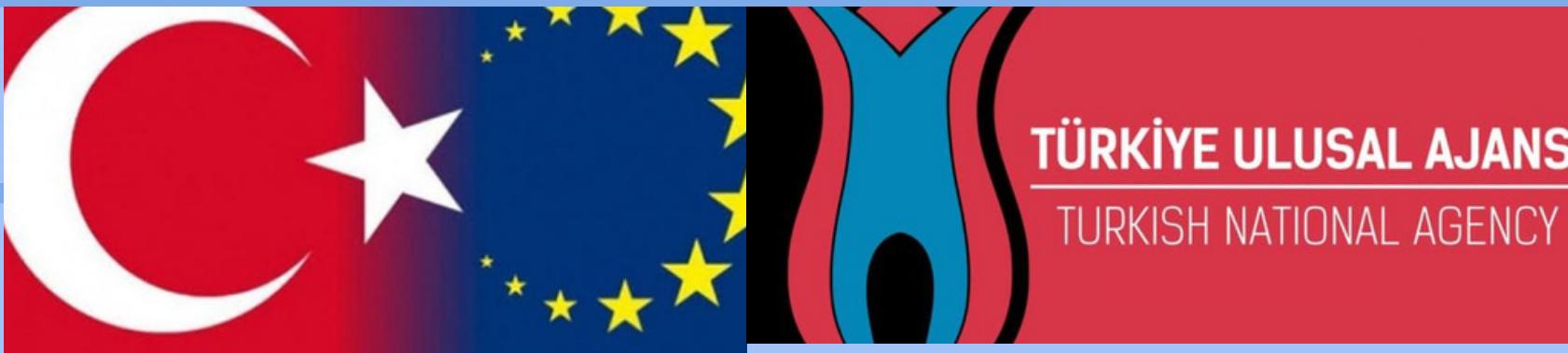


# İNTERNETİN GÜVENLİ KULLANIMI REHBERİ



**SİBER GÜVENLİK OKULLARDADA  
ERASMUS PROJESİ**  
**2020-1-TR01-KA229-094378\_1**

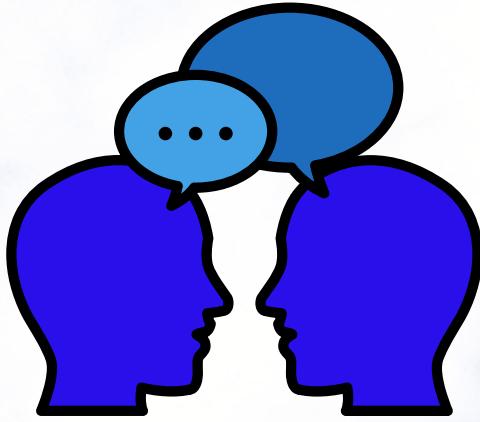
Turkish



**Erasmus+**

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





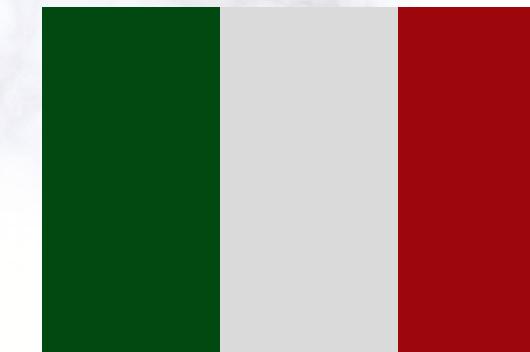
# GÜVENLİ İNTERNET KULLANIM REHBERİ

**IES Antonio Menarguez costa.Los Alcazares-İSPANYA**

**KTSO VOCATIONNAL HIGH SCHOOL TÜRKİYE**

**1ο GEL Agiou Dimitriou Athēns YUNANİSTAN-  
Escola Secundaria Campos de Melo,Covilha-PORTEKİZ**

**IPSCEOA "N.Gallo" di Agrigento-İTALYA**



- Cihazlarınız çok sayıda özel Bilgi depolar



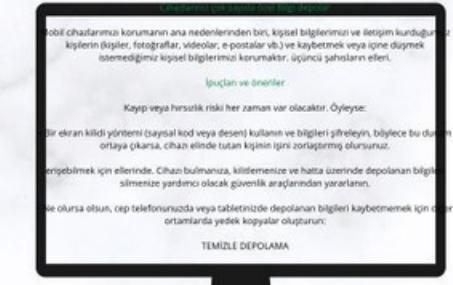
Mobil cihazlarımızı korumanın ana nedenlerinden biri, kişisel bilgilerimizi ve iletişim kurduğumuz kişilerin (kişiler, fotoğraflar, videolar, e-postalar vb.) ve kaybetmek veya üçüncü kişilerin eline geçmesini istemediğimiz kişisel bilgilerimizi korumaktır.



### 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 bulmanızı, 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:



# INTERNETİN KULLANIMI GÜVENLİ

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 aygit düzgün çalışmayı durdurması nedeniyle de kaynaklanabilir.



**Hiçbir koşulda kaybetmek istemeyeceğiniz bilgileri seçin.**



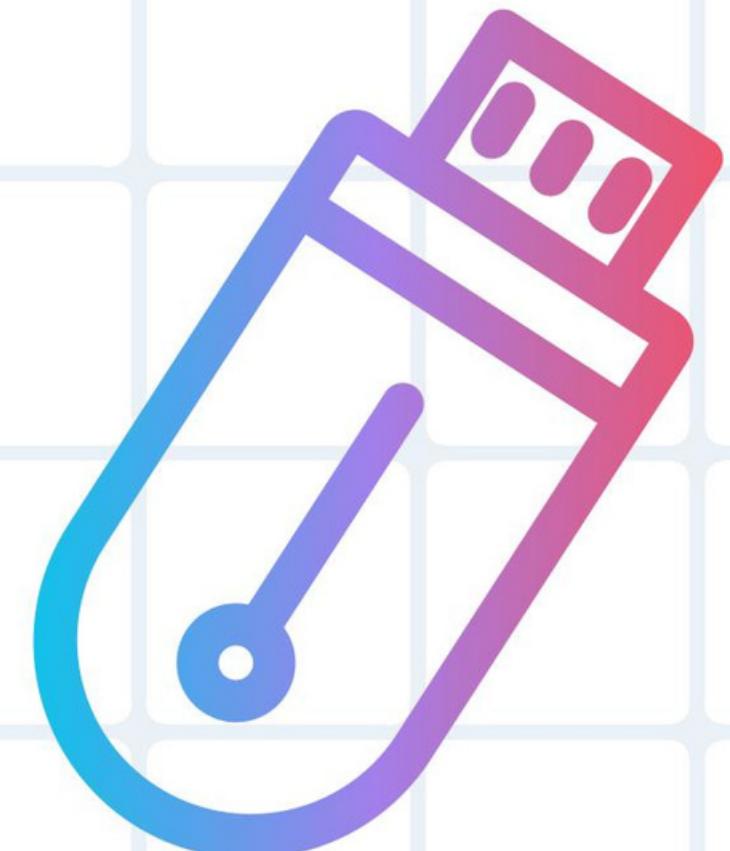
**Bilgileri depolayacağınız ortamı seçin.**



**Yedeklemeyi yapın.**



**Kopyalarınızı periyodik olarak tekrarlayın.**





# İNTERNETTE GEZİNİRKEN ATTığINIZ ADIMLARI ORTADAN KALDIRMAK ÖNEMLİDİR.

İnternette gez n rken,  
varsayılan olarak tarayıcı le  
gerçekleş rd ğn z tüm  
şlemler, doğrudan  
b lg sayarınızın veya  
e hazzınızın 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 gerekiyor.

E-posta, hem işte hem de özel alanınızda size birçok olanağın 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 seçin.

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

Bilinmeyen kullanıcılarından 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 görünüyorrsa, o kişinin e-posta adresini tahrif etmediğini doğrulamak için doğrudan o kişiye danışın.  
• Yedek kopyalar almayı unutmayın. Böylece posta sunucusıyla ilgili bir sorun olması durumunda, değerli bilgilerinizi kaybetmemiş olursunuz.

# Anlık mesajlaşma 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 internet hizmetleriyle ilişkili risklere maruz kalırlar: istenmeyen e-posta, aldatmacalar, dolandırıcılık, dolandırıcılık, kötü amaçlı yazılım vb.

Durumunuzu kendiniz hakkında özel bilgi vermek için kullanmayın

Hakkınıza 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 sunarı 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 gereklidir.

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



Kişisel  
bilgilerinize  
kimin erişimi  
olduğunu  
bilmelisiniz.  
  
Bilgileriniz bulutta  
saklanıyor mu?  
Kim erişebilir?  
Verilerinizi ne  
kadar süreyle  
saklamak  
istiyorsunuz?

Uygulamaya kişisel  
verilerinizi işlemesi  
için hangi izinleri  
verdiğiniz önemlidir.



# KTSO MESLEKİ VE TEKNİK ANADOLULİSESİ

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 yararı olabilir.
- Zorbalığı bildirerek, zorbaya davranışının yanlış olduğunu ve cezalandırılacağını da gösteririz.
- Açil 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 gösteren dağıtım yöntemi nedeniyle adlandırılır. Ancak, bilgisayar virüsleri veya solucanların aksine, bir Truva atı kendi kendine çoğalmaz, bu nedenle geçerli bir kullanıcı tarafından yüklenmesi gereklidir. 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 zorludur.
- Ölçü boşluğu genellikle düşüktür.
- Problem çözme becerileri düşüktür.
- Öfke, üzüntü, hayal kırıklığı gibi duygularının anlantısı ve düzenlemesinde zorluktur.
- İnternette söyleşidelerini o kişiin yüzüne söylememesi pek olası değil.



Sunumu görmek için QR kodu okutunuz.



# IES Antonia Menarguez Costa. Los Alcazares

İSPANYA

**GÜVENLİ INTERNET**

KULLANIMI

!

**İNTERNETİ GÜVENLİ KULLANIN Güvenli**  
bir web sitesinin ne olduğunu öğrenmek için ipuçları

- İçgündülerinizi ve sağıduyunuzu kullanın.
- Bir adres, telefon olup olmadığını kontrol edin numara ve/veya e-posta kişişi.
- Asma kilit yoksa veya 'https://'  
ile başlıyorsa bilgi vermeyin.  
olduğundan daha fazla kişisel bilgi  
normalde vermeyi beklerler, muhtemelen kötü niyetlidirler.
- Yabancılardan gelen istenmeyen e-postalarda reklamı  
yapılan web sitelerine karşı dikkatli olun.

**GÜVENLİ WEB SİTELERİ**

Bir web sitesinde şifreler veya kredi kartı bilgileri gibi özel bilgileri girmeden önce şunları yapabilirsiniz:  
bağlantının iki şekilde güvenli olduğundan emin olun:

- Tarayıcı penceresi çerçevesinde  
bir asma kilit simgesi  
bulunmalıdır.
- Web adresi 'https://'  
ile başlamalıdır. 's', 'güvenli'  
anlamına gelir.

**ÇEREZLER**

**Cookies**

This site uses cookies to offer you a better browsing experience. Find out more on [how we use cookies and how you can change your settings](#).

I accept cookies I refuse cookies

Bu site size daha iyi bir tarama deneyimi sunmak için çerezler kullanır.

• Çerezleri nasıl kullandığımız ve ayarlarınızı nasıl değiştirebileceğiniz hakkında  
daha fazla bilgi edinin.

Çerezleri kabul ediyorum. Çerezleri reddediyorum.



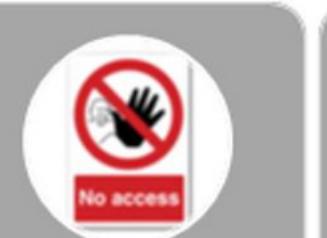
Slaytı görmek için QR  
kodu okutunuz.



# Io GEL Agiou Dimitriou Athens

YUNANİSTAN

## Özel hayatınızı koruyun



Internette paylaşım verilerinize sadece aile üyelerinize, yakın arkadaşlarınıza ve gerçek hayatı tanadığınız ve güvendiğiniz kişilere erişim vererek gizliliğinizi sınırlayın.

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

Çevrimiçi tanışığınız birleyle asla yüz yüze görüşmeyin. Bunu yapmaya karar verirseniz, anne babaniza veya güvendiğiniz bir yetişkinne haber verin, hatta onlardan birini yanınızda alın.

← →

## İnternette paylaşamadıklarımız

**Hiçbir zaman!**

Kişisel veri  
ev adresleri  
internet adresleri  
Kişisel Fotoğraflar  
Çıplak Fotoğraflar  
Çevrimiçi video **Hiçbir zaman!**

## Sahte Haber mi?



- Internette 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

## Genel kural!

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

geri



Slaytı görmek için QR kodu okutunuz.



# IPSCEO A "N.Gallo" di Agrigento

ITALYA



## Presentation IPSCEO A GALLO



### ZORBALIK VE SİBERZORBALIK Aynı Madalyonun İki Yüzü mü?

Aslında biz gençlerin alışkanlıkları çok değişti ve daha önce hayatımız düzenli bir şekilde okullar, diğer aktiviteler, diğer sporlar veya belki sadece arkadaşlarla akşamlar şekilde geçiyorsa, şimdi her şey 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, yazmalarppardımız fark etmeyiz.



### Evrensel Önlem: Öğrenciler Ve Kız Öğrenciler



Slaytı görmek için QR  
kodu okutunuz.



# Escola Secundaria Campos de Melo,Covilha

PORTEKİZ

## Çevrimiçi Güvenlik

Guilherme Alberto - Portugal



Çevrim içi Güvende kalma



Güçlü şifre yaratma

### Güçlü Şifre için tavsiyeler

1 Asla kişisel bilgi kullanmayın.

2 Daha uzun bir parça kullanınız.

3 Her hesap için aynı şifreyi kullanmayın.

4 Rakamlar,simgeler ve hem büyük hem de küçük harfler eklemeyi deneyin.

5 Sözlükte bulunabilecek kelimeleri kullanmaktan kaçınınız.Örneğin YÜZMEN 1 zayıf bir şifre olacaktır.

6 Rastgele paralolar en güçlüsüdür.Sifre oluşturucu kullanabilirsiniz.

### Güçlü Şifre için Tavsiyeler



Slaytı görmek için QR kodu okutunuz.



# GUIDEBOOK OF SAFE USE OF INTERNET

## Cyber Security in Schools



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 the 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 (\$, &, #....)

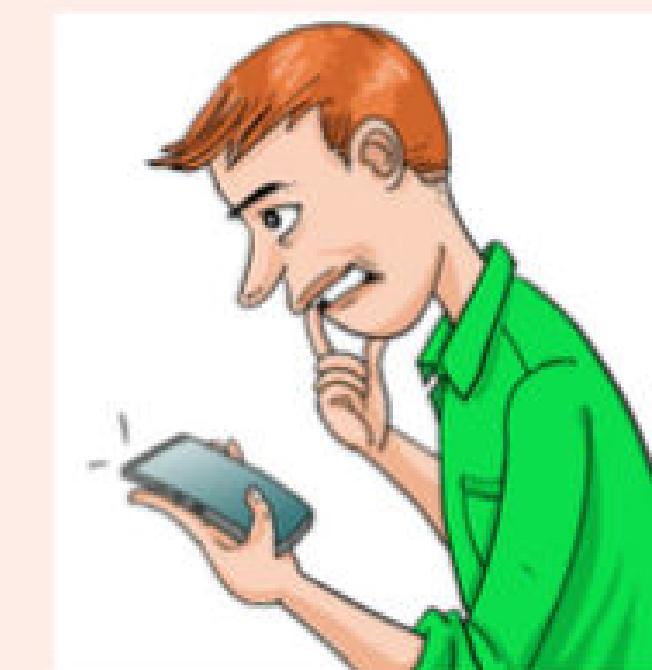
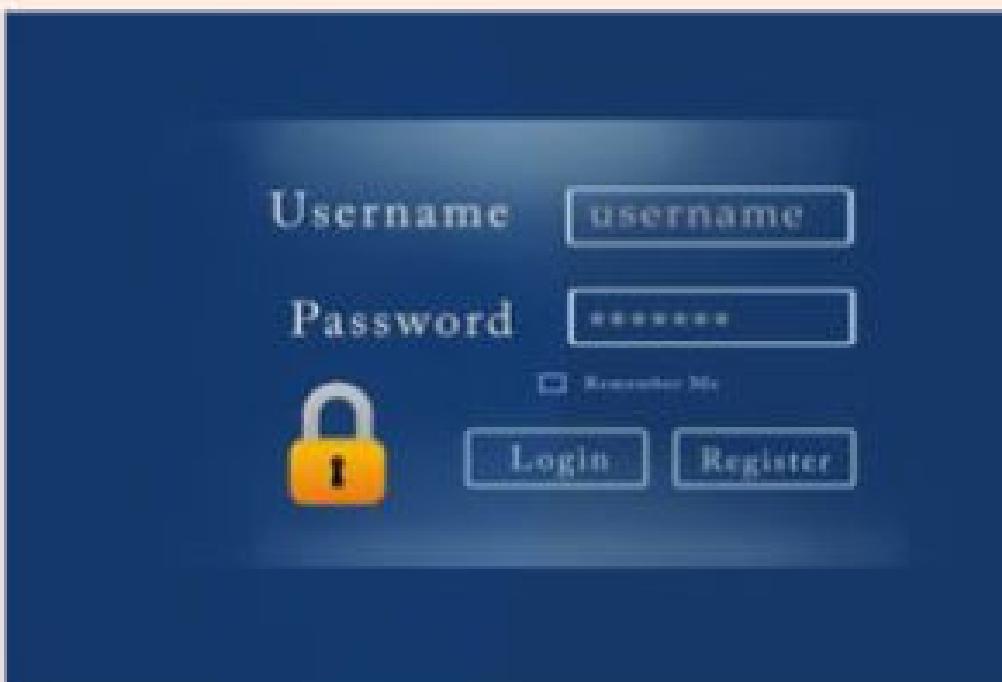
◆ DO NOT use easy-to-guess passwords such as:

"12345678", "qwerty", "aaaaaa", 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.



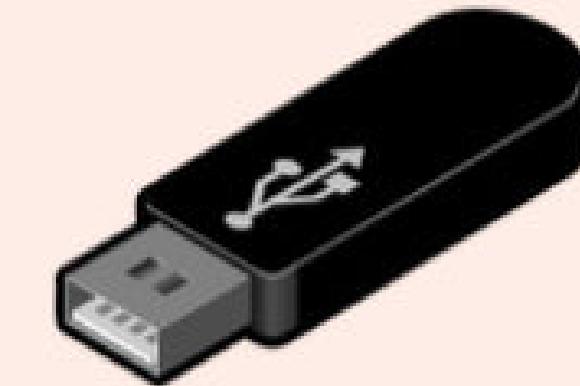
# **Don't wait for a problem, make backup copies.**

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 antivirus.
- ◆ 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:

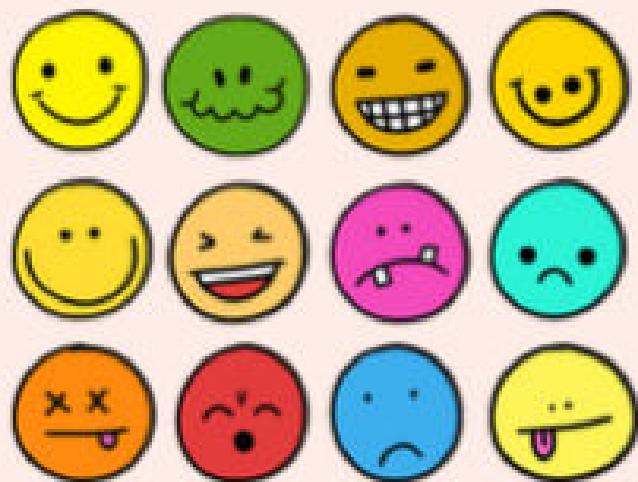
- ◆ Make sure you use a strong password.
- ◆ Whenever a service provides it, turn on 2-Step Verification to add an extra layer of security to the checkout process authentication.
- ◆ Avoid providing information that could compromise your privacy, if you have no other choice, encrypt or compress the files 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, 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.



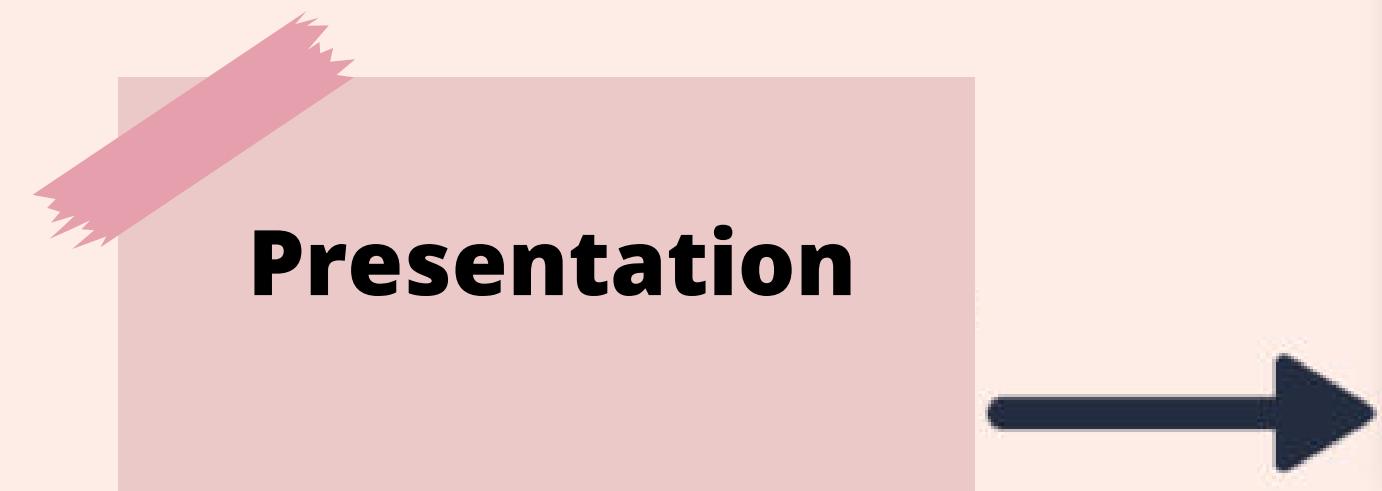
## The security of Wearables.

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.

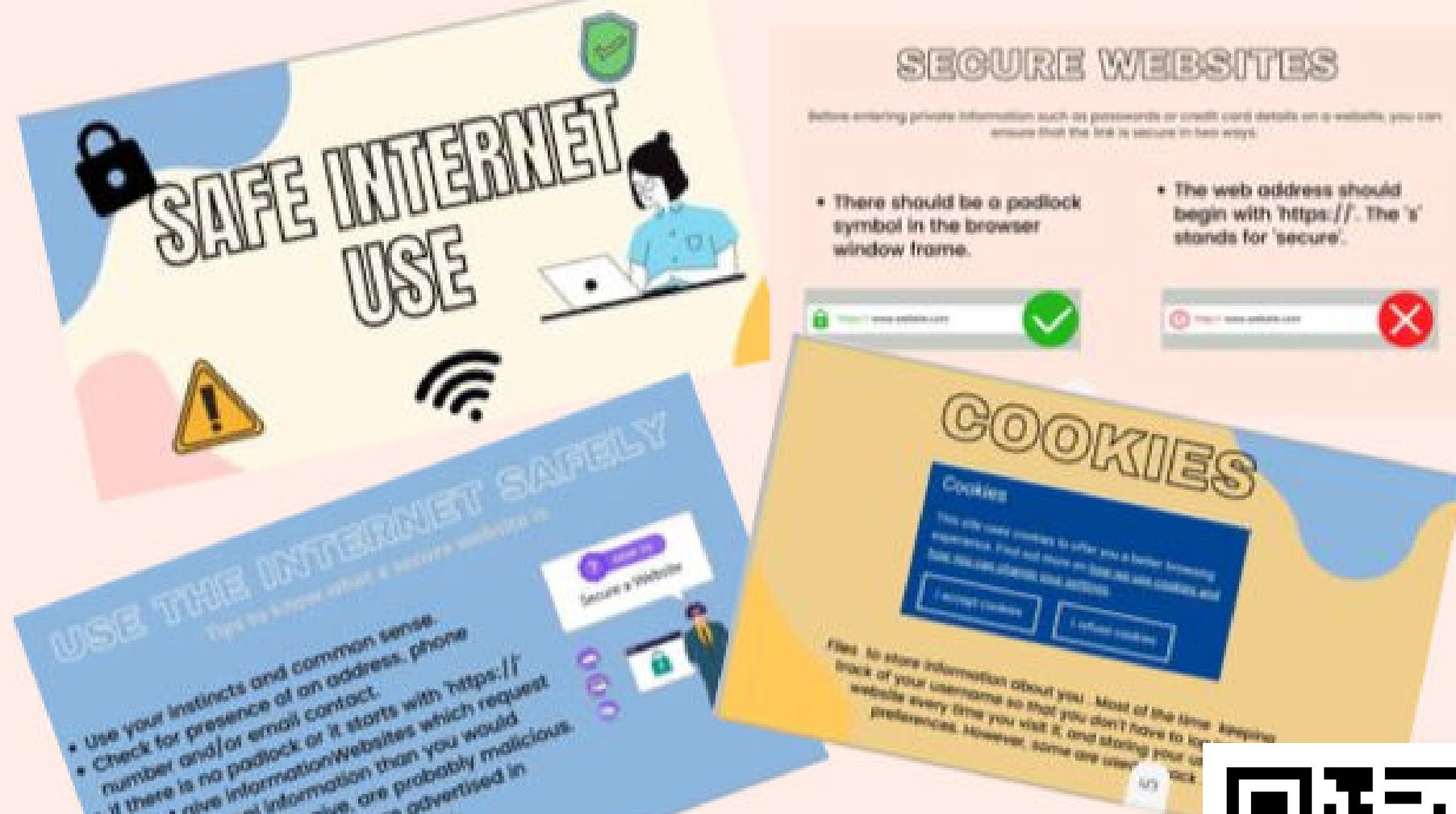


- ◆ They must use some encryption mechanism that guarantees the confidentiality of your information.
  - ◆ You must know who has access to your personal information.
  - ◆ It is important what permissions you give the app to process your personal data.
- Now you need to ask yourself these questions:
- ◆ 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



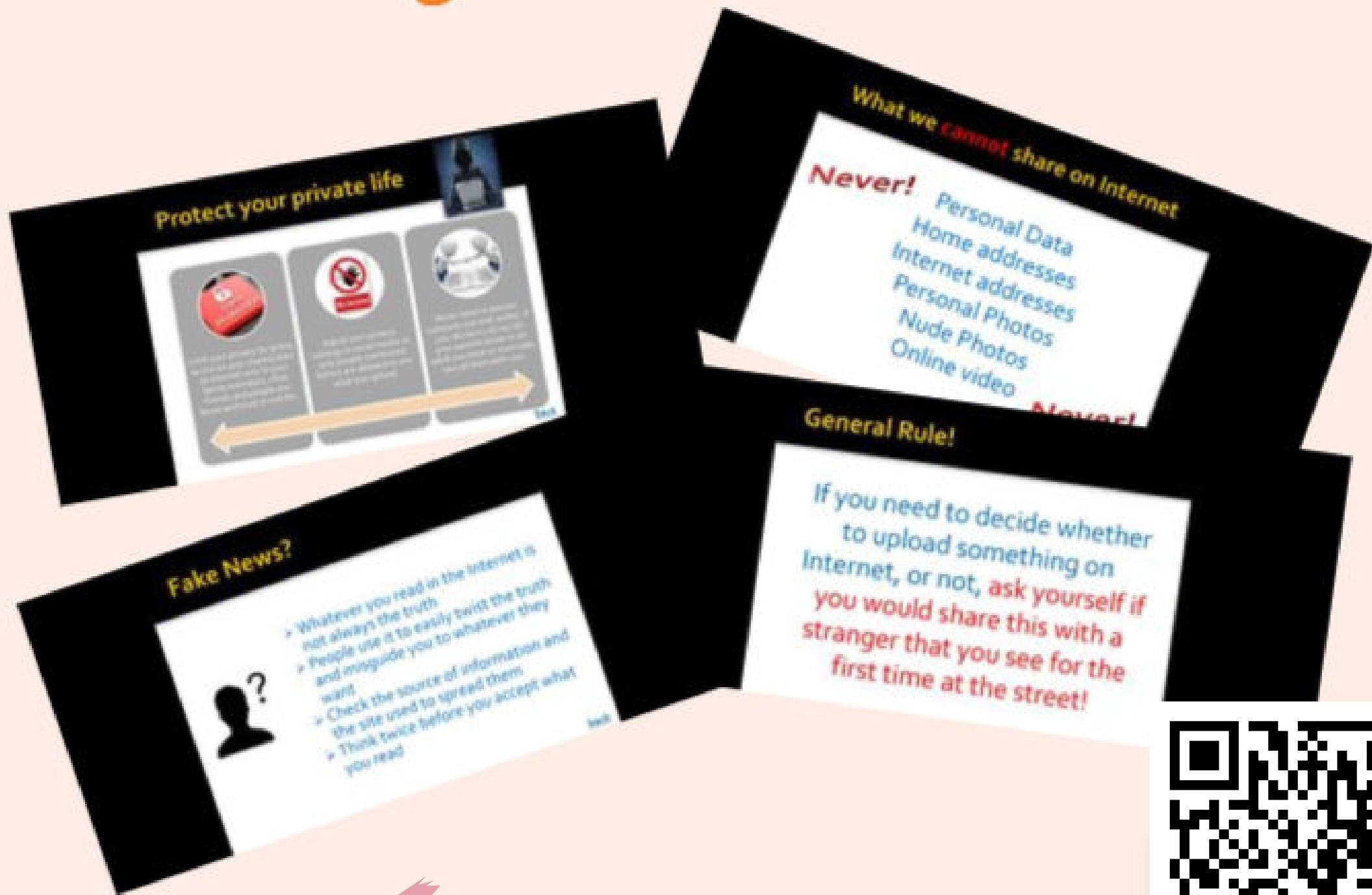
# IES Antonio Menárguez Costa. Los Alcázares - Spain



Presentation



# 1ο GEL Agiou Dimitriou Athens - Greece



Presentation



**IPSCEOA "N. GALLO" di Agrigento - Italia**

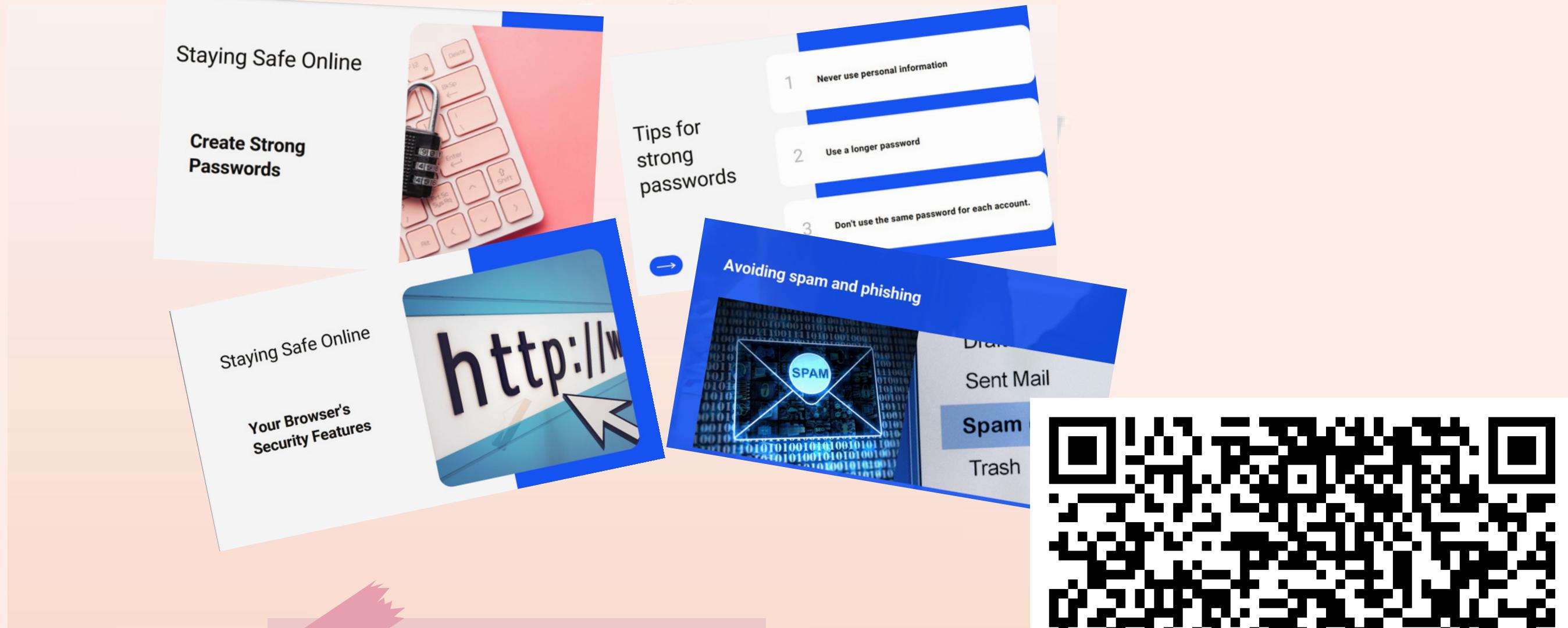


# Presentation

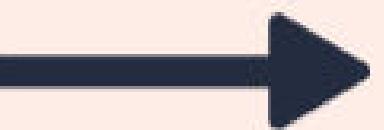


# Escola Secundária Campos Melo

## Covilhã - Portugal



Presentation



# Οδηγός ασφαλούς χρήσης του Διαδικτύου



Greek

# Συνεργατικός Οδηγός

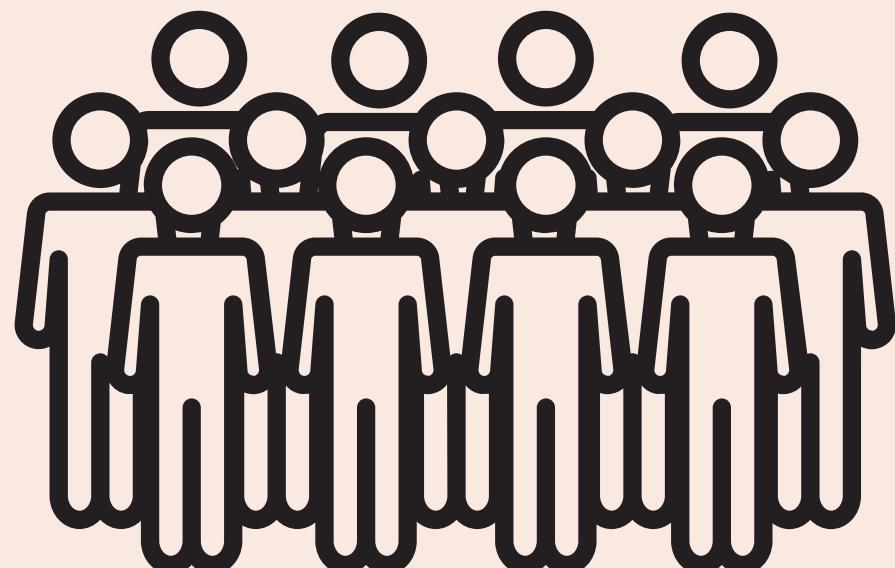
**IES Antonio Menarguez Costa - Λος Αλκαζάρες - Ισπανία**

**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", "ααααα", 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.

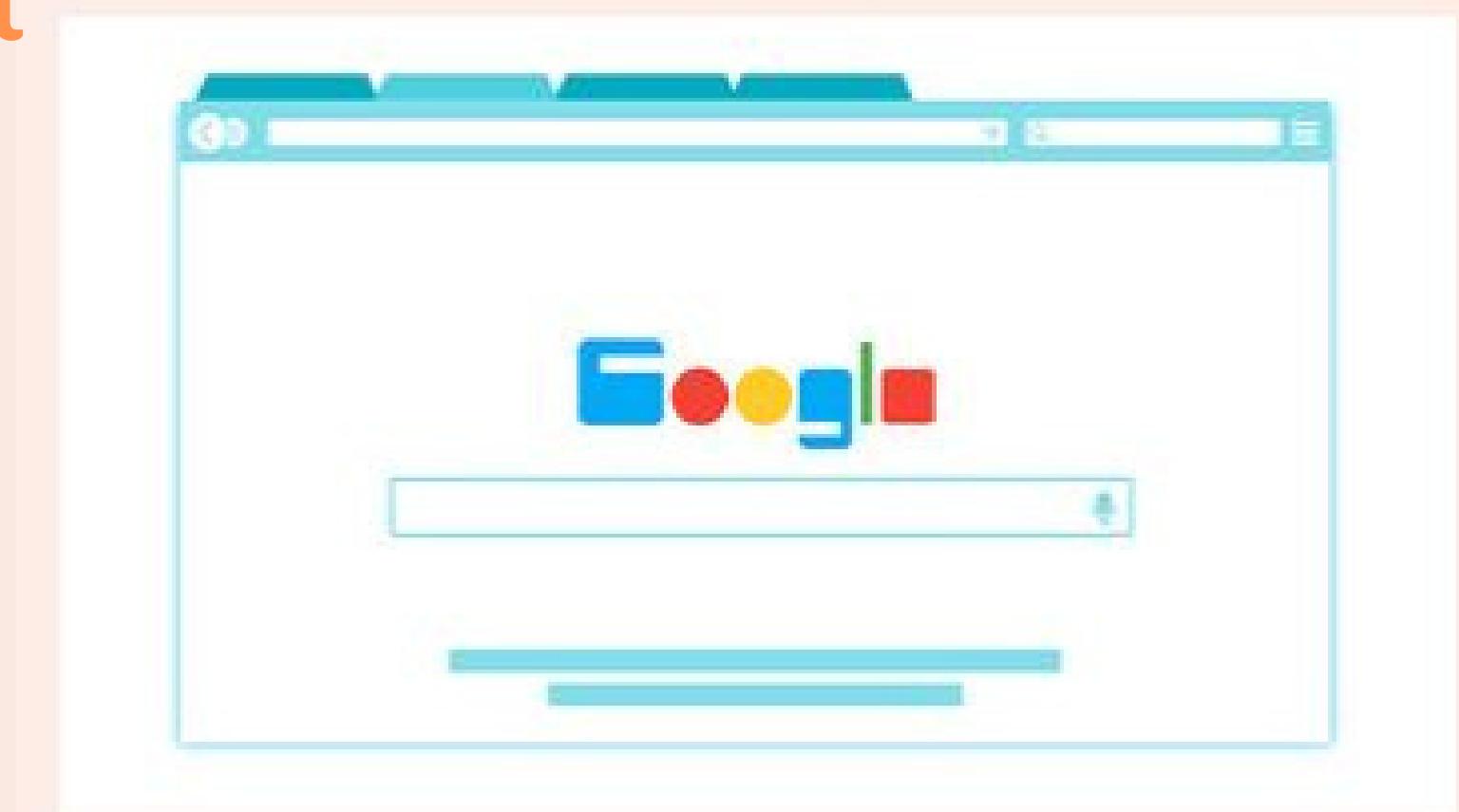
Επέλεξε τα δεδομένα που δεν θα ήθελες να χάσεις σε καμία περίπτωση.

- 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 ίντερνετ:

- 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

The collage consists of three brochures:

- Top Left Brochure:** Title: ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (Safety on the Internet). It features the school's logo, the Erasmus+ logo, and a list of contact information:
  - Όνομα: Beyzanur Canbolat
  - Σχολείο: KTSO Επαγγελματικό Λύκειο
  - Τι αφορά αυτή η εργασία: Διαδικτυακός εκφοβισμός, ασφάλεια, Ιοί, κλπ.
- Top Right Brochure:** Title: Τι είναι ένας ιός Trojan Horse? It discusses the concept of a Trojan horse in computing, noting it is a disguised program that can damage or steal data. It includes a screenshot of a Windows error message "A Trojan Horse Was Found!" and a cartoon illustration of a person sitting at a desk with a laptop, surrounded by speech bubbles containing symbols like #, \$, %, @, !, \*, and !!".
- Bottom Brochure:** Title: ΤΙ ΜΠΟΡΩ ΝΑ ΚΑΝΩ ΑΝ ΗΣΩ ΘΥΜΑ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΚΦΟΒΙΣΜΟΥ (What can I do if I am a victim of cyberbullying). It provides advice:
  - Μπορείτε να συλλέξετε στοιχεία πραβούντας στην προβληματική περιοχή για να χρησιμοποιήσετε όταν πρέπει να στογχίσετε την λενθασμένη και υπόκειται σε τιμωρία.
  - Με την αναφορά του εκφοβισμού, δείχνουμε επίσης στον φάραγγα ότι η συμπεριφορά του είναι λενθασμένη και υπόκειται σε τιμωρία.
  - Είναι βρίσκετε σε επείγοντα κίνδυνο (όσα καλοί συνέχοις και σας ενοχλούν, ή τοποθετείσανται κ.λπ.) μπορείτε να επικονιωθείτε με την αστυνομία.



# IES Antonio Menarguez Costa - Λος Αλκαζάρες - Ισπανία

**Ασφαλής Χρήση Διαδικτύου**

- Πρέπει να υπάρχει ένα λουκέτο στο πρόγραμμα περιήγησης στο πλαίσιο παραθύρου της διεύθυνσης
- Η διεύθυνση πρέπει να ξεκινάει με "https://". Το "s" βγαίνει από την αγγλική λέξη secure που σημαίνει ασφάλεια.

**ΜΠΙΣΚΟΤΑΚΙΑ**

**Cookies**

This site uses cookies to offer you a better browsing experience. Find out more on [how we use cookies and how you can change your settings](#).

I accept cookies I refuse cookies

Είναι αρχεία για την αποθήκευση πληροφοριών σχετικά με εσάς. Τις περισσότερες φορές αποθηκεύετε το όνομα χρήστη σας, ώστε να μην χρειάζεται να συνδεθείτε σε μία ιστοσελίδα κάθε φορά που την επισκέπτεστε και για να αποθηκεύονται οι προτιμήσεις σας. Ωστόσο, ορισμένα χρησιμοποιούνται για την παρακολούθηση σας.

**ΧΡΗΣΙΜΟΠΟΙΗΣΤΕ ΤΟ INTERNET ΜΕ ΑΣΦΑΛΕΙΑ**

Συμβουλές για το πωά σελίδα είναι ασφαλής

- Χρησιμοποιήστε το ένστικτό σας και την κοινή λογική.
- Ελέγχετε για την παρουσία διεύθυνσης, τηλεφώνου ή / και email επικοινωνίας.
- Εάν δεν υπάρχει λουκέτο ή ξεκινά με 'https://' μην δίνετε πληροφορίες. Ιστότοποι που ζητούν περισσότερες προσωπικές πληροφορίες από ό,τι θα περιμένατε κανονικά, είναι πιθανώς κακόβουλοι.
- Να είστε προσεκτικοί με τους ιστότοπους που διαφημίζονται σε ανεπιθύμητα email από αγνώστους.



# 1ο ΓΕΛ Αγίου Δημητρίου - Αθήνα - Ελλάδα

Ασφάλεια στο διαδίκτυο

Ιωάννης Σάρτζ  
1ο ΓΕΛ Αγίου Δημητρίου

Χάκινγκ

Παρενόχληση

Κυβερνο-εκφοβισμός

Εξάρτηση

Παραπληροφόρηση

Για Κωδικούς

Ασφαλές διαδίκτυο...?

Αποφύγετε τα προφανή και μη χρησιμοποιείτε λέξεις που υπάρχουν στο λεξικό. Δεν χρησιμοποιούμε κωδικούς πρόσβασης όπως "123456" ή τη λέξη "password" ή το όνομά σας κ.λπ.

Πρέπει να χρησιμοποιήσετε τη φαντασία σας για να δημιουργήσετε τον κωδικό πρόσβασής σας, ώστε να είναι κάπι που μπορείτε να θυμάστε εύκολα, αλλά οι άλλοι δεν θα το μαντέψουν ποτέ!

Χρησιμοποιήστε γράμματα μαζί με αριθμούς και σύμβολα στους κωδικούς πρόσβασής σας!

Χρησιμοποιήστε περισσότερους από 8 χαρακτήρες. Όσο μεγαλύτεροι είναι οι κωδικοί, τόσο πιο δύσκολο είναι να σπάσουν.

Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης σε δόλους τους λογαριασμούς σας. Αποσυνδεθείτε όταν τελειώσετε.

Μην μοιράζεστε τους κωδικούς σας με κανέναν. Οι κωδικοί μας είναι καθαρά προσωπικοί.

Ενεργοποιήστε την επαλήθευση ταυτότητας δύο παραγόντων (2FA). Απαιτείται όποιος το έχει ενεργοποιήσει πέρα από τον κωδικό πρόσβασής του, να εισάγει άλλο ένα στοιχείο στους λογαριασμούς του. Αυτή η μέθοδος θα ενισχύει την προστασία των διαδικτυακών λογαριασμών σας ενεργοποιώντας τα πιο ισχυρά διαθέσιμα εργαλεία ελέγχου ταυτότητας, όπως βιομετρικά στοιχεία ή έναν κωδικό πρόσβασης μίας χρήσης που αποστέλλεται στο τηλέφωνό σας.

Χρησιμοποίησε ισχυρούς κωδικούς για όλους τους λογαριασμούς

Χρησιμοποίησε διαφορετικούς κωδικούς για κάθε λογαριασμό

Κατήγγειλε ότι ύποπτη συμπεριφορά πέφει στην αντίληψή σου

Μη δημοσιεύει προσωπικά δεδομένα

Χρησιμοποίησε αντικά προγράμματα στον υπολογιστή σου

Μην πατάς σε όποιο υπεραυνδέαμο σου προτείνουν

Μην ανεβάζεις βίντεο ή φωτογραφίες

Μην ανεβάζεις φωτογραφίες ή βίντεο άλλων



# IPSCEOA "N. Gallo" - Αγριτζέντο - Ιταλία

The collage consists of four posters:

- Top Left:** A poster titled "Παρουσίαση IPSCEOA GALLO" featuring the school's logo (I.I.S.S. "GALLO" AGRIGENTO) and a word cloud centered around the term "cyberbulismo". The word cloud includes terms like "adulti", "online", "minorenne", "cellulari", "violenza", "molesia", "giuristi", "utilizzato", "cittadino", "ordinamento", "attivo", "ordinamento", "elettronico", "privacy", "messaggistica", "cyberharassment", "civile", "ma", "volte", "riguardo", "on", "elettronico", "solito", "bo", "dall'educatore", "corrente".
- Top Right:** A flowchart titled "Παγκόσμια πρόληψη: φοιτήτες και φοιτήτριες". It shows a circular process:
  - Start: Ενημερώστε και ενασθήτοποιήστε
  - Step 1: Ο εκφοβισμός και ο διαδικτυακός εκφοβισμός είναι συχνά ανάμεσα μας
  - Step 2: Μπεσοτηθέση του άλλου
  - Step 3: Δράσε
  - Step 4: Καταλαβέστι μερικές συμπεριφορές δεν είναι αστεία και μπορούν να βλάψουν
  - Step 5: Κατανόηση από ποιον πρέπει να ζητήσεις βοήθεια
  - End: Ενημερώστε και ενασθήτοποιήστε
- Bottom Left:** A poster titled "ΕΚΦΟΒΙΣΜΟΣ ΚΑΙ ΚΥΒΕΡΝΟΕΚΦΟΒΙΣΜΟΣ Δύο όψεις του ίδιου νομίσματος;" featuring a quote in Greek and an illustration of a person looking at a screen.
- Bottom Right:** A poster titled "CYBERBULLISMO I νοοί" showing social media icons (Facebook, YouTube) and a keyboard.



# Escola Secundaria Campos de Melo - Κοβίλια - Πορτογαλία

**Ασφάλεια στο Διαδίκτυο**  
Guilherme Alberto  
Πορτογαλία

**Για να μείνεις ασφαλής online**

Προσπάθησε να συμπεριλάβεις νούμερα, σύμβολα, κεφαλαία και γράμματα

Αποφέυγουμε να χρησιμοποιούμε που υπάρχουν στο λεξικό πχ. είναι ένας αδύναμος και τυχαίοι κωδικοί είναι οι που δεν μπορείς να φτιάξεις χρησιμοποίησε μία μηχανή τυχαίων κωδικών.

**Για να μείνεις ασφαλής online**

Φτιάξε ισχυρούς κωδικούς

**Για να μείνεις ασφαλής online**

Απέφυγε το κακόβουλο λογισμικό



# 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

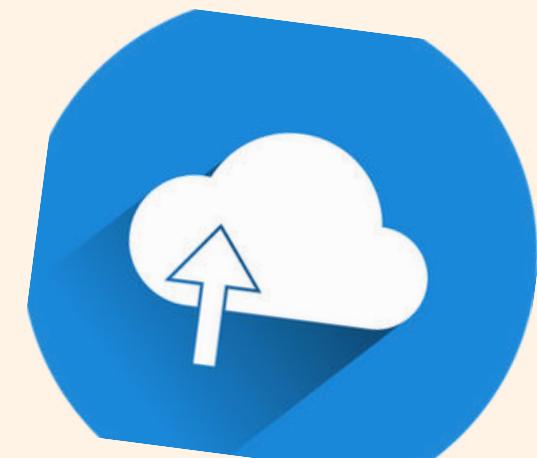
# I tuoi dispositivi memorizzano molte informazioni private

Uno dei motivi principali per proteggere i nostri dispositivi è 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 (\$, &, #...);

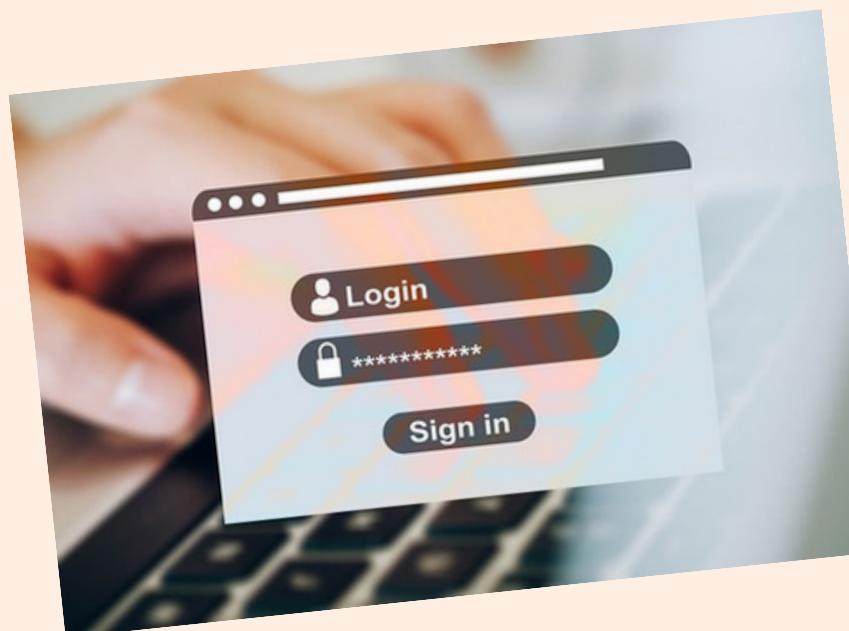
**NON** utilizzare password facili da indovinare

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.

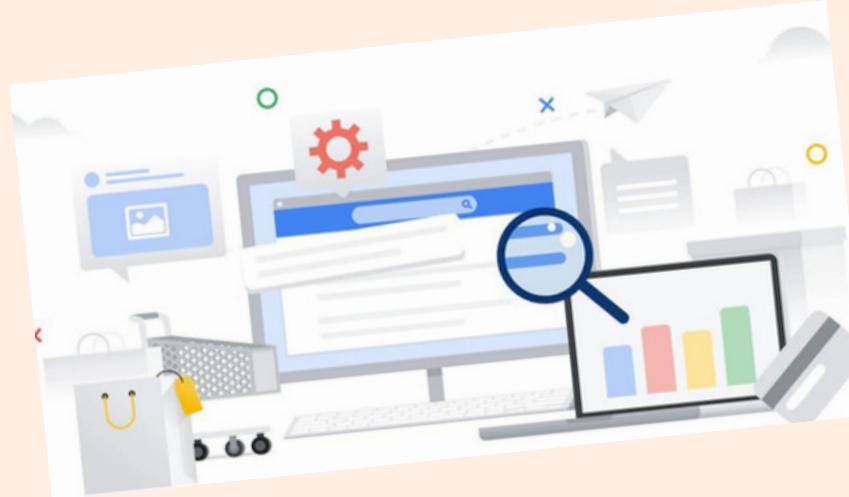
**NON** utilizzare la stessa password su piú servizi.



# **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 catturare 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*

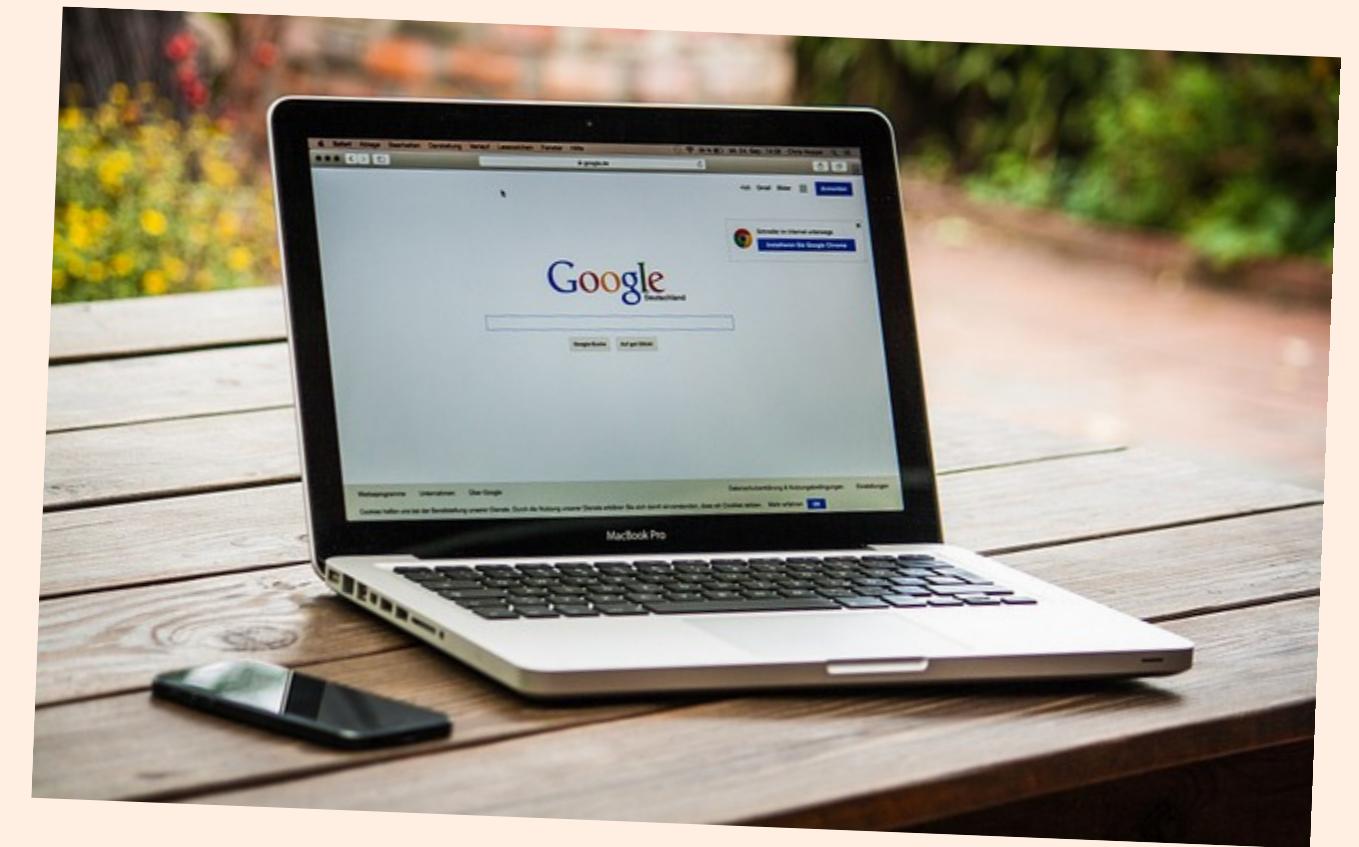


*3. Eseguire il backup*

*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 tutti 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 possibilità, 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 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 messaggistica istantanea

WhatsApp e il resto delle applicazioni di messaggistica istantanea incorporano molte funzionalità: 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 critografato.

\*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 trattamento delle tue informazioni personali.

Devono utilizzare un meccanismo di crittografia che garantisca la riservatezza delle tue informazioni.

Devi sapere chi ha accesso alle tue informazioni personali.

È 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 può accedervi?

Per quanto tempo vuoi conservare i tuoi dati?



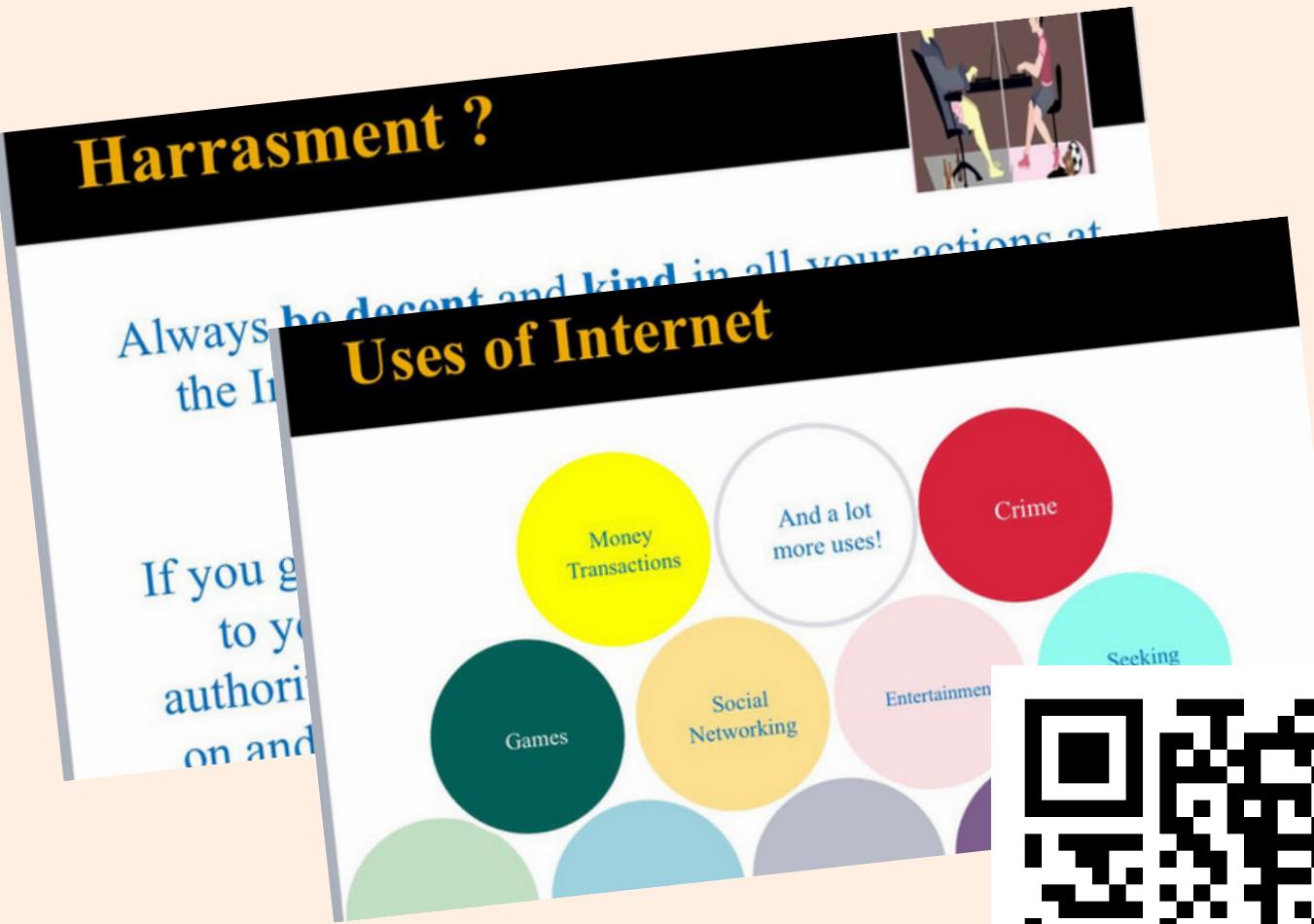
# KTSO VOCATIONAL HIGH SCHOOL TURKEY



# IES Antonio Mènarguez Costa. Los Alcàzares SPAIN



# 1ο GEL Agiou Dimitriou Athens GREECE



# IPSCEOA Nicolò Gallo di Agrigento ITALY

In the last year, there have been many suicides of children who have been victims of bullying and cyberbullying, and it is important to talk at school to prevent these phenomena, through constant information, because the school together with the family is the center of our formation and must consciously watch over what happens. We young people often underestimate the phenomena of bullying and cyberbullying, we consider them only "jokes", "stunts" and perhaps

IN FACT, DURING THE PANDEMIC, WITH DISTANCE TEACHING, WE GUYS HAD VERY FEW OPPORTUNITIES TO COMPARE AND WE FELT ALONE, WE WERE ALONE IN FRONT OF A COLD SCREEN, THAT MADE US AND MAKES US FEEL PROTECTED. THIS LEADS US SLOWLY TO NO LONGER PERCEIVE THE "TRUE" AND REAL EMOTIONS, THAT OFTEN TO ACT WITHOUT THINKING THAT ON THE OTHER SIDE THERE ISN'T A ROBOT, BUT A REAL PERSON WITH HIS TRUE EMOTIONS, HIS TRUE FEELINGS AND HIS TRUE FRAGILITY. SO OFTEN WE DO NOT REALIZE WHAT WE WRITE OR PUBLISH OR THAT WE SPREAD, IMAGES, VIDEOS, WORDS, COMMENTS WHICH ARE HEAVY AND OFFENSIVE THAT LIVES OF OTHERS IN A MASSIVE

BULLING AND  
CYBERBULLYNG  
Two sides of the same coin?

In fact, the habits of us young people  
In fact, the habits of us young people



I.I.S.S.  
"GALLO"  
AGRIENTO  
Presentation IPSCEOA  
GALLO

Cyberbulismo  
adulti penale  
online minorene  
distinzione non cibebulismo  
violazione  
cellulari  
stato molestia  
o ossia giuristi  
messaggistica  
effettuati  
utilizzato  
cibeharassment



# 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

26

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

The collage consists of three separate graphic elements:

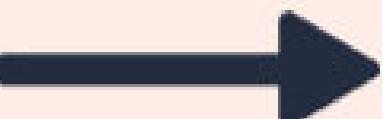
- Top Left:** A white card titled "USO SEGURO DE INTERNET" (Safe Internet Use) featuring a lock icon, a checkmark, and a person using a laptop. It includes a yellow warning sign icon.
- Bottom Left:** A blue card titled "UTILICE INTERNET DE FORMA SEGURA" (Use the Internet Safely) with the subtext "Comprueba que las páginas web que visitas son seguras". It lists several tips:
  - Usa tu sentido común.
  - Comprueba la presencia de una dirección teléfono.
  - Si no hay candado, o comienza con https:// no dar información personal de la que deseas a más, en otras palabras, web que solicitan información secreta a tí.
  - Tenga cuidado con las webs que se anuncian en Google o las aplicaciones de correo.
- Top Right:** A pink card titled "SITIOS WEB SEGUROS" (Safe Websites) with the subtext "Before entering private information such as passwords or credit card details on a website, you can ensure that the site is secure in the way". It shows two browser windows: one with a green lock and checkmark labeled "www.galletas.com" and another with a red X and error icon labeled "www.galletas.com".

A large black arrow points from the bottom left infographic towards a large QR code on the right.

# 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**

**ESCOLA SECUNDARIA CAMPOS DE MELO, COUILHA 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 "AAAAA",  
PLACAS DE VEHÍCULOS, ETC. NO COMPARTAS TUS  
CONTRASEÑAS.



MAYÚSCULAS (A, B, C...) MINÚSCULAS (a, b, c...)



NÚMEROS (1, 2, 3...)

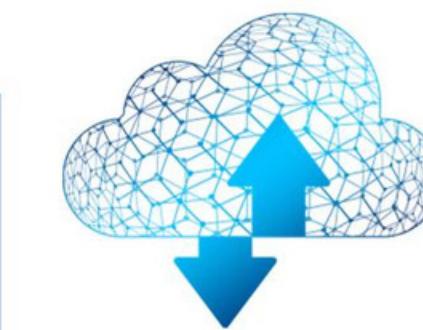


**I. SELECCIONA LA  
INFORMACIÓN QUE BAJO  
NINGÚN CONCEPTO TE  
GUSTARÍA PERDER.**

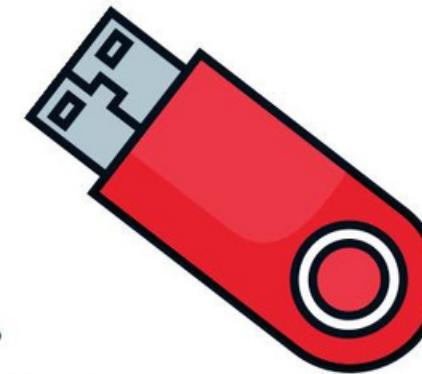
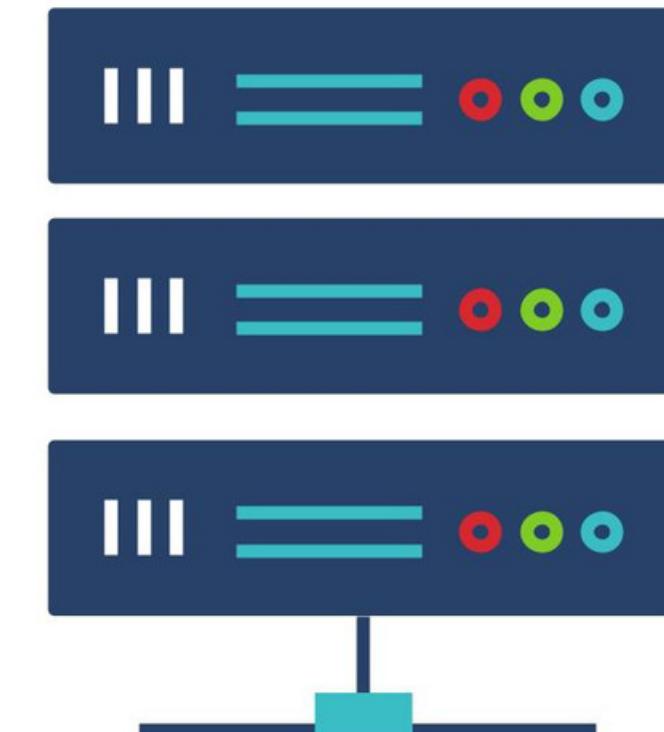
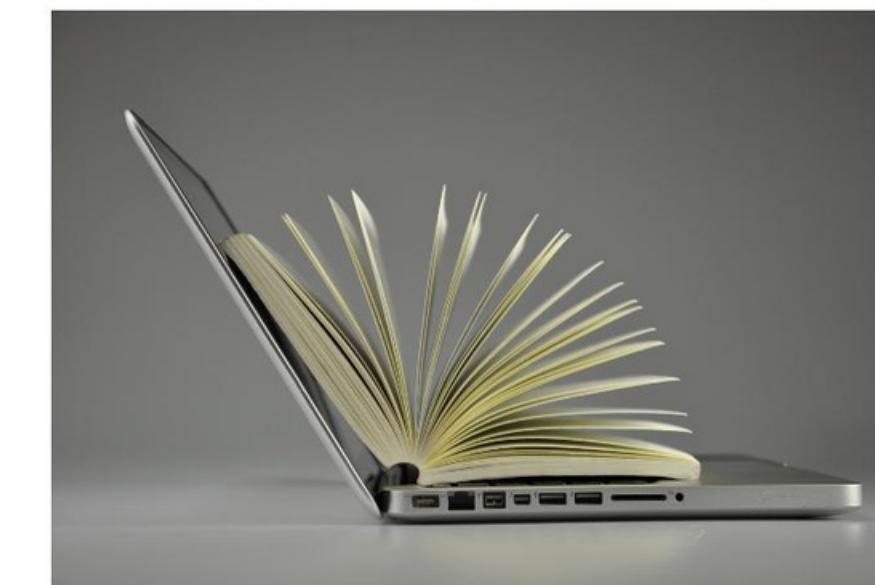
**2. ELIGE EL MEDIO  
DONDE SE ALMACENARÁ  
LA INFORMACIÓN.**

**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.**



```
if ($window.scrollTop() > header1_initialDistance) {  
    if (parseInt(header1.css('padding-top'), 10) <= header1_initialPadding) {  
        header1.css('padding-top', '' + $window.scrollTop() - header1_initialDistance);  
    }  
} else {  
    header1.css('padding-top', '' + header1_initialPadding + 'px');  
}  
  
if ($window.scrollTop() > header2_initialDistance) {  
    if (parseInt(header2.css('padding-top'), 10) <= header2_initialPadding) {  
        header2.css('padding-top', '' + $window.scrollTop() - header2_initialDistance);  
    }  
} else {  
    header2.css('padding-top', '' + header2_initialPadding + 'px');  
}
```

A screenshot of a computer screen displaying a block of JavaScript code. The code uses jQuery to check the scroll position of the window against two specific header elements. If the scroll position is greater than a defined initial distance, it checks if the current padding top of the header is less than or equal to the initial padding. If so, it updates the padding top to the current scroll position minus the initial distance. If not, it sets the padding top to the initial value. Similar logic is applied to another header element.

# CORREO ELECTRONICO



**CORREO ELECTRÓNICO!**

**DÉBES 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 ELLA, 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**

**COMPRISE 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**

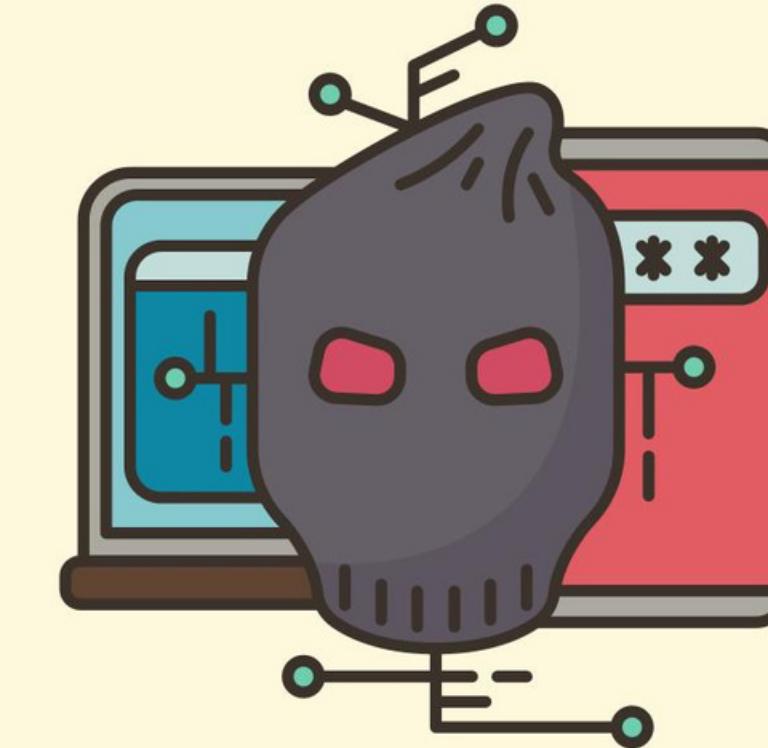
**DIRECTAMENTE A ESA PERSONA PARA CONFIRMAR QUE NO HA FALSIFICADO SU DIRECCIÓN DE CORREO ELECTRÓNICO.**

**NO OLVIDES REALIZAR COPIAS DE SEGURIDAD PARA NO PERDER INFORMACIÓN VALIOSA EN EL CASO DE UN PROBLEMA CON EL SERVIDOR DE CORREO.**



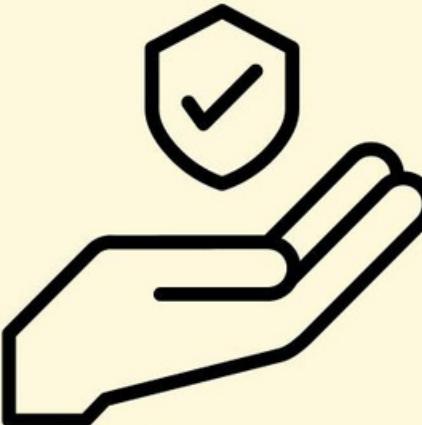
# RIESGOS EN LOS SERVICIOS DE MENSAJERÍA INSTANTÁNEA.

- 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.
- ASEGUÍRATE 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 ENCRYPTACIÓN 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?



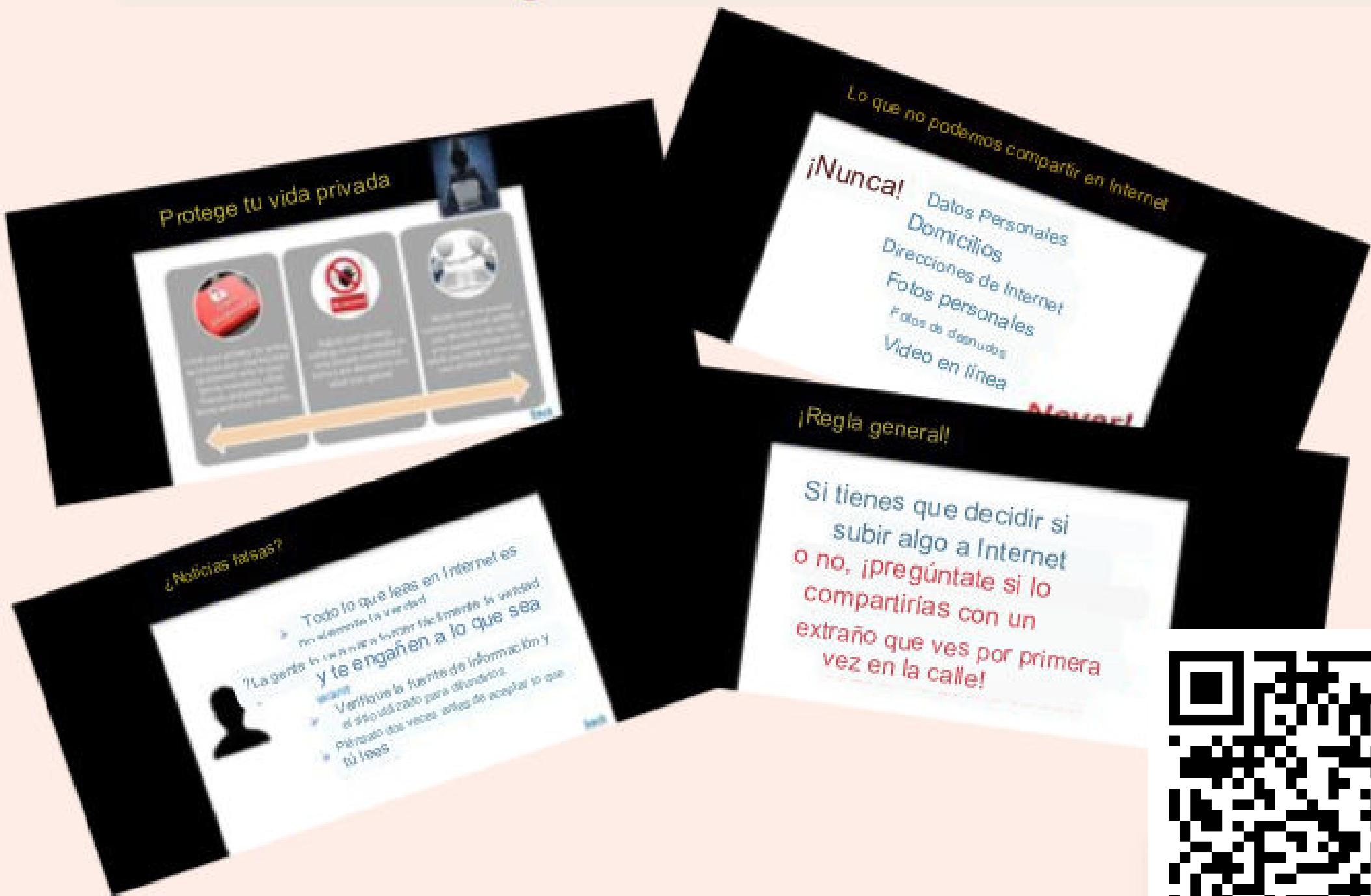
# ESCUELA SECUNDARIA PROFESIONAL KTSO TURQUÍA



# 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



