EDİLMİŞ ALAN

BİLGİSAYAR GÜVENLİĞİ.

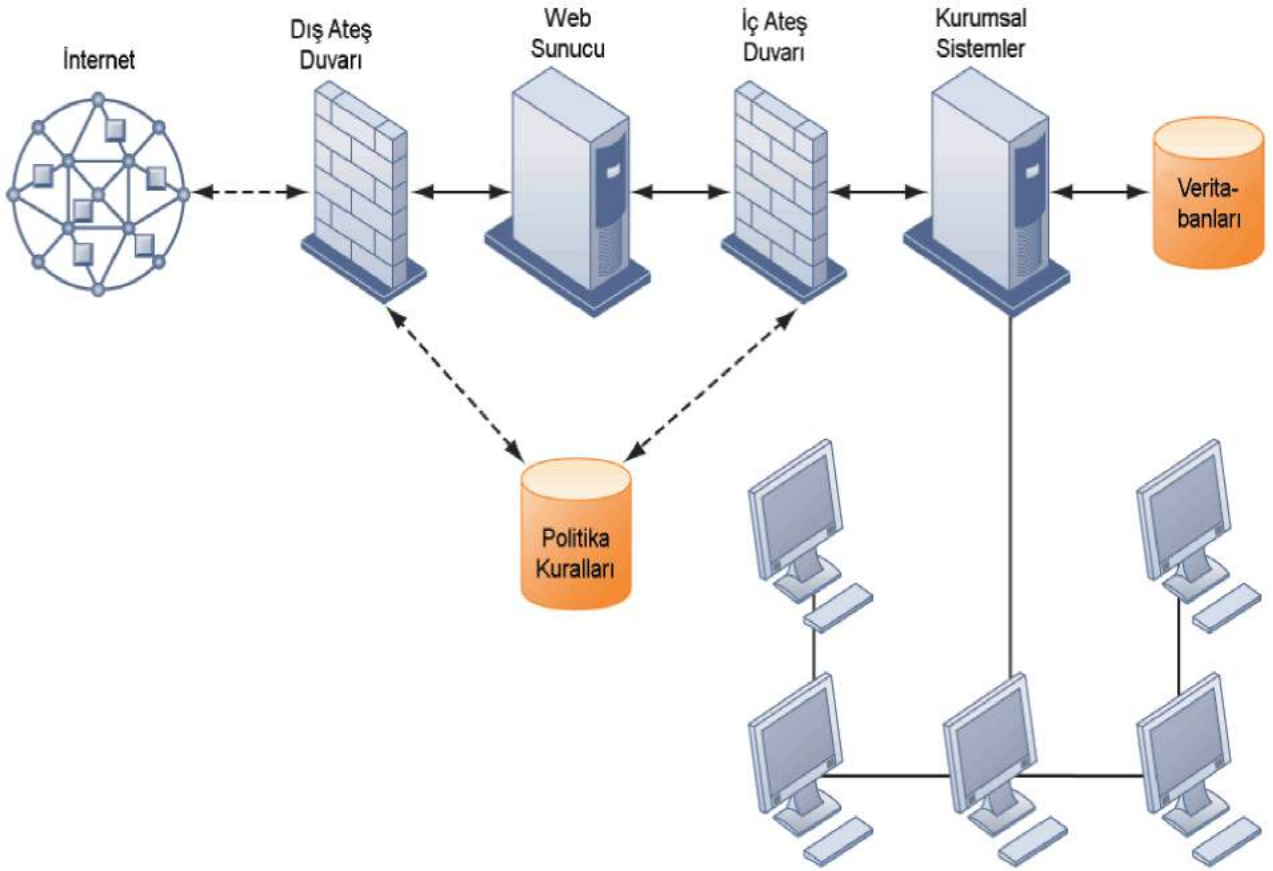
- MAC VE LINUX'E VİRÜS BULAŞMAZ MI?
  - VİRÜSLER NEDEN WINDOWS'A BULAŞIR
  - MAC OSX DOSYA SİSTEMİ NASIL FARKLI?

BİLGİSAYAR GÜVENLİĞİ.

- GÜVENLİK DUVARI-FIREWALL
  - YAZILIM VEYA DONANIM OLABİLİR
  - İNTERNET ÜZERİNDEN GELEN VERİLERİ TARAR
  - BELİRLENMİŞ İSTENMEYENLERE ENGEL OLUR
  - İZİNSİZ VE YETKİSİZ ERİŞİMLERİ DURDURUR
  - WINDOWS İLE BİRLİKTE GELİR

BİLGİSAYAR GÜVENLİĞİ.

- GÜVENLİK DUVARI-FIREWALL



BİLGİSAYAR GÜVENLİĞİ.

- ANTISPYWARE
  - CASUS YAZILIMLARI KONTROL EDER
  - BİLİNEN CASUS YAZILIM LİSTESİ KULLANILIR
  - ANTİVİRÜS, INTERNET SECURITY VE FIREWALL'DAN AYRICA KURULMASI GEREKİR

GÜVENLİK ÇERÇEVESİ.

- SİSTEMLER NEDEN ZAYIF?
  - AĞLARA ERİŞİLEBİLİRLİK
  - DONANIM SORUNLARI (ÇÖKME, YAPILANDIRMA HATASI, HATALI KULLANIM HASARLARI)
  - YAZILIM SORUNLARI (PROGRAMLAMA HATALARI, KURULUM HATALARI, YETKİSİZ DEĞİŞİMLER)

GÜVENLİK ÇERÇEVESİ.

- SİSTEMLER NEDEN ZAYIF?
  - FELAKETLER
  - AĞLARIN/BİLGİSAYARLARIN İŞLETME KONTROLÜ DIŞINDA KULLANIMI, TÜRKCELL ÖRNEĞİ
  - TAŞINABİLİR CİHAZLARIN KAYBEDİLMESİ VE ÇALINMASI, ARAÇ ÖRNEĞİ

GÜVENLİK ÇERÇEVESİ.

- ENFORMASYON SİSTEMİ GÜVENLİĞİ
  - YETKİSİZ ERİŞİM, DEĞİŞTİRME, HIRSIZLIK VEYA FİZİKSEL HASARLARI ENGELLEMEK İÇİN VAR OLAN KURALLAR, YORDAMLAR, TEKNİK TEDBİRLER

GÜVENLİK ÇERÇEVESİ.

- ENFORMASYON SİSTEMİ KONTROLLERİ
  - ÖRGÜT VARLIKLARI İLE İLGİLİ TUTULAN KAYITLARIN DOĞRULUĞUNUN, GÜVENİLİRLİĞİNİN VE YÖNETİM STANDARTLARINA UYUMUNUN KONTROLÜ

GÜVENLİK ÇERÇEVESİ.

- ENFORMASYON SİSTEMİ KONTROLLERİ

Fonksiyon: Borçlar Yer: Peoria, IL		Hazırlayan: J. Ericson Veri: 16 Haziran 2011		Alan: T. Benson Gözden Geçirme Tarihi: 28 Haziran 2011
Zayıflığın Niteliği ve Etkisi	Hata/Suistimal İhtimali		Yönetim Bilgilendirmesi	
	Evet/ Hayır	Gerekçe	Rapor Tarihi	Yönetimin Cevabı
Şifresiz kullanıcı hesapları	Evet	Dışarıdaki yetkisizlere veya saldırganlara karşı sistemi açık bırakır	5/10/11	Şifresiz hesapları kapatın
Ağ bazı sistem dosyalarını paylaşmaya izin verecek	Evet	Kritik sistem dosyalarını ağa bağlı saldırgan şahıslara açık etmekte	5/10/11	Yalnızca gerekli klasörlerin paylaşıldığına ve güçlü şifrelerle korunduklarına emin olun
Yazılım yamaları Standart ve Kontrol grubunun son onayı olmadan üretim programlarını güncelleyebilmekte	Hayır	Tüm üretim programları yönetim onayı gerektirir; Standart ve Kontrol grubu bu tür olayları bir geçici üretim durumu olarak atar		

GÜVENLİK ÇERÇEVESİ.

- ENFORMASYON SİSTEMLERİNDE KONTROL
  - YAZILIM & DONANIM
  - BİLGİSAYAR İŞLEMLERİ
  - VERİ GÜVENLİĞİ
  - UYGULAMA
  - YÖNETİM

GÜVENLİK ÇERÇEVESİ.

- YAZILIM VE DONANIM KONTROLLERİ
  - SİSTEM VE UYGULAMA YAZILIMLARINA İZİN ERİŞİMİ ENGELLER
  - TEÇHİZATLARI, BAKIM VE ARIZALARI KONTROL EDER
  - YEDEKLEME VE KURTARMA PROSEDÜRLERİ İLE İLGİLENİR
  - YAZILIM KALİTESİ TESTLERİ

GÜVENLİK ÇERÇEVESİ.

- BİLGİSAYAR İŞLEMLERİ KONTROLLERİ
  - BİLGİSAYARLARDA RUTİN TANIMLANMIŞ HİS
  - ORTA DÜZEY YÖNETİME HİZMET VEREN SİSTEMLER

GÜVENLİK ÇERÇEVESİ.

- VERİ GÜVENLİĞİ KONTROLÜ
  - İŞ VERİLERİNİN YETKİSİZ ERİŞİM, DEĞİŞTİRİLME VE YOK EDİLMEYE KONU OLMAMASINI SAĞLAR
- UYGULAMA KONTROLLERİ
  - SİSTEM GELİŞTİRME SÜREÇLERİNİ KONTROL EDER

GÜVENLİK ÇERÇEVESİ.

- YÖNETİM KONTROLLERİ
  - STANDARTLAR, KURALLAR, PROSEDÜRLER VE KONTROL DİSİPLİNLERİNİ SOMUTLAŞTIRIR

GÜVENLİK ÇERÇEVESİ.

- **RİSKLER VE FELAKETLER**
  - RİSK EYLEM PLANI
  - FELAKET EYLEM PLANI
  - İŞ SÜREKLİLİĞİ PLANI

GÜVENLİK ÇERÇEVESİ.

- **KİMLİK DOĞRULAMASI**
  - ŞİFRELER
  - BİYOMETRİK DOĞRULAMA
  - AKILLI KARTLAR

GÜVENLİK ÇERÇEVESİ.

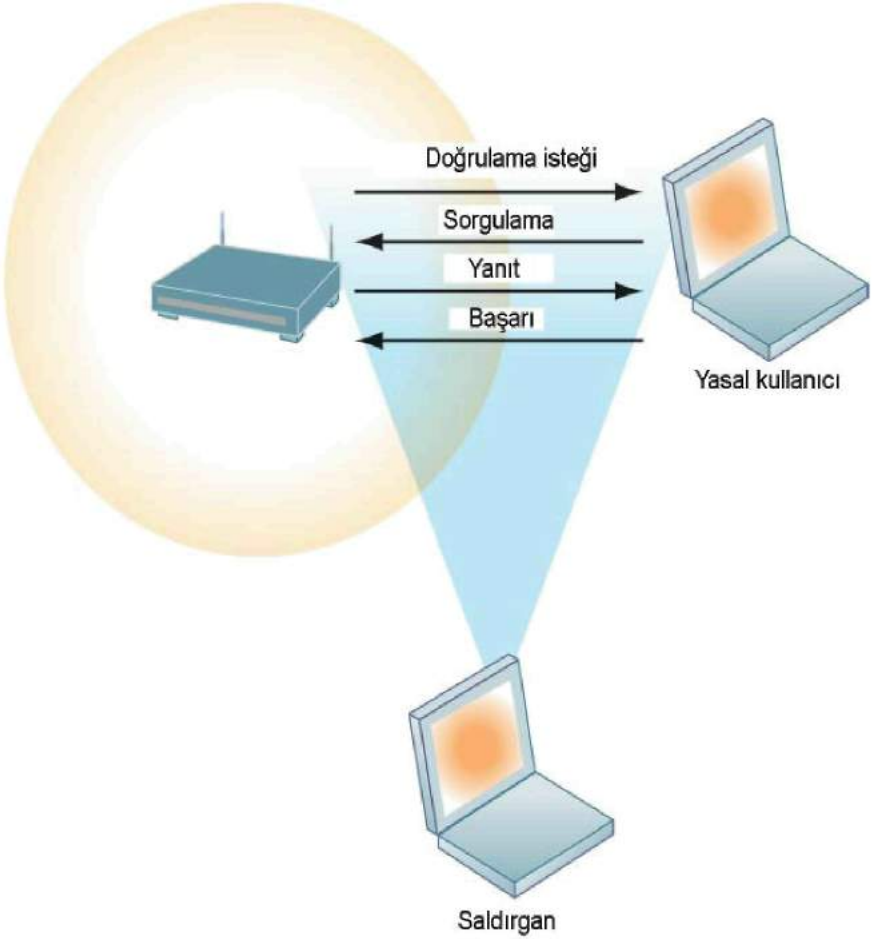
- **ADLİ BİLİŞİM**
  - MAHKEMEDE KANIT OLABİLECEK VERİLERİ TOPLAR, İNCELER, DOĞRULAR, KORUR VE ANALİZ EDER
  - ORTAM VERİLERİNİ (GÖRÜNÜR OLMAYAN VERİLERİ) AÇIĞA ÇIKARIR

GÜVENLİK ÇERÇEVESİ.

- KİMLİK DOĞRULAMASI: **ŞİFRELER**
  - Samsun123 sinop57
  - 1453 1903
  - AykP#.@KsTza.

GÜVENLİK ÇERÇEVESİ.

- WI-FI GÜVENLİĞİ
- 192.168.1.1
- WPA2



GÜVENLİK ÇERÇEVESİ.

- BULUT GÜVENLİĞİ
- AKILLI TELEFON GÜVENLİĞİ
  - BLUETOOTH (AÇIK BLUETOOTH)
  - MOBİL UYGULAMALAR

GÜVENLİK ÇERÇEVESİ.

- GÜVENLİ E-TİCARET
  - HTTPS VE RENKLENDİRME
  - GÜVENLİK SERTİFİKALARI
  - GEÇMİŞ TECRÜBELER

GÜVENLİK ÇERÇEVESİ.

- SOSYAL AĞLAR
  - SAHTECİLİK
  - YÜZYÜZE TANINMAYAN KİŞİLERLE ARKADAŞLIK
  - ÇOCUKLARA YÖNELİK TEHDİTLER
  - SİBER/SANAL ZORBALIK