

# GEMLİK CELAL BAYAR ANATOLIAN HIGH SCHOOL

eTwinning kulübü öğrencileri





# E-GÜVENLİK



➔ İnternet güvenliđi, yalnızca internet, tarayıcı güvenliđi ile ilgili deđil, aynı zamanda ađ güvenliđi, uygulama ve işletim sistemleri ile bir bütün olarak ilgilidir.



➔ İnternet, bilgi alışverişi için güvenli olmayan bir kanalı temsil eder; bu da kimlik avı, çevrimiçi virüsler truva atları, solucanlar ve daha fazlası gibi yüksek bir saldırı veya dolandırıcılık riskine yol açar.





# SORUNLAR



➔ E-dolandırıcılık Kimlik avı, çevrimiçi kullanıcıları kullanıcı adı, şifre ve kredi kartı bilgileri gibi hassas bilgilerini ele geçirmeyi hedefleyen bir saldırıdır.





➔ Kurbanlar, sahte e-postalar, anlık mesajlaşma, sosyal medya veya diğer yollar aracılığıyla meşru görünecek şekilde tasarlanmış sahte web sayfalarına yönlendirilir



➔ Uygulama güvenlik açıkları internet kaynaklarına erişmek için kullanılan uygulamalar hatalı kimlik doğrulama kontrolleri gibi güvenlik açıkları içerebilir .



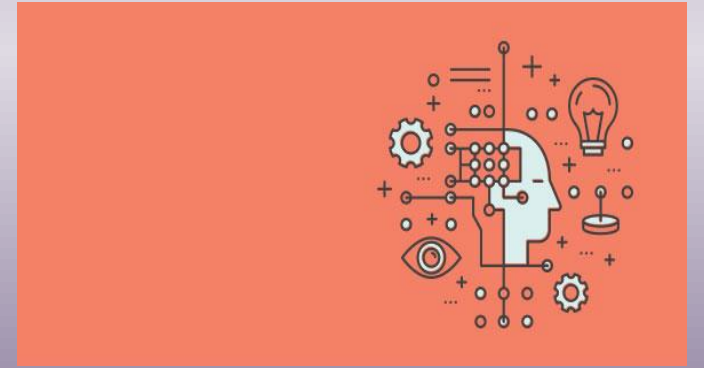


➔ Bu hataların en şiddetli olanı ağ saldırganlarına bilgisayar üzerinde tam kontrol verebilir. Birçok güvenlik uygulaması bu tür saldırılara karşı yeterli savunmaya sahip değildir.





# ÇÖZÜMLER



➔ Antivirüs virüsten koruma yazılımı ve internet güvenlik programları, programlanabilir bir aygıtı kötü amaçlı yazılımları algılayıp ortadan kaldırarak saldırılara karşı koruyabilir.



➔ Antivirüs yazılımı internetin ilk yıllarında ağırlıklı olarak Shareware'di, bütün platformlar için internet üzerinde seçilebilecek pek çok ücretsiz antivirüs yazılımı bulunmaktadır.







- Marco Verch- Flickr

## **En çok kırılan şifre 123456**

NCSC ayrıca '123456' şifresini kullanan 23.2 milyon kişiye ait hesapların internet korsanları tarafından kırıldığını açıklanırken, 123456789 şifresinin de yaklaşık 8 milyon vakada dolandırıcıların eline geçtiğini duyurdu.

İsim olarak en çok kullanılan ve kırılan şifrelerse ashley, michael, daniel, jessica ve charlie olarak kayıtlara geçti.

# DÜNYADAKİ EN POPÜLER İNTERNET ŞİFRELERİ



2019	Önceki Yıla Göre Değişim
● <b>123456</b> (ya da çeşitleri)	0
● <b>qwerty</b> (Q klavye)	+3
● <b>password</b> (şifre)	-1
● <b>iloveyou</b> (seni seviyorum)	+2
● <b>111111</b>	-2
● <b>123123</b>	+6
● <b>abc123</b>	+4
● <b>qwerty123</b>	+12

2018	Önceki Yıla Göre Değişim
● <b>123456</b> (ya da çeşitleri)	0
● <b>password</b> (şifre)	0
● <b>111111</b>	Yeni
● <b>sunshine</b> (güneş, güneş ışığı)	+44
● <b>qwerty</b> (Q klavye)	-2
● <b>iloveyou</b> (seni seviyorum)	0
● <b>princess</b> (prenses)	Yeni
● <b>admin</b> (yönetici)	-1

TRT HABER

www.trthaber.com

Kaynak: SplashData, Statista



Ankete göre internet kullanıcılarının yarısından çoğu, e-posta, sosyal medya ya da alışveriş yaparken birbirinden farklı şifre kullanmadıklarını ve bu şifrelerin kırılmasının ya da tahmin edilmesinin zor olmadığını ifade etti. Son 2 senede şifrelerinin kırılarak para kaybettiklerini söyleyenlerin oranıysa yüzde 12 olarak kayda geçti.

## Şifre alırken dikkat, 123456 şifresi 23 milyon kez 'hack'lendi

Kerem Congar • 23/04/2019



Çok faktörlü kimlik doğrulama “Multi Factor Authentication”

→ (MFA), bir kullanıcıya yalnızca bir kimlik doğrulama mekanizmasına birkaç ayrı kanıt parçasını başarılı bir şekilde sunduktan sonra erişim izni verilen bir bilgisayar erişim kontrolü yöntemidir



➔ Web siteleri ve e-posta gibi internet kaynakları çok faktörlü kimlik doğrulama kullanılarak güvence altına alınabilir.









# E-Güvenlik için bazı ipuçları

- ▣ Antivirüs Programı kullanmak
- ▣ Kişisel Firewall (Ateş Duvarı) Programı kullanmak
- ▣ E-posta güvenliğini sağlamak
- ▣ İşletim sistemi güvenliğini araştırmak
- ▣ Bilgisayarınızın fiziki güvenliğini sağlamak
- ▣ Şifre kullanımını arttırmak ve farklı türde şifre kullanmak
- ▣ Akıllı Şifre ve Mobil İmza kullanımı - Tek Kullanımlık Şifre Teknolojisi

# SMARTthinking



<h1>S</h1>	<p>Safe</p>   <p><b>STOP</b> and <b>THINK</b> Will the information you share keep you safe?</p>
<h1>M</h1>	<p>Meeting</p>  <p><b>STOP</b> and <b>THINK</b> Are your online friends who they say they are?</p>
<h1>A</h1>	<p>Accepting</p>  <p><b>STOP</b> and <b>THINK</b> How do you know files and pictures are safe?</p>
<h1>R</h1>	<p>Reliable</p>  <p><b>STOP</b> and <b>THINK</b> How do you know that people or pages aren't lying?</p>
<h1>T</h1>	<p>Tell</p>  <p><b>STOP</b> and <b>THINK</b> Who can you tell if you feel uncomfortable about something online?</p>







# TARİHÇE





➔ 1972'de Mısırlı mühendis Mohamed M. Atalla uzaktan PIN doğrulama sistemi için U.S. Patent 3.938.091 bir patent aldı.



## ➔ Esafetylabel.eu sayfasında alınan e güvenlik etiketinin amacı nedir?

Avrupa genelindeki okullarda çevrim içi güvenliğin temel, güçlü ve zayıf yönlerinin belirlenmesine ve iyileştirme alanlarının öğrenilmesine olanak sağlamıştır.





**Temmuz 2022 ye kadar etiketimiz var**

# HAZIRLAYANLAR VE SUNANLAR

- ▣ Nilüfer.Y
- ▣ Kağan Kayra.Ç
- ▣ Elif Selay.S
- ▣ Başak.Z
- ▣ Aleyna.Y
- ▣ Emirhan.B
- ▣ Fatmanur.B
- ▣ Gülçin.A

