İNTERNETİN GÜVENLİ KULLANIMI REHBERİ

SİBER GÜVENLİK OKULLARDA ERASMUS PROJESİ

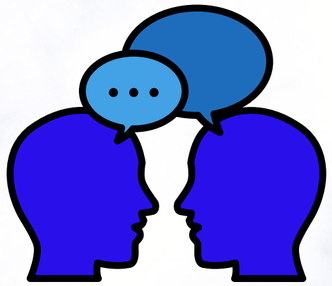
2020-1-TR01-KA229-094378_1

Turkish

TÜRKİYE ULUSAL AJANSI
TURKISH NATIONAL AGENCY

Erasmus+

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



GÜVENLİ İNTERNET KULLANIM REHBERİ

IES Antonio Menarguez costa.Los Alcazares-İSPANYA

KTSO VOCATIONNAL HIGH SCHOOL TÜRKİYE

10 GEL Agiou Dimitriou Athens YUNANİSTAN-

Escola Secundaria Campos de Melo,Covilha-PORTEKİZ

IPSCEOA"N.Gallo" di Agrigento-İTALYA






- Cihazlarınız çok sayıda özel Bilgi depolar

Mobil cihazlarımızı korumanın ana nedenlerinden biri, kişisel bilgilerimizi ve iletişim kurduğumuz kişilerin (kişiler, fotoğraflar, videolar, e-postalar vb.) ve kaybetmek veya üçüncü kişilerin eline geçmesini istemediğimiz kişisel bilgilerimizi korumaktır.

İpuçları ve öneriler

Kayıp veya hırsızlık riski her zaman var olacaktır. Öyleyse:

- Bir ekran kilidi yöntemi (sayısal kod veya desen) kullanın ve bilgileri şifreleyin, böylece bu durum ortaya çıkarsa, cihazı elinde tutan kişinin erişimini zorlaştırmış olursunuz.

- Cihazı bulmanıza, kilitlemenize ve hatta üzerinde depolanan bilgileri silmenize yardımcı olacak güvenlik araçlarından yararlanın.

- Ne olursa olsun, cep telefonunuzda veya tabletinizde depolanan bilgileri kaybetmemek için diğer ortamlarda yedek kopyalar oluşturun:

İNTERNETİN GÜVENLİ KULLANIMI

Kimsenin şifrelerinizi tahmin etmesine izin vermeyin

En az 8 karakterden oluşan ve aşağıdakilerden oluşan güçlü veya sağlam parolalar seçin:

büyük harf (A, B, C...) küçük harf (a, b, c)

sayılar (1, 2, 3) ve özel karakterler (5. &. #...)

Aşağıdaki gibi Tahmin edilmesi kolay şifreler KULLANMAYIN:

12345678", "qwerty", "aaaa"
aile adları, araç plakaları vb.

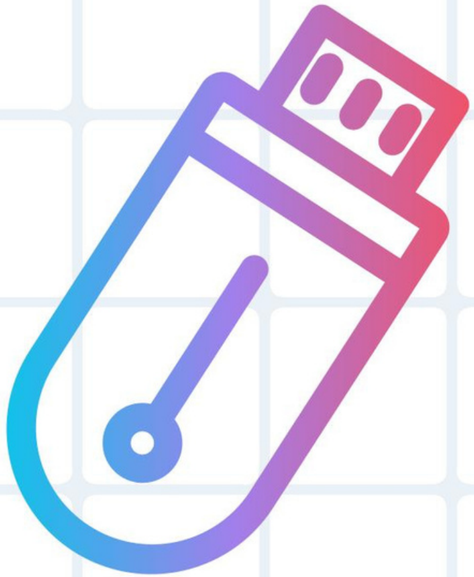
Şifrelerinizi PAYLAŞMAYIN. Bunu yaparsanız, artık gizli olmayacak ve diğer insanlara erişim izni vermiş olacaksınız.

gizliliğinize. Aynı parolayı birden fazla hizmette KULLANMAYIN.

Sorun beklemeyin, yedek kopyalar oluşturun.

Yanlışlıkla silme, bilgi kaybının en yaygın nedenlerinden biridir. Tek olmamasına rağmen,akıllı telefon ,tablet,dizüstü bilgisayar,harici disk ,flash sürücü gibi bilgiyi içeren cihazın kaybolması, kaza geçirmesi veya çalınması nedeniyle bilgileri şifreleme veya silme yeteneğine sahip bir virüsün eyleminden veya aygıt düzgün çalışmayı durdurması nedeniyle de kaynaklanabilir.

- **Hiçbir koşulda kaybetmek istemeyeceğiniz bilgileri seçin.**
- **Bilgileri depolayacağınız ortamı seçin.**
- **Yedeklemeyi yapın.**
- **Kopyalarınızı periyodik olarak tekrarlayın.**



İNTERNETTE GEZİNİRKEN ATTIĞINIZ ADIMLARI ORTADAN KALDIRMAK ÖNEMLİDİR.

İnternette gez n rken, varsayılan olarak tarayıcı le gerçekleşt rd ğ n z tüm şlemler, doğrudan b lg sayarınızın veya c hazınızın hafızasında saklanır, kaybolmaz, böylece nternette bel rl b r zamanda attığınız tüm adımları b lmen z mümkün olur.

İNTERNETTE GEZİNİRKEN RİSKLERİ EN AZA İNDİRECEK ÖNLEMLER:

- TARAYICINIZI GÜNCEL TUTUN. GÜVENİLİR EKLENTİLERİ VE EKLENTİLERİ SEÇİN
- GENELLİKLE BÜYÜK ANTİVİRÜSLER TARAFINDAN SAĞLANAN BİR WEB SAYFASI DENETLEYİCİSİ YÜKLEYİN.
- ERİŞİM KODLARINIZI SAKLAMAK VE KORUMAK İÇİN BİR PAROLA YÖNETİCİSİ KULLANIN:
- KULLANICI ADI VE ŞİFRE İLE KİMLİĞİNİZİ DOĞRULADIĞINIZ BİR SAYFADAN AYRILDIĞINIZDA HER ZAMAN OTURUMU KAPATIN.

E-postanızı korumanız gere kir.

E-posta, hem işte hem de özel alanınızda size birçok olanak sunan bir araçtır.Ancak kullanırken dikkatli olmalısınız, bu nedenle aşağıdaki önerileri uygulayın:

Güçlü bir parola kullandığınızdan emin olun. Bir hizmet bunu sağladığında, fazladan bir güvenlik katmanı eklemek için 2 Adımlı Doğrulamayı açın.

Başka seçeneğiniz yoksa gizliliğinizi tehlikeye atabilecek bilgiler vermekten kaçının,dosyaları yalnızca e-postanın alıcısının ve sizin bildiğiniz bir parola ile şifreleyin ve sıkıştırın.

Bilinmeyen kullanıcılardan gelen e-postaları açmayın ve onları silin: kötü amaçlı yazılım içeren dosyalar, kötü amaçlı sayfalara bağlantılar veya bir varlığın kimliğini taklit eden dosyalar içerebilirler.

E-postayı gönderen kişi biliniyor olsa bile, mesaj size şüpheli görünüyorsa, o kişinin e-posta adresini tahrif etmediğini doğrulamak için doğrudan o kişiye danışın.

•Yedek kopyalar almayı unutmayın.Böylece posta sunucusuyla ilgili bir sorun olması durumunda ,değerli bilgilerinizi kaybetmemiş olursunuz.

Anlık mesajlasma hizmetlerinde riskler

WhatsApp ve diğer anlık mesajlaşma uygulamaları birçok işlevi bünyesinde barındırır: metin mesajları, videolar, fotoğraflar gönderme/alma... ve bu nedenle, e-posta ve sosyal ağlar gibi diğer İnternet hizmetleriyle ilişkili risklere maruz kalırlar: istenmeyen e-posta, aldatmacalar, dolandırıcılık, dolandırıcılık, kötü amaçlı yazılım vb.

Durumunuzu kendiniz hakkında özel bilgi vermek için kullanmayın

Hakkınızda bilgilerin herkese açıklanmasını istemiyorsanız, yaymamak daha iyi. Fazla taviz vermeyen bir profil fotoğrafı kullanın. İletim kurmak istemediğiniz kullanıcıları engelleyin.

Mesaj alışverişinin şifreli olduğundan emin olun.
Mesajlarınızı kaybetmek istemiyorsanız yedek kopyalar oluşturun.

Giyilebilir Teknolojik cihazların güvenliği.

Giyilebilir bir cihaz ile kişisel aktivitenizi izlemek istiyorsanız, seçmeden önce size en iyi özellikleri sunanı arayın, ancak kişisel bilgilerinizin doğru kullanım ve işlemini yapabilmesi için size en iyi güvenlik ve gizlilik garantilerini de sunması gerektiğini unutmayın.

Bilgilerinizin gizliliğini garanti eden bazı şifreleme mekanizmalarını kullanmaları gerekir.

Şimdi kendinize şu soruları sormalısınız: Sosyal medyada hangi bilgileri paylaşıyorsunuz?

Kişisel bilgilerinize kimin erişimi olduğunu bilmelisiniz.

Uygulamaya kişisel verilerinizi işlemesi için hangi izinleri verdiğiniz önemlidir.

Bilgileriniz bulutta saklanıyor mu? Kim erişebilir? Verilerinizi ne kadar süreyle saklamak istiyorsunuz?

KTSO MESLEKİ VE TEKNİK ANADOLU LİSESİ TÜRKİYE

Erasmus+

Keşan Ticaret ve Sanayi Odası Mesleki ve Teknik Anadolu Lisesi

ZORBALIĞA UĞRUYORSAM NE YAPABİLİRİM

- Gerektiğinde kullanmak üzere rahatsız edici içeriğin resimlerini çekerek kanıt toplayabilirsiniz. Bu kanıt, yasal haklarınızı kullanmanızda yararlı olabilir.
- Zorbalığı bildirerek, zorbaya davranışının yanlış olduğunu ve cezalandırılacağını da gösteririz.
- Acil bir tehlike altındaysanız (sürekli aranıyor ve rahatsız ediliyorsunuz, konumunuz takip ediliyor vb.) polise başvurabilirsiniz.

Truva Atı Virüsü Nedir?

Truva atı, meşru bir program kılığında bir bilgisayara indirilen bir kötü amaçlı yazılım türüdür. Truva atı, tipik olarak bir saldırganın meşru yazılım içindeki kötü amaçlı kodu gizlemek için sosyal mühendislik kullandığını gören dağıtım yöntemi nedeniyle adlandırılır. Ancak, bilgisayar virüsleri veya solucanların aksine, bir Truva atı kendi kendine çoğalmaz, bu nedenle geçerli bir kullanıcı tarafından yüklenmesi gerekir. Bir cihazda etkin olan bir Truva atının belirtileri, bilgisayar ayarlarının beklenmedik bir şekilde değiştirilmesi gibi olağandışı etkinlikleri içerir.

Truva atlarından nasıl kaçınılır?

Güvenlik programları, truva atlarının indirilmesini engelleyebilir.

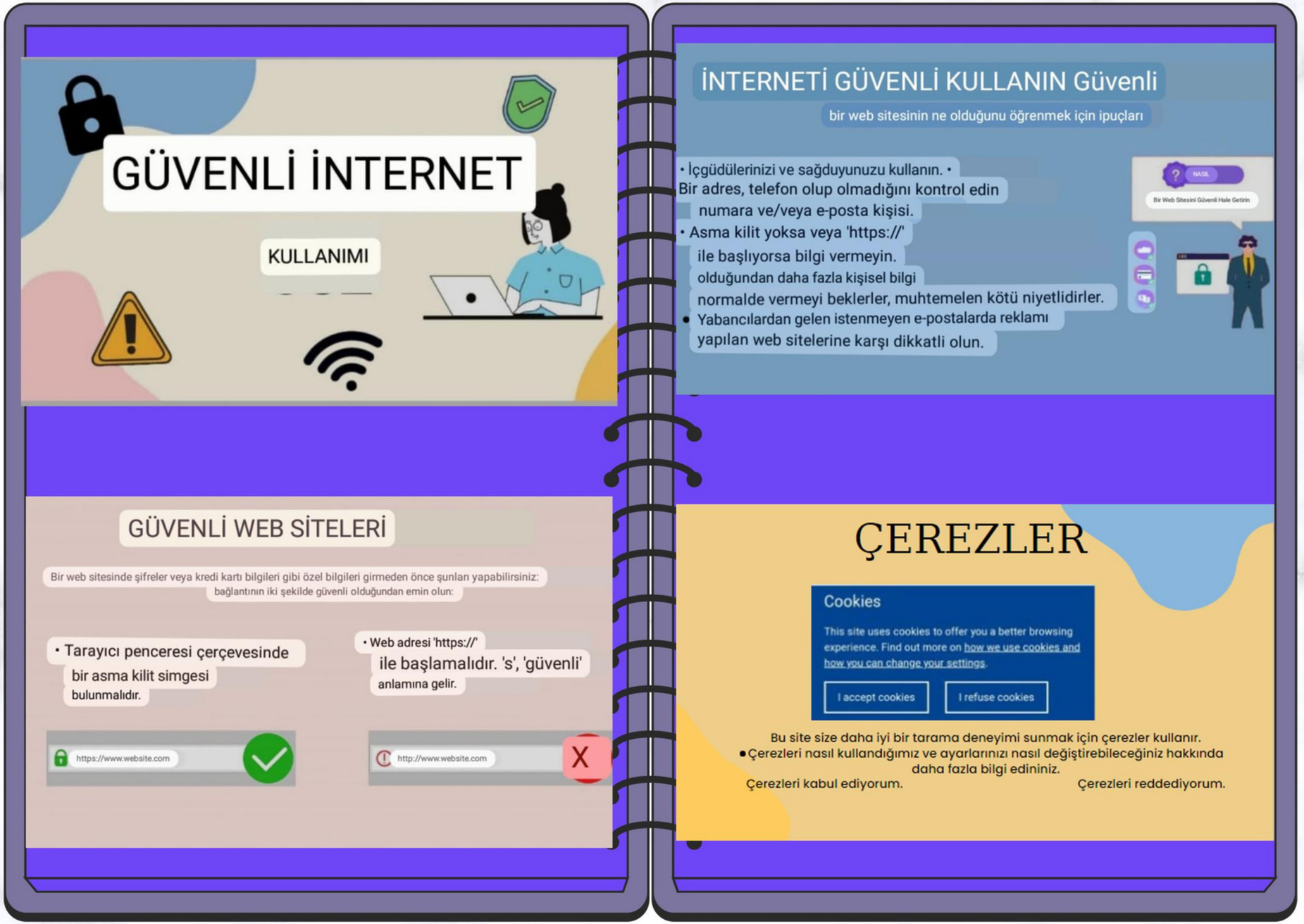
BİR SİBER ZORBANIN ÖZELLİKLERİ

- Yüz yüze iletişimde genellikle zorbadır.
- Okul başarısı genellikle düşüktür.
- Problem çözme becerileri düşüktür.
- Öfke, üzüntü, hayal kırıklığı gibi duygularını anlamakta ve düzenlemekte zorlanır.
- İnternette söylediklerini o kişinin yüzüne söylemesi pek olası değil.

Sunumu görmek için QR kodu okutunuz.

IES Antonia Menarguez Costa. Los Alcazares

İSPANYA



Slaytı görmek için QR kodu okutunuz.

1o GEL Agiou Dimitriou Athens

YUNANİSTAN

Özel hayatınızı koruyun

İnternetteki paylaşım verilerinize sadece aile üyelerinize, yakın arkadaşlarınıza ve gerçek hayatta tanıdığınız ve güvendiğiniz kişilere erişim vererek gizliliğinizi sınırlandırın.

Sosyal medyadaki gizlilik ayarlarınızı, yüklediklerinizi yalnızca daha önce bahsedilen kişilerin görmesine izin verecek şekilde düzenleyin.

Çevrimiçi tanıştığınız biriyle asla yüz yüze görüşmeyin. Bunu yapmaya karar verirseniz, anne babanıza veya güvendiğiniz bir yetişkine haber verin, hatta onlardan birini yanınıza alın.

İnternette paylaşamadıklarımız

HİÇBİRZAMAN!

Kişisel veri
ev adresleri
internet adresleri
Kişisel Fotoğraflar
Çıplak Fotoğraflar
Çevrimiçi video

HİÇBİRZAMAN!

Sahte Haber mi?

- İnternette okuduğunuz her şey her zaman doğru olmayabilir.
- İnsanlar bunu gerçeği kolayca çarpıtmak ve sizi istedikleri şeye yönlendirmek için kullanıyor.
- Bilgi kaynağını ve bunları yaymak için kullanılan siteyi kontrol edin
- Okuduklarınızı kabul etmeden önce iki kez düşünün

geri

Genel kural!

İnternete bir şey yükleyip yüklememeye karar vermeniz gerekiyorsa, Sokakta ilk kez gördüğün bir yabancıyla bunu paylaşıp paylaşmayacağını sor kendine!

Slaytı görmek için QR kodu okutunuz.

IPSCEOA"N.Gallo" di Agrigento

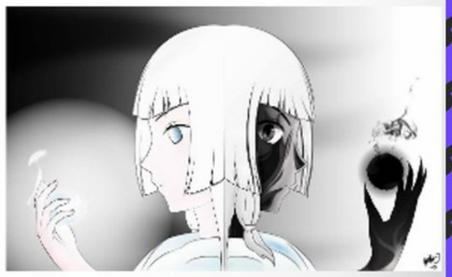
ITALYA

I.I.S.S.
"GALLO"
AGRIGENTO

Presentation IPSCEOA
GALLO

ZORBALIK VE
SİBERZORBALIK
Aynı Madalyonun İki Yüzü mü?

Aslında biz gençlerin alışkanlıkları çok değişti ve daha önce hayatımız düzenli bir şekilde okullar,diğerAktiviteler,diğer sporlar veya belki sadece arkadaşlarla akşamlar şekilde geçiyorsa,şimdi herşey farklı. Biraz korkudan,biraz alışkanlıktan, biraz bağımsızlıktan,evimiz odamız ve güvenliğimizin simgesi haline gelen bilgisayar ve cep telefonumuz dışında normal yaşamayı yeniden düşünmek zorlaştı.



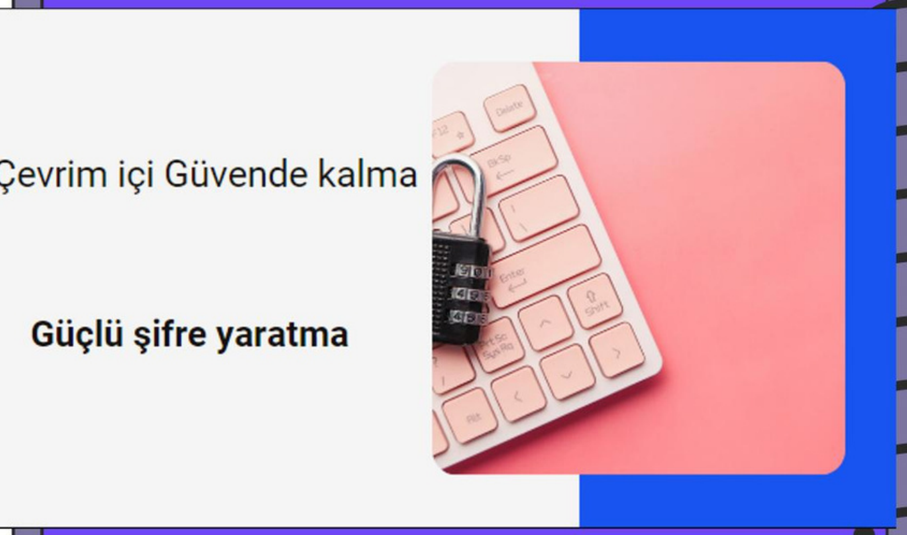
Aslında pandemi sürecinde uzaktan eğitimle kıyaslama yapmak için çok az fırsatımız oldu ve kendimizi yalnız hissettik,Bizi güvende hissettiren soğuk bir ekranın önünde yalnızdık.Buda bizi yavaş yavaş''Gerçek'' ve gerçek duyguları artık algılamamaya ve çoğu zaman karşı tarafa bir robot değil,gerçek duyguları,gerçek hisleri ve gerçek kırılganlığımızı ya da bizi etkileyen ve başkalarının hayatlarına ağır ve saldırgan resimler,videolar,kelimeler,yazmalar yaydığımız fark etmeyiz.

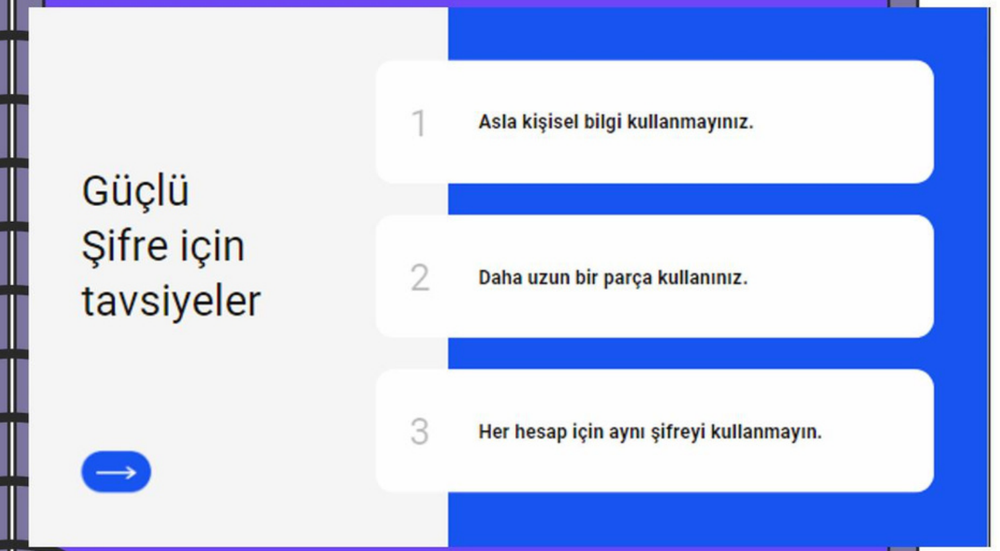
Evrensel Önlem:
Öğrenciler Ve Kız Öğrenciler

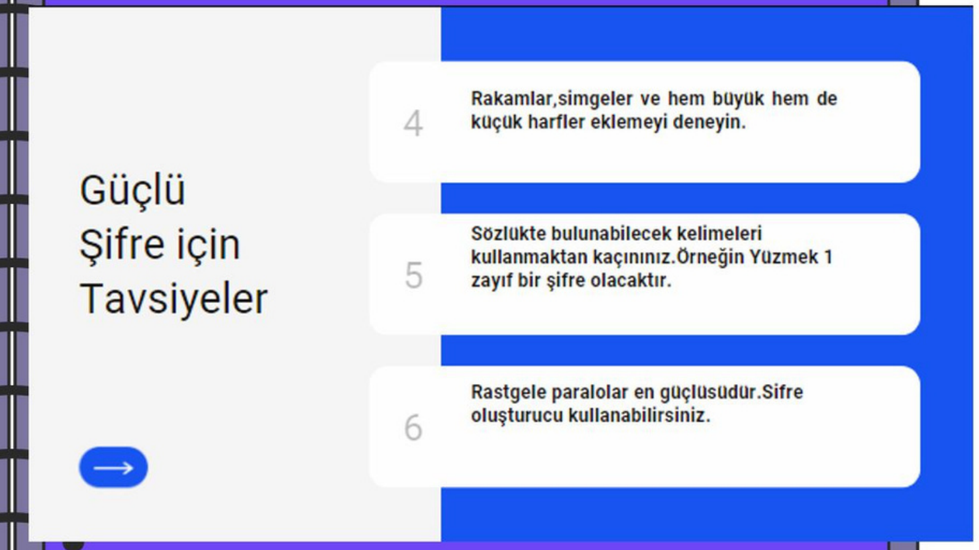
Slaytı görmek için QR kodu okutunuz.

Escola Secundaria Campos de Melo,Covilha

PORTEKİZ







Slaytı görmek için QR kodu okutunuz.

GUIDEBOOK OF SAFE USE OF INTERNET

English

Collaborative Guidebook

IES Antonio Menárguez Costa. Los Alcázares - Spain

KTSO VOCATIONAL HIGH SCHOOL TURKEY

1o GEL Agiou Dimitriou Athens - Greece

Escola Secundária Campos de Melo, Covilhã - Portugal

IPSCEOA "N. Gallo" di Agrigento - Italia

Your devices store a lot of private information.

One of the main reasons to protect our mobile devices is to safeguard our personal information and that of those with whom we communicate: contacts, photographs, videos, emails, etc., and that we would not like to lose or fall into. hands of third parties.

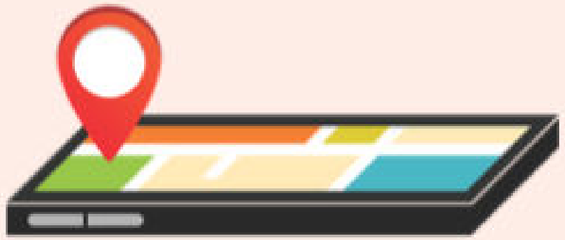
Tips and recommendations

The risk of loss or theft will always exist. Therefore:

◆ Use a screen lock method (numerical code or pattern) and encrypt the information so that if this situation occurs, you make it difficult for the person who ends up with the device in their hands to have access.

◆ Make use of security tools that will help you locate the device, lock it and even delete the information stored on it.

◆ Make backup copies on other media so that, no matter what happens, you don't lose the information stored on the mobile or tablet.



Don't let anyone guess your passwords

Choose strong or robust passwords
at least 8 characters and composed of:

- uppercase (A, B, C...)
- lowercase (a, b, c...)
- numbers (1, 2, 3...)
- and special characters ($, &, #...)
- DO NOT use easy-to-guess passwords such as:

"12345678", "qwerty", "aaaaa",family names, vehicle license plates, etc.

- DO NOT share your passwords.

If you do, it will no longer be secret and you will be giving other people access to your privacy.

- DO NOT use the same password on multiple services.

Don't wait for a problem, make backup copies.

Accidental deletion is one of the most common causes of loss of information, although it is not the only one, can also be due to the action of a virus capable of encrypting or deleting the information, due to the loss, accident or theft of the device that contains the information: smartphone, tablet, laptop, external hard drive , flash drive or because the device stops working correctly.

1. Select the information that under no circumstances would you like to lose.

2. Choose the media where you will store the information.

3. Make the backup.

4. Repeat your copies periodically.

It is important to eliminate the steps you take when you browse the internet.

When you browse the Internet, by default all the activity you have carried out with the browser is stored directly in the memory of your computer or device, it does not disappear, in such a way, that it is possible to know all the steps you took at a given time on the Internet.

Measures to minimize the risks when you browse the Internet:

- Keep your browser up to date.
- Choose trusted add-ons and plugins.
- Install a web page checker, usually provided by major antiviruses.
- Review the browser configuration options and enable those that you consider most interesting to protect your privacy and keep you safer.

- Clear browsing history.
- Delete cookies.
- Use a password manager to store and safeguard your access codes.
- Always close the session when you leave a page where you have authenticated yourself with a username and password.

You must protect your email.

Email is a tool that offers you many possibilities, both at work and in the private sphere, but you have to be careful when you use it, therefore, apply the following recommendations:

- Make sure you use a strong password.
- Whenever a service provides it, turn on 2-Step Verification to add an extra layer of security to the checkout process authentication.
- Avoid providing information that could compromise your privacy, if you have no other choice, encrypt or compress the files with a password that only the recipient of the email and you know.
- Do not open emails from unknown users and delete them: they could contain files with malware, links to malicious pages or that impersonate the identity of some entity.
- Even if the sender of the email is known, if the message seems suspicious to you, consult that person directly to confirm that they have not falsified their email address.
- Don't forget to make backup copies so that you don't lose valuable information in the event of a problem with the mail server.

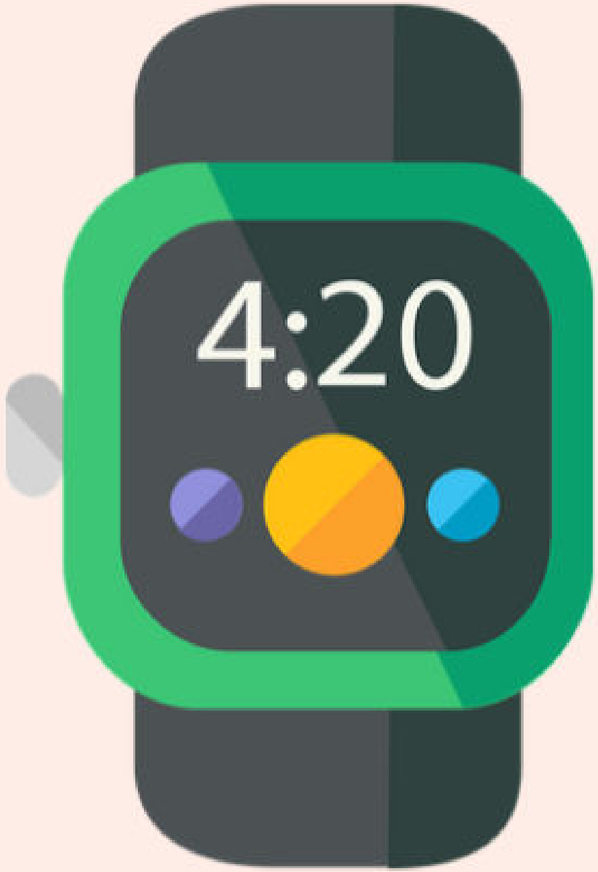
Risks in instant messaging services

WhatsApp and the rest of the instant messaging applications incorporate many functionalities: send/receive text messages, videos, photos... and as such, they are exposed to the same risks associated with other Internet services such as email and social networks: spam , hoaxes, scams, scams, malware, etc.

- If you do not want information about you to be made public, better not spread it.
- Look for a profile photo that is not too compromising.
- Use the blocking of users with whom you do not want to have communication.
- Do not use your status to provide private information about yourself.
- Make sure that the exchange of messages is encrypted,
- Make backup copies if you don't want to lose the messages of chat.

The security of Wearables.

If you want to monitor your personal activity with a Wearable, before choosing, look for the one that offers you the best features, but without forgetting that it must also offer you the best security and privacy guarantees so that it makes correct use and treatment of your personal information.



◆ They must use some encryption mechanism that guarantees the confidentiality of your information.
◆ You must know who has access to your personal information.
◆ It is important what permissions you give the app to process your personal data.
Now you need to ask yourself these questions:
◆ What information are you sharing on social networks?
◆ Is your information stored in the cloud?
◆ Who can access it?
◆ How long do you want to keep your data?

KTSO VOCATIONAL HIGH SCHOOL TURKEY

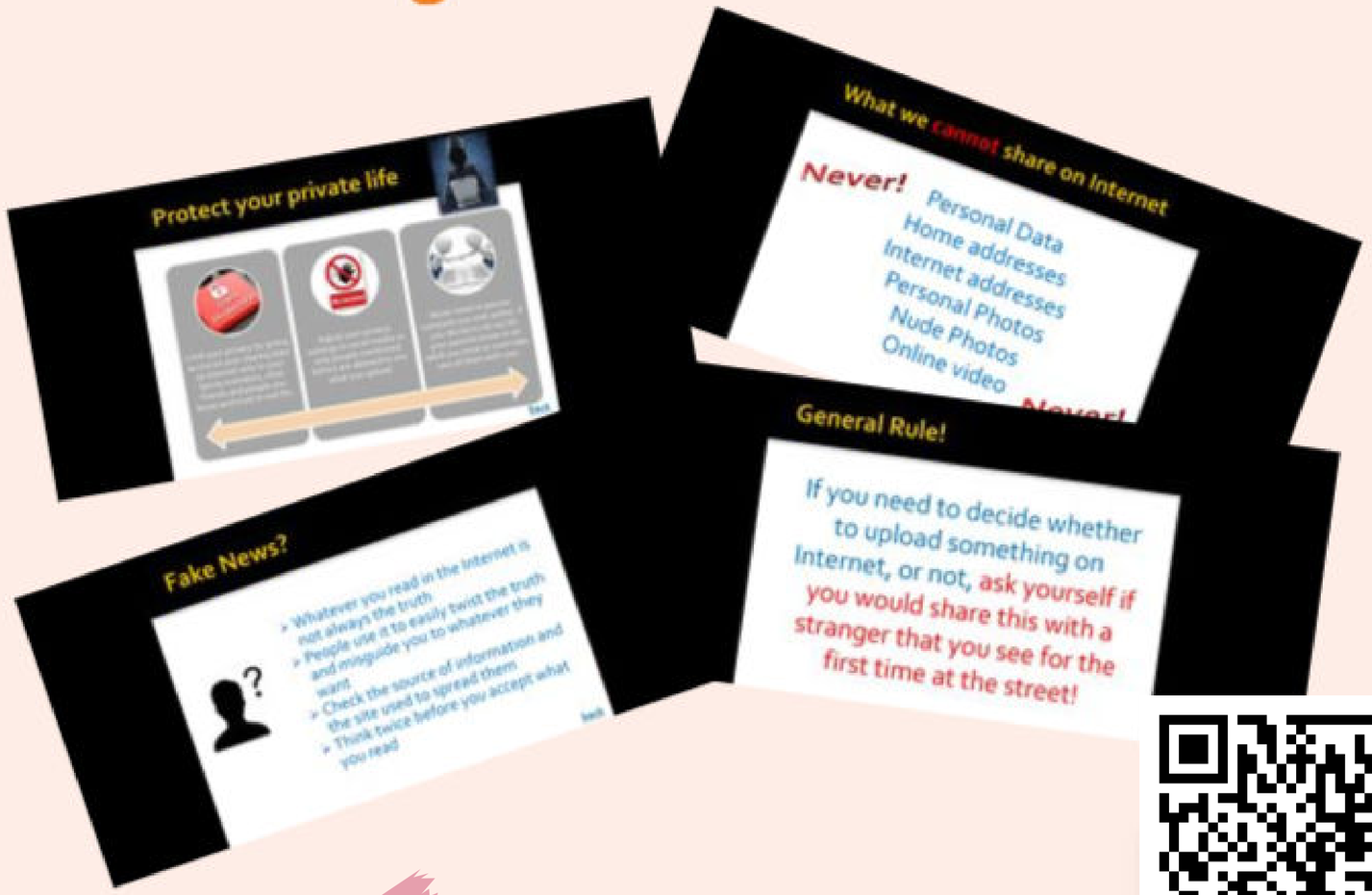
Añadir un poco de texto

Presentation

IES Antonio Menárguez Costa. Los Alcázares - Spain

Presentation

1o GEL Agiou Dimitriou Athens - Greece



Presentation

IPSCEOA "N. GALLO" di Agrigento - Italia

Presentation

Escola Secundária Campos Melo
Covilhã - Portugal

Presentation

Οδηγός ασφαλούς χρήσης του Διαδικτύου

Greek

Συνεργατικός Οδηγός

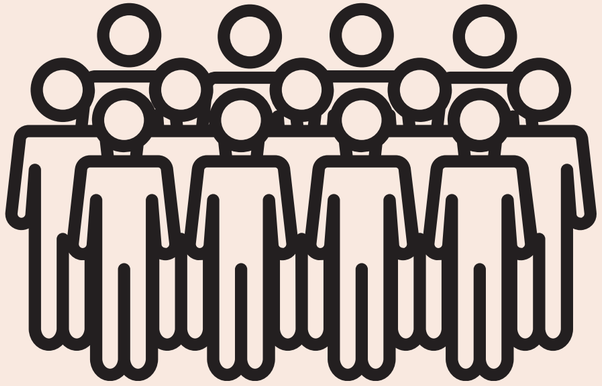
IES Antonio Menarguez Costa - Λος Αλκαζάρες - Ισπανία

KTSO Vocational High School - Κεσάν - Τουρκία

1ο ΓΕΛ Αγίου Δημητρίου - Αθήνα - Ελλάδα

Escola Secundaria Campos de Melo - Κοβίλια - Πορτογαλία

IPSCEOA "N. Gallo" - Αγριτζέντο - Ιταλία



Οι συσκευές σας αποθηκεύουν πολλές προσωπικές πληροφορίες

Ένας από τους σημαντικότερους λόγους για να προστατεύσουμε τις κινητές συσκευές μας είναι η προστασία των προσωπικών μας δεδομένων και αυτών με τους οποίους επικοινωνούμε : επαφές, φωτογραφίες, βίντεο, ηλεκτρονικό ταχυδρομείο, κλπ τα οποία δεν θα θέλαμε να τα χάσουμε ή να πέσουν σε λάθος χέρια.

Συμβουλές και Συστάσεις

Το ρίσκο ζημιάς ή κλοπής πάντα υπάρχει. Γι αυτό :

- Χρησιμοποίησε το κλείδωμα οθόνης (κωδικός ή διάγραμμα) και κρυπτογράφησε τα δεδομένα σου, έτσι ώστε αν τύχει, το κάνεις δύσκολο σε αυτόν που θα φτάσει η συσκευή σου, να έχει πρόσβαση σε αυτή.
- Κάνε χρήση προγραμμάτων ανίχνευσης συσκευής, κλειδώματος συσκευής ή ακόμα και διαγραφής δεδομένων που είναι αποθηκευμένα σε αυτή.
- Πάρε αντίγραφα ασφαλείας σε άλλα μέσα, έτσι ώστε οτιδήποτε και αν συμβεί να μην χάσεις τα δεδομένα στο τηλέφωνο ή τάμπλετ.

Μην επιτρέψετε να μαντέψουν τους κωδικούς σας

Επιλέξτε ισχυρούς κωδικούς με τουλάχιστον 8 χαρακτήρες που αποτελούνται από :

- Κεφαλαία γράμματα (Α, Β, Γ, Δ, ...).
- Πεζά γράμματα (α, β, γ, δ, ...).
- Νούμερα (1, 2, 3, ...).
- Ειδικούς χαρακτήρες (%, #, @, ...)
- Μην χρησιμοποιείς κωδικούς που είναι εύκολο να βρεθούν όπως : "123456", "σκύλος", "αααααα", ονόματα, πινακίδες αυτοκινήτων, κλπ
- Μην δίνεις τους κωδικούς σου σε άλλους. Αν το κάνεις τότε δεν είναι μυστικοί και δίνεις πρόσβαση σε άλλους στα προσωπικά σου δεδομένα.
- Μην χρησιμοποιείς τον ίδιο κωδικό σε πολλές συσκευές ή λογαριασμούς.

Μην περιμένεις να υπάρξει πρόβλημα για να πάρεις αντίγραφα ασφαλείας

Ένας από τους πιο συχνούς λόγους απώλειας δεδομένων είναι η διαγραφή κατά λάθος, όπως επίσης από κάποιον ιό που μπορεί να σβήσει ή να κρυπτογραφήσει τα δεδομένα μας. Άλλος λόγος είναι η απώλεια, η καταστροφή ή η κλοπή της συσκευής που έχει τα δεδομένα όπως το κινητό τηλέφωνο, το τάμπλετ, ο φορητός υπολογιστής, ο εξωτερικός δίσκος κλπ.

- Επέλεξε τα δεδομένα που δεν θα ήθελες να χάσεις σε καμία περίπτωση.

- Επέλεξε το μέσον στο οποίο θέλεις να αποθηκεύσεις τα δεδομένα.

- Κάνε τα αντίγραφα ασφαλείας.

- Κάνε τα αντίγραφα ασφαλείας ανά διαστήματα.

Είναι σημαντικό να μειώσεις τις σελίδες που πηγαίνεις στο ίντερνετ

Όταν περιηγήσε στο ίντερνετ ο φυλλομετρητής καταγράφει στη μνήμη όλες τις κινήσεις σου στον υπολογιστή ή στη συσκευή που χρησιμοποιείς, δεν διαγράφονται αυτές και έτσι είναι εφικτό να μάθει κάποιος ποιές σελίδες επισκεύτηκες.

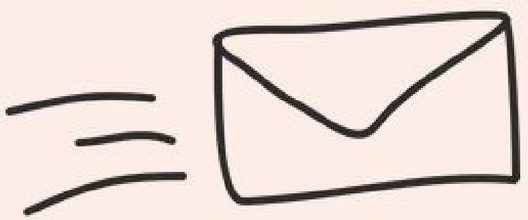
Μέτρα που πρέπει να πάρεις για να ελαττώσεις το ρίσκο στο ιντερνετ:

- Να έχετε ενημερωμένο τον φυλλομετρητή σας.
- Χρησιμοποιήστε έμπιστα πρόσθετα
- Χρησιμοποιήστε ένα ελεγκτή σελίδων που συνήθως παρέχεται με αντιικά προγράμματα.
- Ελέγξτε τις ρυθμίσεις του φυλλομετρητή και ενεργοποιήστε αυτές που θεωρείτε πιο σημαντικές για να προστατέψετε την ιδιωτικότητά και την ασφάλειά σας.
- Καθαρίστε το ιστορικό του φυλλομετρητή.
- Σβήστε τα μπισκοτάκια - ίχνη που κρατάει ο φυλλομετρητής.
- Χρησιμοποιήστε μία μηχανή διαχείρισης κωδικών.
- Κάντε πάντοτε αποσύνδεση του λογαριασμού σας όταν αποχωρείτε από μία συσκευή.

Προστατέψτε το Ηλεκτρονικό σας Ταχυδρομείο

Το ηλεκτρονικό ταχυδρομείο σου δίνει πολλές δυνατότητες στην εργασία και στην προσωπική ζωή, αλλά πρέπει να προσέχουμε όταν το χρησιμοποιούμε για αυτό ακολούθησε τις παρακάτω συμβουλές :

- Επιλέξτε ισχυρούς κωδικούς.
- Όποτε είναι εφικτό χρησιμοποίησε την επαλήθευση ταυτότητας δύο παραγόντων (2FA) για να προσθέσεις ένα επιπλέον επίπεδο ασφάλειας.
- Απέφυγε τη δημοσιοποίηση δεδομένων που θα θέσουν σε κίνδυνο την ιδιωτικότητά σου. Αν δεν υπάρχει άλλη επιλογή χρησιμοποίησε κωδικούς που μόνο εσύ και ο παραλήπτης του μηνύματος θα ξέρει.
- Μην ανοίγετε μηνύματα από άγνωστους αποστολείς. Μπορεί να περιέχουν κακόβουλο λογισμικό, υπερσυδέσμους σε κακόβουλες σελίδες ή τη δημιουργία ψεύτικου αντιγράφου του λογαριασμού σας.
- Αν το μήνυμα σας φαίνεται ύποπτο, ακόμα και αν είναι από άτομο που γνωρίζεται, μιλήστε πρώτα μαζί του, για να επιβεβαιώσετε ότι δεν έχετε παραλάβει μήμυμα από ψεύτικο λογαριασμό.
- Κάνετε αντίγραφα ασφαλείας έτσι ώστε να μη χάσετε τα δεδομένα σας σε περίπτωση βλάβης του εξυπηρετητή του ταχυδρομείου σας.



Κίνδυνοι στα άμεσα μηνύματα

Τα προγράμματα άμεσων μηνυμάτων παρέχουν πολλές δυνατότητες : ανταλλαγή μηνυμάτων, βίντεο, φωτογραφιών κλπ και έτσι εκτίθενται στους ίδιους κινδύνους που βρίσκονται στις εφαρμογές του διαδικτύου όπως τα μέσα κοινωνικής δικτύωσης και ηλεκτρονικά ταχυδρομεία.

- Αν δεν θέλεις τα προσωπικά σου δεδομένα να βρεθούν στο διαδίκτυο τότε να μην τα διανέμεις.
- Βρες μία φωτογραφία για το προφίλ σου η οποία δεν θα δίνει πολλά στοιχεία για εσένα.
- Απέκλεισε χρήστες που δεν θέλεις να έχεις επαφές μαζί τους.
- Μην αναφέρετε στην κατάσταση του προφίλ σας πληροφορίες που αποκαλύπτουν πράγματα για εσάς.
- Επιβεβαιώστε ότι η ανταλλαγή των μηνυμάτων γίνεται με κρυπτογράφηση.
- Κάνετε αντίγραφα ασφαλείας έτσι ώστε να μη χάσετε τα μηνύματά σας σε περίπτωση βλάβης του εξυπηρετητή.

Η ασφάλεια των συσκευών που "φοράμε"

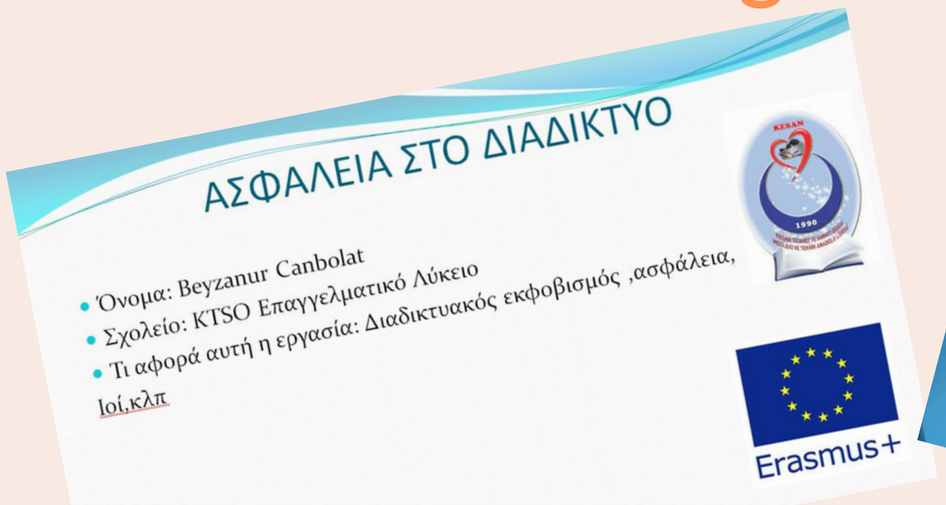
Αν θέλετε να καταγράφετε την δραστηριότητά σας με μία συσκευή παρακολούθησης που φοριέται, επιλέξτε μία που είναι κατάλληλη για εσάς, αλλά παράλληλα προσφέρει την απαραίτητη ασφάλεια και εγγύηση για την ιδιωτικότητά σας, ώστε να γίνεται ορθή χρήση των προσωπικών σας δεδομένων.

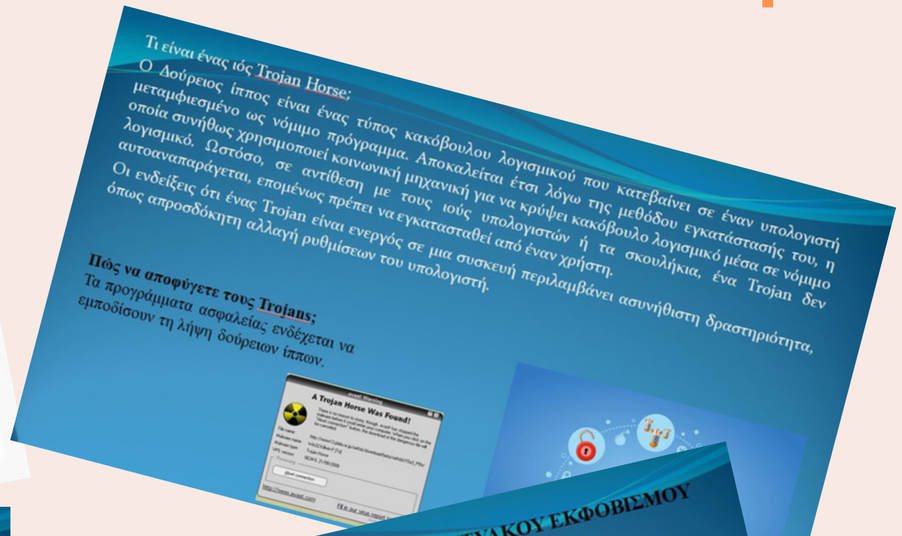
- Πρέπει να έχουν κάποιο μηχανισμό κρυπτογράφησης των δεδομένων που εγγυάται την εμπιστευτικότητα τους.
- Πρέπει να γνωρίζετε ποιός έχει πρόσβαση στα προσωπικά σας δεδομένα.
- Είναι σημαντικό να γνωρίζεται τί δικαιώματα δίνεται στη συσκευή για την επεξεργασία των δεδομένων σας.

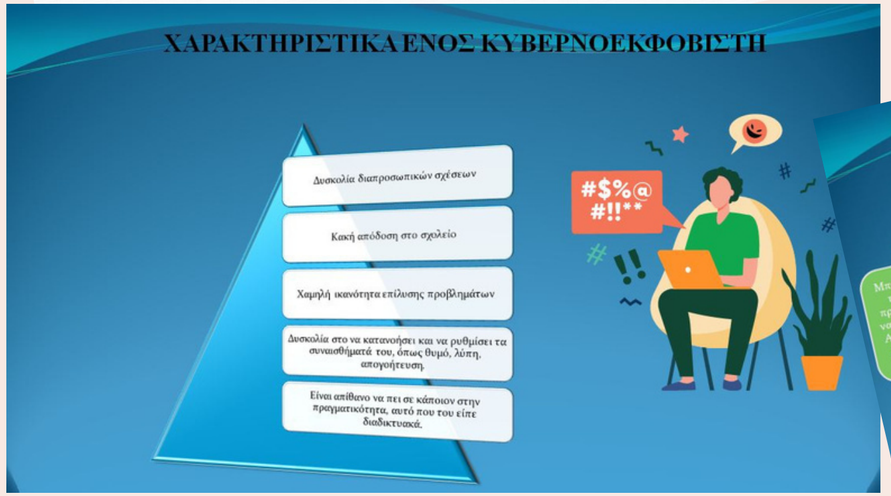
Πρέπει να αναλογιστείτε τα εξής :

- Τί δεδομένα διαμοιράζω στα κοινωνικά μέσα δικτύωσης;
- Είναι τα δεδομένα αποθηκευμένα σε έναν εξυπηρετητή;
- Ποιός έχει πρόσβαση στα δεδομένα;
- Πόσο καιρό θέλετε να είναι τα δεδομένα σας αποθηκευμένα στον εξυπηρετητή;

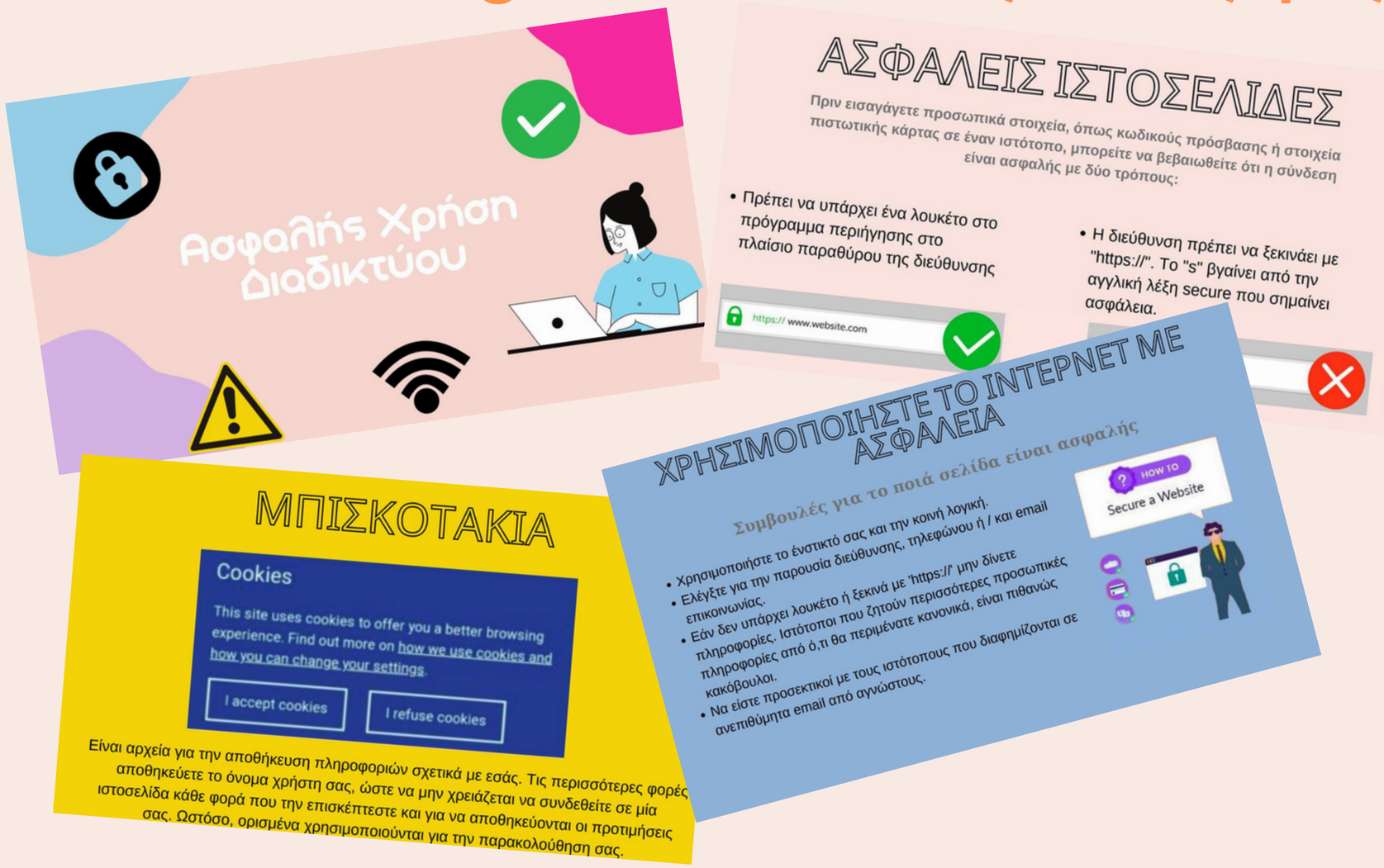
KTSO Vocational High School - Κεσάν - Τουρκία



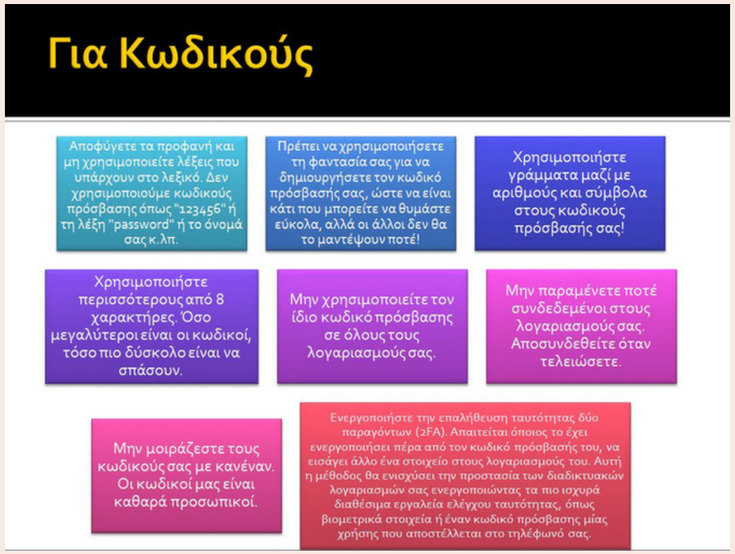




IES Antonio Menarguez Costa - Λος Αλκαζάρες - Ισπανία



1ο ΓΕΛ Αγίου Δημητρίου - Αθήνα - Ελλάδα



IPSCEOA "N. Gallo" - Αγριτζέντο - Ιταλία

Escola Secundaria Campos de Melo - Κοβίλια - Πορτογαλία

Libro-guida per utilizzare internet in modo sicuro

Italian

LIBRO-GUIDA COLLABORATIVO

IES Antonio Menàrguez. Los Alcàzares - Spagna

KTSO VOCATIONAL HIGH SCHOOL - Turchia

1o GEL Agiou Dimitriou Athens - Grecia

Escola Secundària Campos de Melo, Covilha - Portogallo IPSCEOA "N. Gallo" di Agrigento - Italia

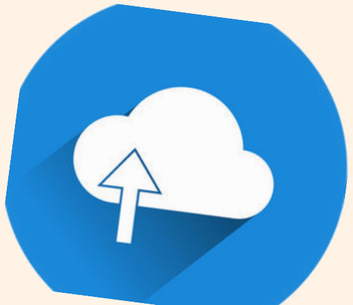
I tuoi dispositivi memorizzano molte informazioni private

Uno dei motivi principali per proteggere i nostri dispositivi é salvaguardare le nostre informazioni personali e quelle di coloro con cui comunichiamo: contatti, fotografie, video, e-mail, ecc... e in cui non vorremmo perdere o cadere in mani di terzi

Suggerimenti e raccomandazioni

Il rischio di smarrimento o furto esisterà sempre. Pertanto:

- Utilizza un metodo di blocco dello schermo (codice numerico o sequenza) e crittografare le informazioni in modo che se si verifica questa situazione, si rende difficile l'accesso alla persona che finisce con il dispositivo in mano.
- Utilizza gli strumenti di sicurezza che ti aiuteranno a localizzare il dispositivo , bloccalo ed elimina sempre le informazioni memorizzate su di esso.
- Esegui dei backup su altri dispositivi in modo da non perdere le informazioni memorizzate sul cellulare o sul tablet, qualunque cosa accada.



NON PERMETTERE A NESSUNO DI INDOVINARE LE TUE PASSWORD

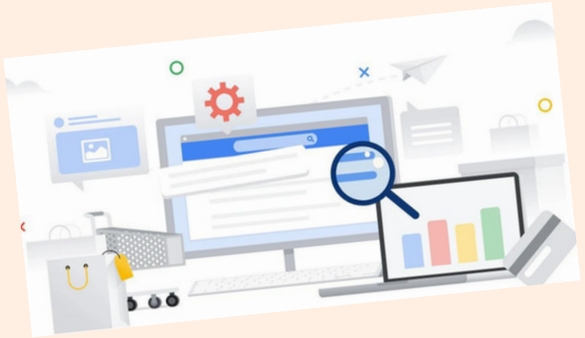
SCEGLI PASSWORD COMPLESSE O ROBUSTE
ALMENO 8 CARATTERI E COMPOSTO DA:
- maiuscolo (A, B, C...);
- minuscolo (a, b, c...);
- numeri (1, 2, 3...);
-e caratteri speciali ($, &, #...);

- NON utilizzare password facili da indovinare
come "12345678", "qwerty", "aaaa", nomi della famiglia, targhe dei veicoli, ecc.
- NON condividere le tue password.
Se lo fai, non sará piú segreto e darai accesso ad altre persone alla tua privacy.
- NON utilizzare la stessa password su piú servizi.

Non aspettare un problema, fai delle copie di backup

La cancellazione accidentale é una delle cause piú comuni di perdita di informazioni, sebbene non sia l'unico, puó anche essere dovuto all'azione di un virus in grado di cittografare o eliminare le informazioni, a causa della perdita, incidente o furto del dispositivo che contiene l'informazione: smartphone, tablet, laptop, disco rigido esterno, unità flash o perché il dispositivo smette di funzionare correttamente.

1. *Seleziona le informazioni che in nessun caso vorresti perdere.*



2. Scegli il sito dove memorizzare le tue informazioni

3. Eseguire il backup

4. Ripeti la copia periodicamente

E' IMPORTANTE ELIMINARE I PASSAGGI CHE SI ESEGUONO DURANTE LA NAVIGAZIONE IN INTERNET

Quando navighi in internet, per impostazione predefinita tutta l'attivita' che hai svolto con il browser viene archiviata direttamente nella memoria del tuo computer o dispositivo, non scompare,in modo tale che sia possibile conoscere tutt i i passaggi fatti in un momento su internet

Misure per ridurre al minimo i rischi durante la navigazione

DEVI PROTEGGERE LA TUA EMAIL

La posta elettronica é uno strumento che ti offre molte possibilitá, sia a lavoro che nella sfera privata, ma devi stare attento quando la usi, quindi applica i seguenti

- consigli:
- assicurati di utilizzare una password complessa.
  ogni volta che un servizio lo fornisce, attiva la verifica in due passaggi
  per aggiungere un ulteriore livello di sicurezza all-autenticazione del processo di
- pagamento.
  evita di fornire informazioni che potrebbero compromettere la tua privacy, se
  non hai altra scelta, bisogna crittografare o comprimere i file con una password che
- solo il destinatario dell'email e tu conosci.
  non aprire email di utenti sconosciuti ed eliminarle: potrebbero contenere file con malware,
- collegamenti a pagine dannose o che impersonano l'identità di qualche entità
  anche se il mittente dell'email è noto, se il messaggio ti sembra sospetto, consulta direttamente
- quella persona per confermare che che non ha falsificato il suo indirizzo email.
  non dimenticare di fare copie di backup in modo da non perdere informazioni preziose in caso
  di problemi con il server di posta.

Rischi nei servizi di messagistica istantanea

WhatsApp e il resto delle applicazioni di messagistica istantanea incorporano molte funzionalitá: inviare/ricevere messaggi di testo,video, foto.. e come tali, sono esposti agli stessi rischi associati ad altri internet servizi come email e reti social: spam, bufale, truffe, malware ecc.

*Se non si desidera che vengano fornite informazioni su di te pubblico, meglio non diffonderle.
*Cerca una foto del profilo che non sia troppo compromettente.
*Utilizzare il blocco degli utenti con cui non si desidera avere comunicazione.
*Non utilizzare il tuo stato per fornire informazioni private su di te.
*Assicurarsi che lo scambio di messaggi sia cittografato.
*Crea copie di backup se non vuoi perdere il file messaggi di chat.

La sicurezza dei dispositivi indossabili.

Se vuoi monitorare la tua attività personale con un wearable, prima di scegliere cercane uno che ti offre le migliori caratteristiche , ma senza dimenticare che deve offrirti anche le migliori garanzie di sicurezza e privacy affinché faccia uso e trattamentodelle tue informazioni personali.

Devono utilizzare un meccanismo di cittografia che garantisca la riservatezza delle tue informazioni.
Devi sapere chi ha accesso alle tue informazioni personali.
É importante quali autorizzazioni congedi all'app per elaborare i tuoi dati personali.
Ora devi farti queste domande
Quali informazioni condividi sui social media?
Le tue informazioni sono archiviate nei cloud?
Chi puó accedervi?
Per quanto tempo vuoi conservare i tuoi dati?

KTSO VOCATIONAL HIGH SCHOOL TURKEY

IES Antonio Mènarguez Costa. Los Alcàzares SPAIN

1o GEL Agiou Dimitriou Athens GREECE

IPSCEOA Nicolò Gallo di Agrigento ITALY

Escola Secundária Campos Melo
Covilhã - Portugal

Ebook sobre utilização de Internet Segura

Portuguese

Ebook produzido em colaboração por:

IES Antonio Menárguez Costa. Los Alcázares - Espanha

KTSO VOCATIONAL HIGH SCHOOL -

GEL Agiou Dimitriou Athens - Grécia

Escola Secundária Campos de Melo, Covilhã - Portugal

IPSCEOA "N. Gallo" di Agrigento - Itália

Os seus dispositivos armazenam muitas informações privadas.

Uma das principais razões para proteger os nossos dispositivos móveis é salvaguardar a nossa informação pessoal e daqueles com quem nos comunicamos: contactos, fotografias, vídeos, emails, etc., e que não gostaríamos de perder ou cair, nas mãos de terceiros.

Dicas e recomendações

O risco de perda ou roubo sempre existirá. Portanto: Use um método de bloqueio de ecrã (código numérico ou padrão) e criptografe as informações para que caso ocorra essa situação, você dificulta o acesso de quem acaba com o aparelho nas mãos, Faça uso de ferramentas de segurança que vão te ajudar a localizar o aparelho,
bloqueá-lo e até deletar o informações armazenadas nele. Faça backups em outras mídias para que, aconteça o que acontecer, você não perca as informações armazenadas no celular ou tablet.

Não deixe ninguém adivinhar suas senhas

Escolha senhas fortes ou robustas com no mínimo 8 caracteres e compostas por:

maiúsculas (A, B, C...)
minúsculas (a, b, c...)
números (1, 2, 3...)
e caracteres especiais ($, &,#...)

NÃO use senhas fáceis de adivinhar tais como:

"12345678",
"qwerty",
nomes de família "aaaaaa", placas de veículos, etc.
NÃO compartilhe suas senhas.

Se o fizer, deixará de ser secreto e estará a dar acesso à sua privacidade a outras pessoas. NÃO use a mesma senha em vários serviços.

Não espere por um problema, faça cópias de segurança.

A exclusão acidental é uma das causas mais comuns de perda de informações, embora não seja a única, também pode ser devido à ação de um vírus capaz de criptografar ou excluir as informações, devido à perda, acidente ou roubo do dispositivo que contém as informações: smartphone, tablet, laptop, disco rígido externo, pen drive ou porque o dispositivo parou de funcionar corretamente.

1. Selecione as informações que em hipótese alguma você gostaria de perder.

2. Escolha a mídia onde irá armazenar as informações.

3.Faça o backup.

4.Repita suas cópias periodicamente.

É importante eliminar as etapas que você executa ao navegar na Internet.

Quando você navega na Internet, por padrão, todas as atividades que você realizou com o navegador são armazenadas diretamente na memória do seu computador ou dispositivo, não desaparecem, de forma que é possível conhecer todas as etapas que você levou em um determinado momento na Internet.

Medidas para minimizar os riscos ao navegar na Internet: Mantenha seu navegador atualizado.

Escolha complementos e plug-ins confiáveis.
Instale um verificador de páginas da web, geralmente fornecido pelos principais antivírus.
Verifique as opções de configuração do navegador e habilite aquelas que você considera mais interessantes para proteger sua privacidade e mantê-lo mais seguro.
Limpar histórico de navegação.
Apagar cookies.
Use um gestor de senhas para armazenar e proteger seus códigos de acesso.
Feche sempre a sessão ao sair de uma página onde você se autenticou com um nome de usuário e senha.

Você deve proteger o seu e-mail.

O e-mail é uma ferramenta que oferece muitas possibilidades, tanto no trabalho quanto na esfera privada, mas você deve ter cuidado ao usá-lo, portanto, aplique as seguintes recomendações:

Certifique-se de usar uma senha forte. Sempre que um serviço fornecer, ative a verificação em duas etapas para adicionar uma camada extra de segurança à autenticação do processo de checkout.

Evite fornecer informações que possam comprometer sua privacidade, caso não tenha outra opção, criptografe ou compacte os arquivos com uma senha que somente o destinatário do e-mail e você sabe.

Não abra e-mails de utilizadores desconhecidos e exclua-os: eles podem conter ficheiros com malware, links para páginas maliciosas ou que representam a identidade de alguma entidade.

Mesmo que o remetente do e-mail seja conhecido, se a mensagem parecer suspeita para você, consulte essa pessoa diretamente para confirmar que ela não falsificou seu endereço de e-mail.

Não se esqueça de fazer cópias de segurança para não perder informações valiosas no caso de um problema com o servidor
de correio.

Riscos em serviços de mensagens instantâneas

O WhatsApp e o resto dos aplicativos de mensagens instantâneas incorporam muitas funcionalidades: enviar/receber mensagens de texto, vídeos, fotos... hoaxes, scams, scams, malware, etc.

Se você não quer que informações sobre você se tornem públicas, melhor não divulgá-las.

Procure uma foto de perfil que não seja muito comprometedora Use o bloqueio de usuários com os quais você não deseja ter comunicação.

Não use seu status para fornecer informações privadas sobre si mesmo.

Certifique-se de que a troca de mensagens seja criptografada.

Faça cópias de backup se não quiser perder o mensagens de chat

A segurança dos wearables

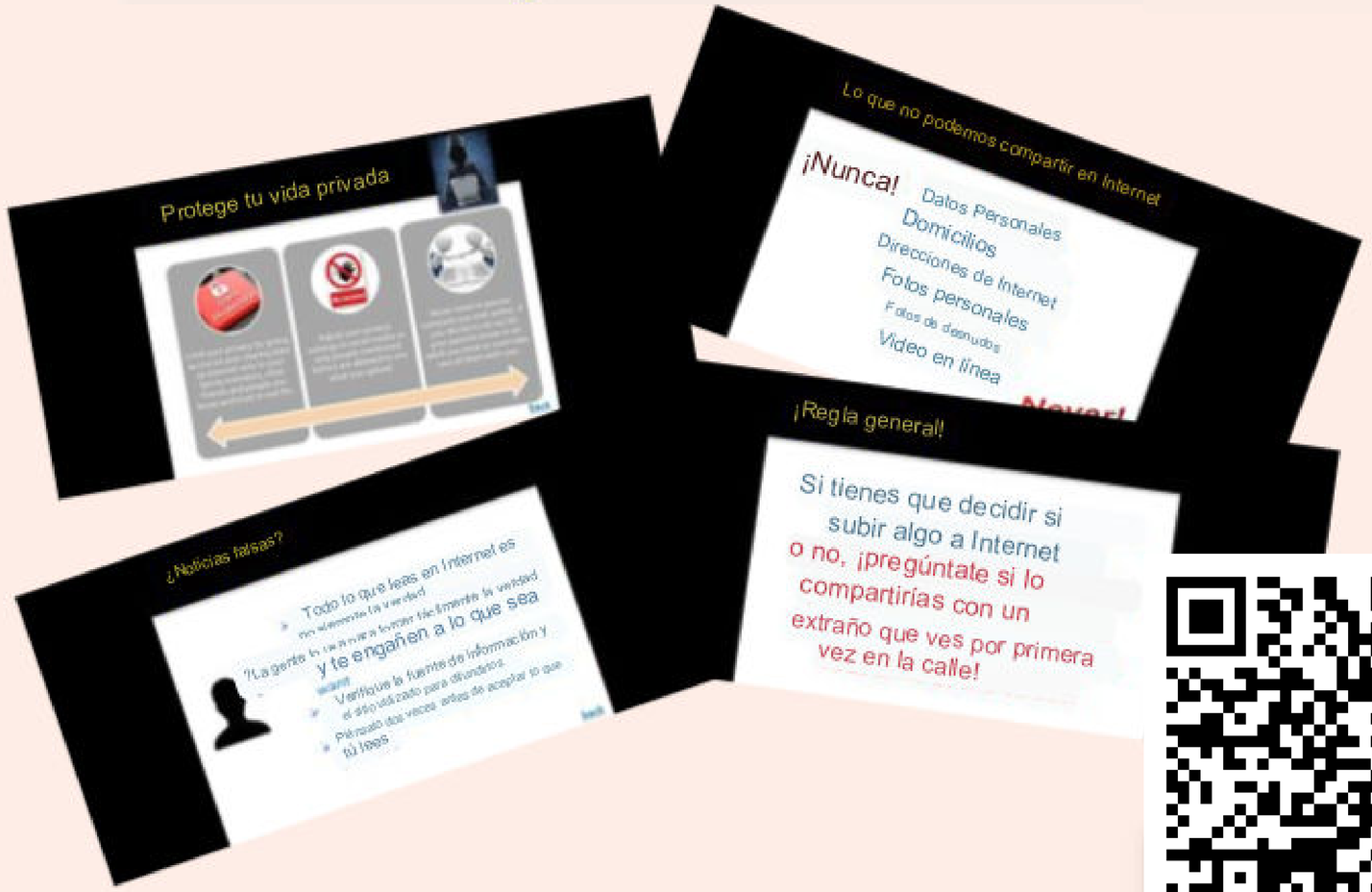
Se você deseja monitorizar a sua atividade pessoal com um Wearable, antes de escolher, procure aquele que oferece as melhores características, mas sem esquecer que ele também deve oferecer as melhores garantias de segurança e privacidade para que faça uso e tratamento corretos suas informações pessoais.

Eles devem usar algum mecanismo de criptografia que garanta a confidencialidade de seu Informação.
Você deve saber quem tem acesso à sua informação pessoal.
É importante quais permissões você dá ao aplicativo para processar seus dados pessoais.
Agora você precisa perguntar o seguinte: Quais informações você compartilha nas redes sociais?
Suas informações estão armazenadas na nuvem? Quem pode acessá-lo?
Por quanto tempo você deseja manter seus dados?

KTSO VOCATIONAL HIGH SCHOOL - TURQUIA

IES Antonio Menárguez Costa. Los Alcázares - Spanha

10 GEL Agiou Dimitriou Athens Grécia



IPSCEOA "N. GALLO" Di Agrigento Itália

Escola Secundária Campos Melo
Covilhã - Portugal

GUÍA DE USO SEGURO DE INTERNET

Spanish

GUÍA COLABORATIVA

IES ANTONIO MENARGUEZ COSTA LOS ALCAZARES ESPAÑA

KTSO VOCATIONAL HIGH SCHOOL TURKEY

IO GEL AGUIOU DIMITRIOU ATHENS GREEC

ESCXOLA SECUNDARIA CAMPOS DE MELO, COVILHA PORTUGAL

IPSCEO A N.GALLO DI AGRIGENTO - ITALIA

Tus dispositivos almacenan mucha información privada.

Una de las principales razones para proteger nuestros dispositivos móviles es salvaguardar nuestra información personal y la de aquellos con quienes nos comunicamos: contactos, fotografías, videos, correos
electrónicos, etc., y que no nos gustaría perder o caer en manos de terceros.

Consejos y recomendaciones

El riesgo de pérdida o robo siempre existirá. Por lo tanto: Utilice un método de bloqueo de pantalla (código
numérico o patrón) y cifre la información para que
si se da esta situación dificulta el acceso de la persona que acaba con el dispositivo en sus manos, haz uso de herramientas de seguridad que te ayudarán a localizar el dispositivo, bloquearlo e incluso borrar la información almacenada en él. Realiza copias de seguridad en otros soportes para que, pase lo que pase, no pierdas la información almacenada en el móvil o tablet.

INFORMACION PRIVADA

QUE NADIE ADIVINE TUS CONTRASEÑAS
ELIJE CONTRASEÑAS SEGURAS O ROBUSTAS DE AL MENOS 8

NÚMEROS (1, 2, 3...)
Y CARACTERES ESPECIALES ($, &, #...)

"12345678", "QWERTY", APELLIDOS "AAAA", PLACAS DE VEHÍCULOS, ETC. NO COMPARTAS TUS CONTRASEÑAS.

MAYÚSCULAS (A, B, C...) MINÚSCULAS (A, B, C...)

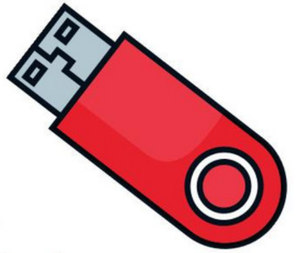
NÚMEROS (1, 2, 3...)

1. SELECCIONA LA INFORMACIÓN QUE BAJO NINGÚN CONCEPTO TE GUSTARÍA PERDER.

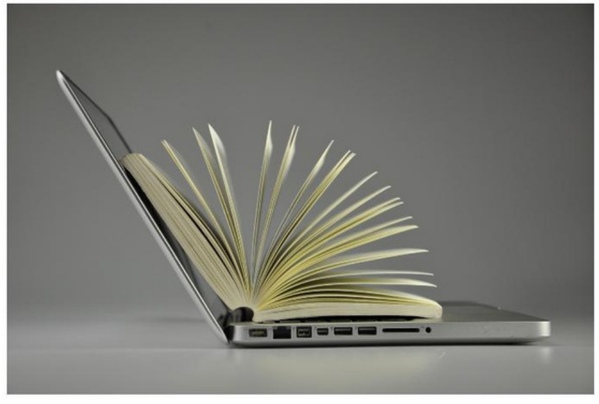
2. ELIGE EL MEDIO DONDE SE ALMACENARÁ LA INFORMACIÓN.

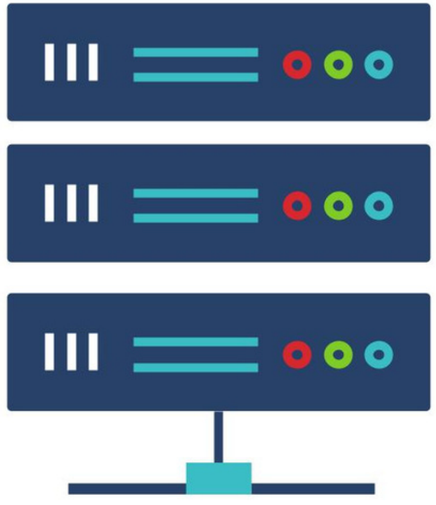
3. REALIZA LA COPIA DE SEGURIDAD.

4. REPITE TUS COPIAS PERIÓDICAMENTE.



No espere a que surja un problema, haz copias de seguridad.
El borrado accidental es una de las causas más comunes de pérdida de información, aunque no es la única,
también puede deberse a la acción de un virus capaz de encriptar o borrar la información, por la pérdida,
accidente o robo del mismo dispositivo que contiene la información: smartphone, tablet, laptop, disco duro
externo, pendrive o porque el dispositivo deja de funcionar correctamente.





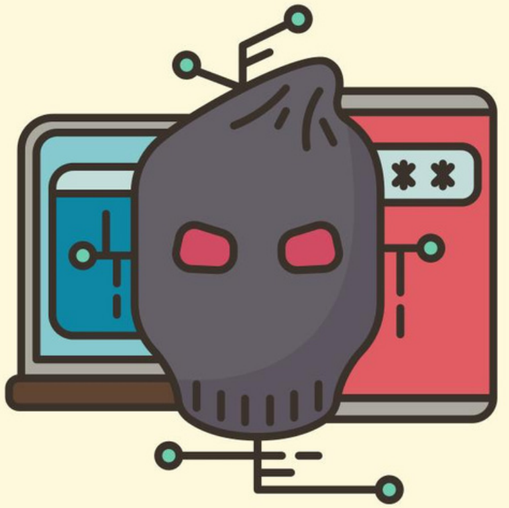
Es importante eliminar los pasos que realizas cuando navegas por Internet.
Cuando navegas por Internet, por defecto toda la actividad que has realizado con el navegador se almacena directamente en la memoria de tu ordenador o dispositivo, no desaparece, de tal forma que es posible conocer todos los pasos que has seguido en un momento dado en Internet.
Medidas para minimizar los riesgos cuando navega por Internet: Manten tu navegador actualizado.
Elije complementos de confianza. Instala un verificador de páginas web, generalmente proporcionado por los principales antivirus.
Revisa las opciones de configuración del navegador y activa aquellas que consideres más interesantes para proteger tu privacidad y mantenerte más seguro.
Borrar historial de navegación. Eliminar las cookies.
Utiliza un administrador de contraseñas para almacenar y proteger tus códigos de acceso. Cierra siempre la sesión cuando salgas de una página donde te hayas autenticado con usuario y contraseña.

CORREO ELECTRONICO

CORREO ELECTRÓNICO!
DEBES PROTEGER TU CORREO ELECTRÓNICO.
EL CORREO ELECTRÓNICO ES UNA HERRAMIENTA QUE TE OFRECE MUCHAS POSIBILIDADES, TANTO EN EL TRABAJO COMO EN EL
ÁMBITO PRIVADO, PERO HAY QUE TENER CUIDADO A LA HORA DE UTILIZARLO, POR ELLO, APLICA LAS SIGUIENTES RECOMENDACIONES:
ASEGÚRATE DE USAR UNA CONTRASEÑA SEGURA. SIEMPRE QUE UN SERVICIO LO PROPORCIONE, ACTIVA LA VERIFICACIÓN EN
DOS PASOS PARA AGREGAR UNA CAPA ADICIONAL DE SEGURIDAD A LA AUTENTICACIÓN DEL PROCESO DE PAGO.
EVITA PROPORCIONAR INFORMACIÓN QUE PUEDA COMPROMETER TU PRIVACIDAD, SI NO TIENES OTRA OPCIÓN, CIFRA O
COMPRIME LOS ARCHIVOS CON UNA CONTRASEÑA QUE SOLO EL DESTINATARIO DEL CORREO ELECTRÓNICO SEPA.
NO ABRA CORREOS ELECTRÓNICOS DE USUARIOS DESCONOCIDOS Y ELIMÍNALOS: PODRÍAN CONTENER ARCHIVOS CON MALWARE,
ENLACES A PÁGINAS MALICIOSAS O QUE SUPLANTAN LA IDENTIDAD DE ALGUNA ENTIDAD.
AUNQUE SE CONOZCA EL REMITENTE DEL CORREO ELECTRÓNICO, SI EL MENSAJE TE PARECE SOSPECHOSO, CONSULTA
DIRECTAMENTE A ESA PERSONA PARA CONFIRMAR QUE NO HA FALSIFICADO SU DIRECCIÓN DE CORREO ELECTRÓNICO.
NO OLVIDES REALIZAR COPIAS DE SEGURIDAD PARA NO PERDER INFORMACIÓN VALIOSA EN EL CASO DE UN PROBLEMA CON EL
SERVIDOR DE CORREO.

RIESGOS EN LOS SERVICIOS DE MENSAJERÍA INSTANTÁNEA.

- RIESGOS EN LOS SERVICIOS DE MENSAJERÍA INSTANTÁNEA.
- WHATSAPP Y EL RESTO DE APLICACIONES DE MENSAJERÍA INSTANTÁNEA INCORPORAN MUCHAS FUNCIONALIDADES:
- ENVIAR/RECIBIR MENSAJES DE TEXTO, VÍDEOS, FOTOS... Y COMO TAL, ESTÁN EXPUESTAS A LOS MISMOS RIESGOS ASOCIADOS
- A OTROS SERVICIOS DE INTERNET COMO EL CORREO ELECTRÓNICO Y LAS REDES SOCIALES: SPAM, BULOS, ESTAFAS, ESTAFAS,
- MALWARE, ETC.
- SI NO QUIERES QUE SE HAGA PÚBLICA INFORMACIÓN TUYA, MEJOR NO LA DIFUNDAS.
- BUSCA UNA FOTO DE PERFIL QUE NO SEA DEMASIADO COMPROMETEDORA USA EL BLOQUEO DE USUARIOS CON LOS QUE NO
- QUIERES TENER COMUNICACIÓN. NO UTILICE SU ESTADO PARA PROPORCIONAR INFORMACIÓN PRIVADA ACERCA DE TI MISMO.
- ASEGÚRATE DE QUE EL INTERCAMBIO DE MENSAJES ESTÉ ENCRIPTADO.
- HAZ COPIAS DE SEGURIDAD SI NO QUIERES PERDER LOS MENSAJES DE CHAT.



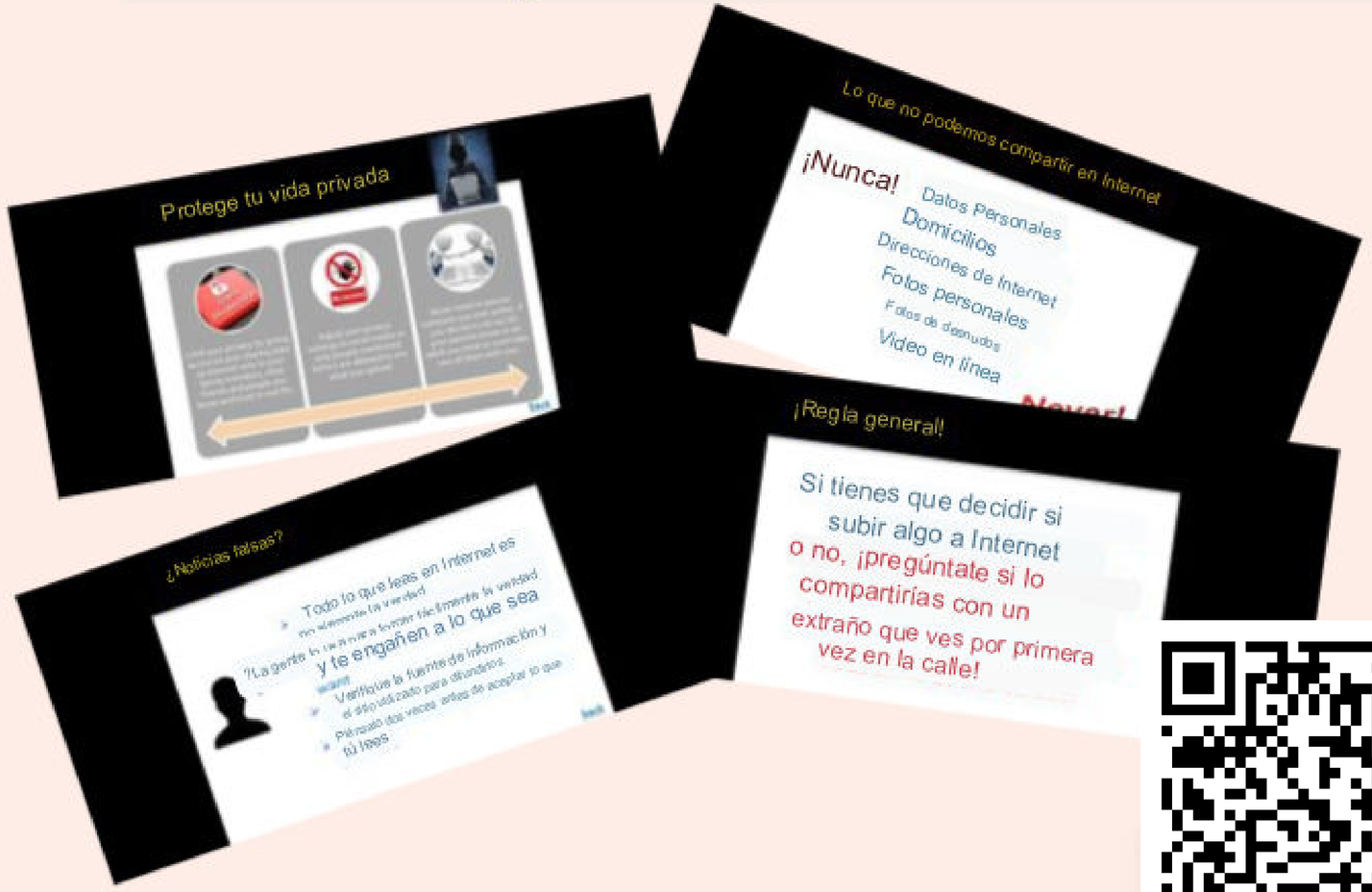
LA SEGURIDAD DE LOS WEARABLES.

- LA SEGURIDAD DE LOS WEARABLES.
- SI QUIERES MONITORIZAR TU ACTIVIDAD PERSONAL CON UN WEARABLE, ANTES DE ELEGIR BUSCA EL QUE MEJORES
- PRESTACIONES TE OFREZCA, PERO SIN OLVIDAR QUE TAMBIÉN DEBE OFRECERTE LAS MEJORES GARANTÍAS DE SEGURIDAD Y
- PRIVACIDAD PARA QUE HAGA UN CORRECTO USO Y TRATAMIENTO DE LOS MISMOS. TU INFORMACIÓN PERSONAL.
- DEBEN UTILIZAR ALGÚN MECANISMO DE ENCRIPTACIÓN QUE GARANTICE LA CONFIDENCIALIDAD DE TU INFORMACIÓN.
- DEBES SABER QUIÉN TIENE ACCESO A TU INFORMACIÓN PERSONAL.
- ES IMPORTANTE QUÉ PERMISOS LE OTORGAS A LA APLICACIÓN PARA PROCESAR TUS DATOS PERSONALES. AHORA DEBES
- HACERTE ESTAS PREGUNTAS: ¿QUÉ INFORMACIÓN ESTÁS COMPARTIENDO EN LAS REDES SOCIALES?
- ¿TU INFORMACIÓN ESTÁ ALMACENADA EN LA NUBE? ¿QUIÉN PUEDE ACCEDER A ÉL?
- ¿CUÁNTO TIEMPO QUIERES CONSERVAR TUS DATOS?

ESCUELA SECUNDARIA PROFESIONAL KTSO TURQUÍA

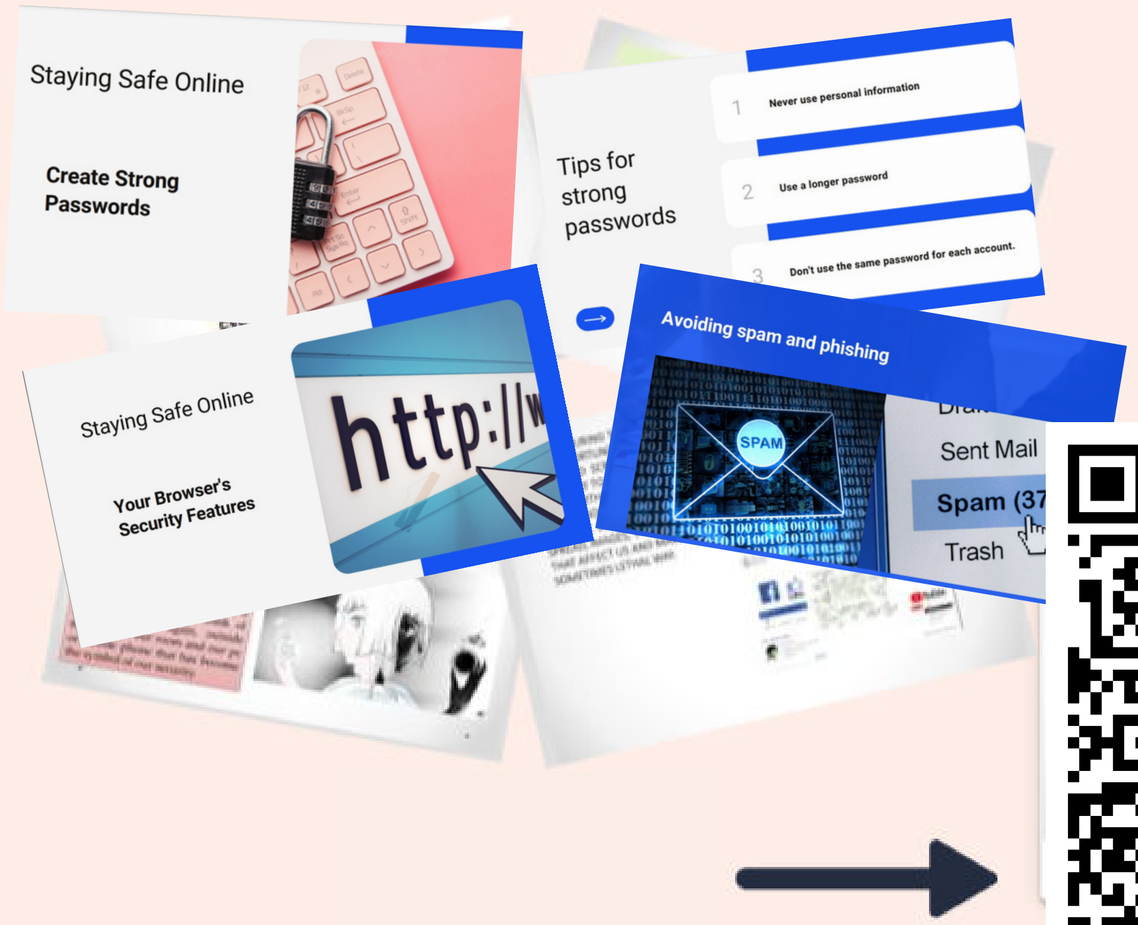
IES Antonio Menárguez Costa. Los Alcázares - Spain

10 GEL Agiou Dimitriou Atenas - Grecia



IPSCEOA "N. GALLO" de Agrigento - Italia

Escuela Secundaria Campos Melo
Covilhã - Portugal



THE END