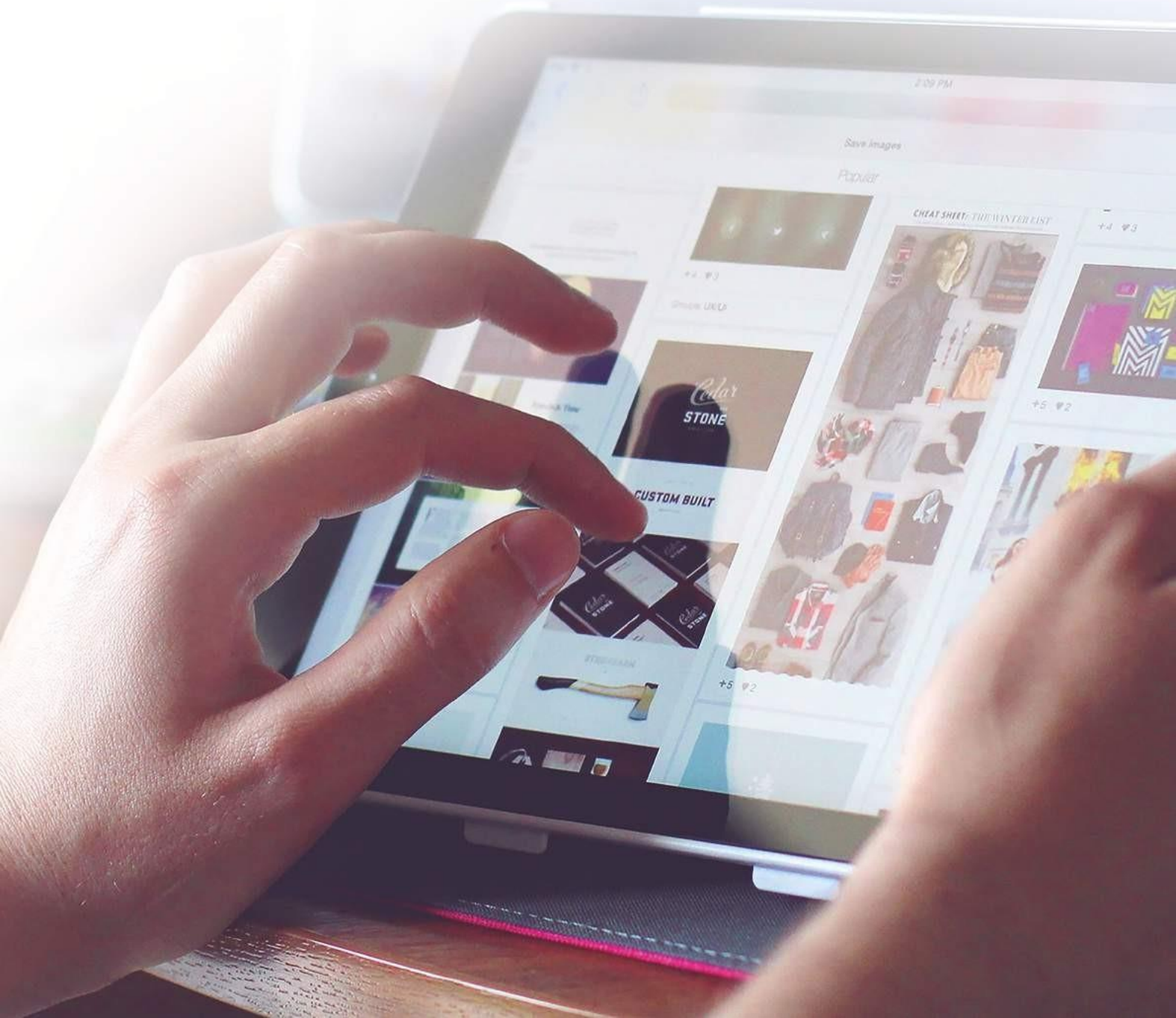
安全网购

实用指南



安全网购

实用指南


AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
aecosan
Policía Nacional

目　录

简介

1. 网购或者网上预定之前

1.1　设备调试
1.1.1. 基本的安全建议
1.1.2. 网络配置
1.2.　确定可信的在线商店
1.2.1. 检查合法的交易信息
1.2.2. 确定业主/负责贸易
1.2.3. 验证域名所有者和其他注册数据
1.2.4. 检查它是否是安全通信（HTTPS）
1.2.5.　信任章
1.3.　欺诈检测
1.3.1. 网络钓鱼
1.3.2. 梳理
1.3.3. 虚假的在线销售页面
1.3.4. 通过电子邮件的诈骗
1.3.5. 针对工业和知识产权的犯罪
1.3.6. 欺诈或可疑的应用程序
1.3.7. 二手销售或购买服务

2. 如果已经决定购买

2.1.　在线付款方式
2.1.1.现金出货
2.1.2.货到付款
2.1.3.银行转帐
2.1.4.银行卡支付
2.1.5.通过第三方付款
2.2.　用户帐户的配置
2.2.1.安全密码
2.2.2.启动双重验证方式
2.2.3.恢复帐户
2.2.4.何时储存付款信息
2.2.5.通过应用程序购买的具体注意事项

3. 购买或者订购之后

3.1.退款权利
3.2.保质期
3.3.破损产品：寄送费用和重新寄送
3.4.个人信息权利
3.5.保密和发布数据的责任
3.6.安全措施以及对于违规行为的通知
3.7.广告

4. 如何申诉

5. 对于安全网购的10个基础建议

附件：有关网络安全、消费和资料保护等材料的授权

简介

电子商务是近几年来社会信息发展较快的一项服务并代表着未来数字经济潜力最大的活动之一。根据国家市场竞争委员会（简称CNMC）统计，在西班牙，2016年的交易额达到了241,8500,0000欧元， 并在2017年的第一季度超过了67，0000，0000欧元， 几乎超过了前一年的四分之一。事实上，根据欧盟统计局的数据，在线订购商品和服务的用户比例为50%，高于欧盟平均水平4个百分点。

根据CNMC统计的交易数量，44%的买卖交易是在西班牙网站上注册。而93%从西班牙卖出的货物到达了欧盟。

这些数字说明了电子商务在几年内获得的维度和对未来增长的预测。 但是，从经济角度来看，公共机构必须确保获得这些服务的消费者和用户的权利，以便在网上购买或签订合同之前，期间和之后为他们提供最好的保护。

在整个过程的每一个阶段，这些服务的消费者和使用者都可能遇到复杂而多样的情况，需要求供货厂商针对其销售领域，做出相应回应。

本指南全面收集协助用户进行在线购买或订购流程的权利，并通过各种方式提供意见和建议：隐私（西班牙资料保护局），安全（西班牙国家网络安全研究所），消费 （西班牙消费，食品安全和营养机构）和起诉犯罪或欺诈行为（国家警察）。 该指南附有七个部分，用户需要注意和考虑的主要问题被更简洁地列出。

此外，推动促进个人资料的保护措施，消费者的权利，进行商业交易的网络和设备的安全以及起诉欺诈行为的做法是建立一个信任的氛围，实现创新和可持续发展的基本先决条件。

本指南不仅仅适用于作为消费者或者电子商务服务用户的普通公民，也适用于在这一行业中展开经济活动的公司们。 为此，加强本指南的推广意味着增强了那些应当增强竞争优势，让市民时刻掌握灵通的信息是任何企业发展的关键，尤其是对于在信息环境下，那些以信任为基础而发展的新型企业。

1.1. 设备调试

1. 1. 1. 基本安全建议

为了实现安全在线购物，必须对所使用的设备进行正确的配置和保护，以防止这种错误配置或可能的恶意软件感染，从而保证用户和在线商店之间交换数据。

预防性保护措施:

- 安装防病毒工具并在交易之前分析设备以检测可能的威胁。 如果该设备受到感染，则可能致使购买本身受到威胁，并可能导致与其相关的信息收到安全威胁。
- 确认设备的操作系统已经更新至最新版本，以及安装的所有程序和应用程序，以避免这些安全漏洞被网络犯罪分子利用，在用户不知情的情况下控制和执行恶意行为。
- 查看已安装的程序和应用程序，并删除所有未使用的程序和应用程序。 我们拥有的程序越多，保持设备更新和保护的难度就越大，同时也会减慢和阻碍设备的性能。
- 避免使用公共或共享的电脑、平板电脑和智能手机进行在线购物。 一般来说，我们无法知道此设备的安全状态或其使用目的（您浏览的页面），并可能包含病毒或任何其他类型的恶意代码。

更多信息请见:

Links

- *受感染设备的症状*
- *免费的防病毒工具*
- *更新的重要性*
- *如何保护设备及其中包含的信息*
- *不安装更新的后果*
- *使用公用计算机时要考虑的注意事项*
- *如何使用公共设备的情况*

1.1.2.网络调试

为了在安全的环境中进行在线购买，将设备正确配置和使用可信的网络连接对于保护我们的信息同样重要。

在WiFi网络中要考虑的注意事项

- 不要将设备连接到公共Wi-Fi网络来进行有机密信息交换的交易，如在线购买，访问银行数据或支付网关的情况，因为在交易过程中通信被截获的风险是很高的。

— 正确配置WiFi家庭路由器，使第三方无法连接到网络。

更多信息请见：

Links

- *保护您的设备*
- *使用公共WiFi网络的风险*
- *何时使用公共WiFi网络*
- *WiFi网络配置的基本措施*
- *如何通过7个步骤来保护WiFi网络*
- *我们刷新你如何保护WiFi家庭网络*

1.2. 确定可信的在线商店

1.2.1. 检查合法的交易信息

— 网上商店的信息，根据不同的法律规定，通常包含在“法律声明”，“使用条款”或“隐私政策”等页面中。 它们通常位于网上商业主页上端或下端的访问链接中。

— 法律知识是十分基础性的，原因如下:

- 面对可能的冲突，能使我们知道应该向谁申诉
- 确定适用的法律和有关负责部门
- 它可以用于帮助用户维护相关权利

— 网上交易的强制信息

- 实体的全名（个人，公司，基金会等）
- 税号（NIF，NIE或CIF）
- 您在商业登记簿上的注册详情
- 邮政地址
- 电子邮件地址

从2018年5月25日期,您需要额外添加以下信息:

- 数据的保存期限
- 数据保护的代表身份（如果有的话）（DPD是关于处理个人数据中任何问题的商家联系人）

更多信息请见:

Links
- *互联网安全和隐私指南*
- *数据保护组织法"第5条*
- *通用数据保护条例"第13条*
- *信息社会和电子商务服务法"第10条*

1.2.2. 确认贸易业主或负责人身份

不建议使用没有正确识别其责任的在线商务服务。

无论顾客是否有固定账户，在线商店都需要收集和处理个人数据。例如，当被联系请求报价时。

个人资料只能在向访客和客户通报后才能使用，如果其中任何一方与采购，订约或咨询的管理没有直接关系（典型情况是发广告的），则在数据收集时必须向用户提供反对该处理的可能。

如果个人资料要传达给另一方，有必要事先告知他们沟通的目的，收件人的身份和他们的联系信息。

网上交易提供个人资料方若没有更改身份，则拥有访问，更正，取消和反对（ARCO权利）的权利。 网上交易必须告知顾客行使这些权利的可能性以及要遵循的程序。

有关权益的更多信息，请参阅本指南的第4部分。

Links
- *ARCO权利和新制定的权利*
- *行使ARCO权利的实例*

正确的法律条文例子

在www.micomercioelec.com中有的电子商务可通过文字进行通知
例如：

> *“在 www.micomercioelec.com 上注册的公司是MCOMERCIOE S.L, 地址 calle de la prueba, 1 2º B 28001 Madrid, C.I.F号: B-12345678, 于马德里商业注册局XX.XXX卷, 共XXX页, X项, M-XXXXX页 (页首, MICOMERCIOE).*
>
> *MICOMERCIOE负责包含本网站访问者和用户数据的文件。 您收集的数据具有以下目的：商业关系的管理，以不同方式（包括电子方式）发送广告通信。*
>
> ☐ *我反对将我的数据用于广告目的。*
>
> *访问者和用户可通过写信到上述邮政地址或通过电子邮件的方式行使访问、更正，取消和反对MICOMERCIOE S.L.的权利。 请求必须附有证明申请人身份的文件副本。*

没有足够信息的例子法律文本

> *该网站及其所有内容均为micomercioelec. com所有。 micomercioelec.com将根据 LOPD管理本网站提供的数据。*
> *如果您想就您的个人资料与我们联系，您可以写信给lopd@micomercioelec.com*

未成年

14岁以下的儿童无法授权网上商店获取和处理其个人资料; 需要可代表本人的法定代理人（家长或监护人）。

那些需要处理14岁以下儿童数据的在线商店必须获得其父母或监护人的同意，例如通过发送给其中一方电子表格的链接的方式。

不能要求14岁以下的儿童提供其家庭环境的信息。 唯一的例外是父母或监护人的身份证明和联系信息，借此向其征求获取其孩子的信息。

“数据保护组织法草案”在本指南出版时（2017年12月）议会章程规定未成年人13岁时可以出具其信息许可。

更多信息请见:

互联网由你定
Links

Cookies政策

访问电子商务时，在所使用的计算机（计算机，平板电脑，智能手机等）中可能会下载、收集并存储有关导航信息的。（称为cookie）。

页面负责人有义务通知其使用情况，并询问访问者或客户是否接受这项请求。

有关cookie的信息必须以页面顶部或底部显示，需提供该页面的基本信息（是否使用cookie，使用者信息和使用目的）以及指向另一个页面的链接（cookie策略）来介绍有关使用的更多细节，以及用户如何拒绝其中的使用条款。
通过配置浏览器，是调控cookie使用的最简单方法
我们可以：

- 拒绝所有的cookies
- 拒绝或接受来自特定域名的Cookie
- 只接受访问过的网站而不是其他网站的cookies
- 关闭浏览器时，将所有的cookies清除

更多信息请见：

Links
- *互联网隐私和安全指南*
- *保护您的隐私*
- *关于使用Cookie的指南*

1.2.3. 验证注册者或其他域名注册数据

域名是我们用来访问网站或在线商店的互联网地址的最后一部分。 例如，在www.agpd.es域名将是agpd.es.

域名可以通过中间人（注册商代理）的服务以个人或组织名称（注册人）注册。

如果我们对在线交易及其提供的法律信息有疑问，可以查看是谁注册了与该网站相关的域名，并检查是否此人就是该网站的负责人或与之相关的人员。

有关域所有权查询服务的更多信息：

Links
- *找出你不应该信任的网站*
- *查询以.es结尾的域名*
- *查询以.eu结尾的域名*
- *查询其余域名*

1.2.4. 检验安全通信（HTTPS）

每次通过互联网（名称，ID，信用卡等）提供私人信息时，必须验证网页或移动应用程序是通过使用安全通信协议https发送信息。 该协议用于保护在购买过程中交换信息的安全性。 这样信息传输进行加密，以便没有人进行拦截，并且它有一个有效的安全证书，用来验证网站的身份。

认证机构是负责颁发数字证书的独立机构。 其充当调解人，通过安全监控和质检证书的发放来保证任何一个数字证书的合法性。

需要考虑的事项

- 检查网上商店的网站是否有安全证书。 若有，浏览器将显示一个挂锁形状的图标，URL将以https而不是http开头。
- 检查网络数字证书是否有效，并对应您真正想进行购买的网站。 这些信息对于每个浏览器都有不同的检查，尽管通常情况是通过点击挂锁形式的图标。 它必须核实颁发证书的颁发者（认证机构），接收者（网上商店和域名的公司名称）及其有效期。
- 如果在线商店没有证书或证书无效，则建议不要继续购买流程，并搜索符合最低安全要求的其他网站。
- 对于移动应用程序而言，必须告知用于保护购买过程中的信息和个人数据的安全机制，但我们建议遵循本指南第1.3.6节中的说明。

更多信息请见:

Links
- *有关浏览器中显示的挂锁的信息*
- *如何检查数字证书*

1.2.5. 信托印章

信托印章是有区别性的，其提供给网上商店以展示其在线销售的质量和安全。 为了获得此类印章，需对其质量和安全进行审核或评估，以确保其符合购买的安全标准，并在隐私和消费者保护方面符合法律要求。

一些有信托印章的商店会放一些行为准则，并经常为消费者提供可选择的简单，快捷的问题解决方案。

无论何时您想要进行购买，您都必须检查网上商店是否良好的遵守电子商务实践守则。

如果网上商店有印章，则最有可能在其主页上显示，并且链接到授予印章的组织的网站。 在这个页面上，您可以找到获得该信任印章的优势。

西班牙最知名的信任商标之一是 *Confianza Online.*

更多信息请见:

Links ·*信任印章*

1.3.欺诈检测

1. 3. 1. 网络“钓鱼”

网络钓鱼是通过互联网取代已知服务页面、公共机构、社交网络以及银行、储蓄所和其他金融机构，从而以欺骗手段获取用户信息的最广泛的方法之一。

它包含冒充用户知道的网络服务来欺骗和请求密码，个人或银行信息，然后将其用于或出售给第三方进行其他欺诈。 为了获取这些信息，网络犯罪分子通常会提供一个链接，将用户重新定向到伪装成合法的网页。

避免成为网络钓鱼的受害者提示

— 我们必须堤防提示性信息，或引起用户注意的消息，通常意图让您立即访问链接或下载附件。

— 您不应回复无故发来的或申请索要您个人及银行信息的电子邮件或消息。 您需要通过直接询问消息中涉及的各方或通过信任的第三方：国家安全部队和机构，INCIBE，AEPD等来对比信息的真实性。

— 同样，如果收到来自未知用户的消息甚至是已知的消息，其内容是可疑的，您必须谨慎，不要点击它可能包含的链接。

— 任何机构、公司或信誉良好的服务部门都不会通过电子邮件向您请求访问在线账户或与用户有关的其他数据。 如果您收到上述信息，必须将其删除。 如有疑问，您可以通过官方渠道直接向公司或服务机构进行提问。

更多信息请见:

Links ·*什么是网络钓鱼*
·*如何识别网络钓鱼*
·*网络钓鱼; 试图窃取我们的个人和银行数据的欺诈行为*

1. 3. 2. 通过行用卡进行欺诈

犯罪活动包括欺诈性地使用大量的有效信用卡/借记卡在虚拟商店进行网上购物。

这种模式主要影响在线商店。 若刚刚遇到此类欺诈行为，持卡人将必须做出相应的投诉，并要求退款。

提示和建议

- 定期查看您银行卡账户变动情况，若看到任何可疑的地方，可以进行申诉。
- 如果丢失或被盗，请及时进行废卡操作。

1.3.3.虚假的在线销售页面

当今，建立一个网站并伪装成网上商店来进行诈骗行为十分简单。用户购买的产品或服务永远不会被送出，因为在该网页背后没有任何商业支持。

避免在虚假商店购买提示

- 最好在官方网站或有威望或加固防火墙的网页上进行购买。
- 不建议进行购买，若没有以下方面的相关信息：
  - 公司的实际和实际数据：持有人，NIF / CIF，财政地址等
  - 销售、退货或索赔条件
  - 法律文本：法律声明，隐私政策等
- 当商店的价格远低于市场价格，或者所有产品以相同的价格出售时，不论型号，您要注意堤防。
- 关于网页的设计，请不要信任：
  - 如果它不传输同质性（在同一个窗口中有许多不同的字体）
  - 封面照片可以在互联网上的其他地方找到
  - 图像质量不好：像素差，质量差或包含水印
  - 网络似乎是某个品牌的合法页面
  - 出现翻译错误的文字。 例如，“Home”部分被翻译为“Casa”来替代“开始”，这是很常见的。
- 如果网站声称有多种付款方式，但最终只接受信用卡支付

更多信息请见：

Links

- *避免在假冒的网上商店中欺诈（I de II）*
- *避免网上商店欺诈（二）*
- *如果...我不会在网上商店购买*
- *此页面可靠吗？*

1. 3. 4. 通过电子邮件诈骗

诈骗模式是利用分销给第三方国家的在线购物活动，买方通过电子邮件来和他们保持日常联系。

犯罪行为通过不同的机制（恶意软件，入侵等）访问商店与其分销商之间的消息流。诈骗者通过商业合法分销商的购物通道，在支付时控制购用户的银行账户或虚拟货币系统支付款项。

提示和建议

– 如果事先存在商业企图，则必须警惕其活动、提出的申请或不常见的请求。

1.3.5.针对工业和知识产权的犯罪行为

– 对于奢侈品或高端品牌，当价格远低于市场价格时，请不要信任他们，因为可能是假冒或被盗产品。

– 如果买方明知产品是假货或来源为非法的前提下进行购买，可能会招致法律判决。

– 应该格外注意那些私人注册的网址，例如请求电子邮件地址，SMS或类似的回复，提供免费下载或云端访问光盘、电影、系列、书籍和其他类似的产品，其可能是没有版权持有人授权的产品。

提示和建议

– 永远要在官方或值得信任的网页进行购买，而不会落入“超级便宜货”的陷阱。

– 如果有确凿的理由表明所购买的产品是伪造的，请向派出所报案。

– 建议向消费者保护组织或当局报告此类销售行为。

1. 3. 6. App欺诈或信誉质疑行为

移动设备是一个非常强大的工具，我们几乎生活上方方面面用到它：与其他人沟通，运动监控，获取位置，检查银行流水，或通过应用程序在线购物等等。 就像我们必须验证传统网站的安全性一样，对于要在网上进行购物的应用程序同样需要安全验证。

对于避免下载劣质App建议

- 需确认下载的是官方App，也就是说，它不是模仿正统App的山寨App。检查应用程序的开发者以及隐私政策是一个很好的习惯。
- 审查应用程序的权限，以控制在安装时会提出什么要求。您同时需要评估App所提出的要求与其功能是否合理匹配。
- 在安装或通过购买App前，检查已使用用户对本应用程序所做的评论和评估。
  它可以帮助您识别欺诈或信誉不好的应用程序。
- App下载数量同样可以说明问题。比如，一个很有名的App，但下载量很低，很有可能这个App不是官方正版，所以，要格外留意此类App的相关信息看是否可信。
- 避免总是从非官方的存储库下载应用程序，因为没有任何安全保证托管在那里的App，任何人都可以进行操纵。
- 阅读隐私，付款和安全政策。

更多信息请见:

Links
- *移动设备应用我们可以信任他们吗?*
- *应用程序和信息窃取*
- 为什么要避免需要许多权限才能使用的应用程序

1.3.7. 买卖服务或二手销售

近年来，出现了新的在线服务，促进了二手商品和产品的销售。 这些服务充当买方和卖方之间的中间人，允许卖方描述产品特征，销售价格以及合同结构。 虽然这些服务提供了许多优势，但它们也不能保证没有任何风险，所以您需要留意以避免购买产品中的欺诈行为。

一些建议

若您想进行消费：

- 在购买之前获得有关卖家的信息：按名称搜索，查看其他用户的评论和评级等。
- 删除包含出售物品照片的广告，或其措辞不注意，似乎是自动翻译或其描述不符合待售物品。
- 如果卖方在国外，并以此为借口来管理该程序以某种方式执行，那么请不要继续购买。
- 永远不要接受这种类型的购买服务，如西联汇款的支付方式或金钱克。
- 如有疑问，请取消购买流程。

若您想进行售卖：

- 在发货之前需询问买家是谁。
- 怀疑所提供的钱是否比广告要求的更多。
- 使用已知的付款方式，以保证购买是在我们的控制之下，而不是在买方的手中
- 不要预付款。 在一些骗局中，买方称您的银行不允许转账低于一定的金额，而这个金额恰好总是大于出售物品的价格。 其目的是试图欺骗卖方，以便通过西联汇款等服务来预付差额以补偿总成本。
- 如有疑问，请取消销售流程。

更多信息请见:

Links · 买卖交易服务

2. 1. 在线付款方式

用户在网上购物时最担心的一个问题就是使用的付款方式。 还有很多人不知道各种付款方式的优缺点。 因此，了解每种付款方式以及哪种选择具有更高的安全性非常重要。

接下来给大家讲一下经常使用的在线商务，以及每一种支付方式中消费者的权利以及它们所提供的安全性的相关知识。

2. 1. 1. 寄送现金

- 这种服务方式是通过转账，包含匿名转账，无法识别转账人以及接受人，因此，不应该被用于网上购物。

- **权利**：电子商务的一个主要方面，就是账户安全，是支付的手段之一。 如果网上交易商要求以现金支付，则应该放弃取消购买或合作。

- **安全**： 虽然这个系统不涉及买家和卖家之间的银行数据交换，但是由于没有记录谁发送或者接收到这个数据，在网上进行购买并不是一个安全的方法，所以它就没有可追踪性。 因此，如果购买出现问题（没有到货，有缺陷或不正确的产品），就很难索赔，特别是在遇到欺诈行为，因为不知道是谁接收到的钱。

2. 1. 2. 货到付款

- 这是邮寄包裹的一种方式，在收到包裹时付现金。

- **权利。**对于买方来说，当收到包裹时付款，是一种相当可靠的系统。然而，很多网上商店不提供这种方式，因为存在交货不付款的风险。另外，还存在交货时客户不在家时产生额外的运输费用。另一方面，对于客户来讲是不切实际的，特别是当现金成本很高的时候。

- **安全。**这是一种很安全的方式，在收到包裹时打开并检查正确后才付款。

2.1.3. 银行转账

- 这种支付方式允许将钱从一个账户转到另一个账户。跟其他付款方式比，它主要的优势就是不需要在网上填写任何资料。但是，不是所有的商店都提供这种付款方式。

- **权利。**如果店家没有交付所购买的商品或服务，您可以向供应商提出索赔，因为他们违反了合同。

- **安全。**卖家只需将银行账户的详细信息提供给买家，以便买房存入相应的金额。然而，还是存在风险的，特别是国际转账，因为资金一旦存入收款人账户，就很难追回。如果收款账户的户主不授权给银行退回，那么就要通过法律途径追回了。

2.1.4. 银行卡支付

- 这是一种网上商店最常用的付款方式。只需填写个人信用卡/借记卡信息。

- **权利。**交易的受益人可能不要求消费者支付使用卡的服务费

  当购物付款存在诈骗或非法使用银行卡支付时，消费者或此用户应当立即取消付款。在这种情况下，卖方和持卡人的账户中的相应的借记和分期付款记录将尽快更新。

  如果是持卡人操作，并且要求退款的理由不是行使自己的权利，那么买方将承担由于取消产生额外的费用。

  在使用银行卡支付续费服务时，应该告知用卡支付系统对于消费者来说保障性较低，并且在要求退期间的费用，取消卡支付更加复杂。

  安全。虽然涉及银行数据在线交换，但是网上商店使用银行提供的支付网关，可以成为非常安全的支付系统，可以验证银行卡的真实性和保护。这种方式，网上商店永远不会有客户的金融数据，从而给付款流程带来更大的安全性。如果网上商店不适用银行的支付网关，那么买方的银行保护数据将落入商店自己的安全机制。因此，如果对网站的可靠性有疑问，最好放弃购买，不要提供信用卡信息，以免使用不当。

  与此同时，如果可以，建议最好使用专门网上支付的银行卡，当我们不使用网上支付时，我们可以关闭
- 此项服务。

2.1.5. 使用第三方支付

- 使用第三方信用公司（例如PayPal）的付款方式来管理买方和卖方的银行数据，并负责正式支付款项。这样，卖方不需要知道买房的数据，反之亦然。**许多网上商店提供这项服务，因为它为用户提供了方便，不必在每次购物时输入他们的银行资料。**

- **权利。**在订阅这个支付系统之前，建议消费者和用户咨询服务的使用条款。

- **安全。**非常安全的支付系统，只要用户使用高级的密码来使用服务。 用户只需要拥有一个账户并连接他的信用卡。 当使用这种支付系统进行在线购买时，客户的财务数据不会被卖方处理，反之亦然，第三受信任的公司将负责与各方进行相应的管理，这提供了更高的安全性。

更多信息请见:

Links

- *如何创建安全密码?*
- *密码是否足够?*
- *哪种类型的在线支付适合我的需求?*
- *Paypal安全*
- *有关Visa验证的信息*
- *关于MasterCard 安全码的信息*

2.2. 设置账户

2.2.1. 安全密码

许多网上商店需要一个用户账号来配置某些参数，例如姓名，订单的送货地址，注册发票的地址，信用卡信息等。 为了保护对该信息的访问，所提供的就是密码。 该密码的强度将决定存储在用户帐户中的数据受到保护的多少，以免被入侵者或不需要的人员访问。 出于这个原因，使用安全密码并正确管理这些密码至关重要，为的时防止有人通过尝试不同的字母和数字组合来猜测或获得密码。

如何设置安全密码


_ 最少有8个字符，字母大小写、数字以及特殊字符的组合


-- 不要使用任何语言的可以从字典里方便找到的单词作为密码


– 谨慎使用与您有关的个人信息：专有名字，宠物的名字，标志性地点，生日或者其他特殊事件等等。


--- 避免使用由多个元素组成的密码。例如：“MARCO1978”（名字+生日）


-- 当然，也不要使用以下密码以及类似的密码：123456，123456789，qwerty，12345678，111111，1234567890，1234567，password，123123，987654321.

更多信息请见:

Links
- *为什么密码如此重要?*
- *如何生成强密码（视频）*
- *为什么不使用相同的密钥用于不同的服务（信息图）*
- *如何防止密码被盗*
- *如何使用密码管理器（视频）*
- *我想保护我的电子邮件*

2.2.2.激活两步验证或双重验证

有的时候，强密码并不能保证账号的安全。例如，如果电脑感染了病毒，或者智能手机或平板电脑安装了一些窃取用户密码的恶意应用程序。换句话说，无论在什么时候，用户在虚假借口下被欺骗的结果就是向网络犯罪分子提供某种服务的访问数据（典型的例子就是网络钓鱼）。

幸运的是，为了防止这些风险，许多在线服务和一些虚拟商店提供激活双重验证的选项。

什么是双重验证

- 在登录/注册过程中或正式购买过程中，向用户请求PIN，密码或附加密钥。
- 只可将验证密码告诉认识的人
- 只可通过您有的一种方式收到，例如您的手机。

更多信息请见:

Links
- *密码足够了吗?*
- *分两步验证，它是什么以及如何帮助我?*
- *为用户帐户添加一个额外的安全层*

2.2.3. 回复账户

用户可能忘记访问他想要处理购买的在线商店的个人帐户的密码。 在线服务允许用户通过各种机制重新获得对账户的控制权。 最常见的是使用电子邮件和安全问题恢复密码。

考虑到一些安全的问题是很重要的，这样这些恢复机制就不会被用户恶意使用，因为如果有人设法重新控制一个拥有注册财务数据的在线商店的帐户， 例如，在帐户所有者不知道的情况下购买，您将直接在银行帐户中看到扣款。

用户账户恢复的问题

通过电子邮件检索密码时：

- 您必须确保访问邮件的密码满足最低安全要求。
- 访问邮件的密码必须与在线商店的账户不同。 相同的密码不应该用于不同的服务
- 如果在线服务在您的配置中允许，请在注册过程中使用另一封电子邮件给员工进行密码恢复。

通过秘密问题恢复密码时：

- 通常你必须手动配置这个选项。 检查您要购买的在线商店是否具有此功能。
- 答案不应该基于真实的信息，虽然一般来说他们更容易记住，但是如果有人最低限度地，亲自地或者通过互联网上发布的信息知道这个人，那么猜测答案可能相对容易。
- 用户应该选择容易记住，并以安全的方式储存。 谨记，在通常情况下，他们是非常零散地使用，只有在密码丢失的情况下，需要记住或轻松恢复该数据。

2.2.4. 何时保存付款信息

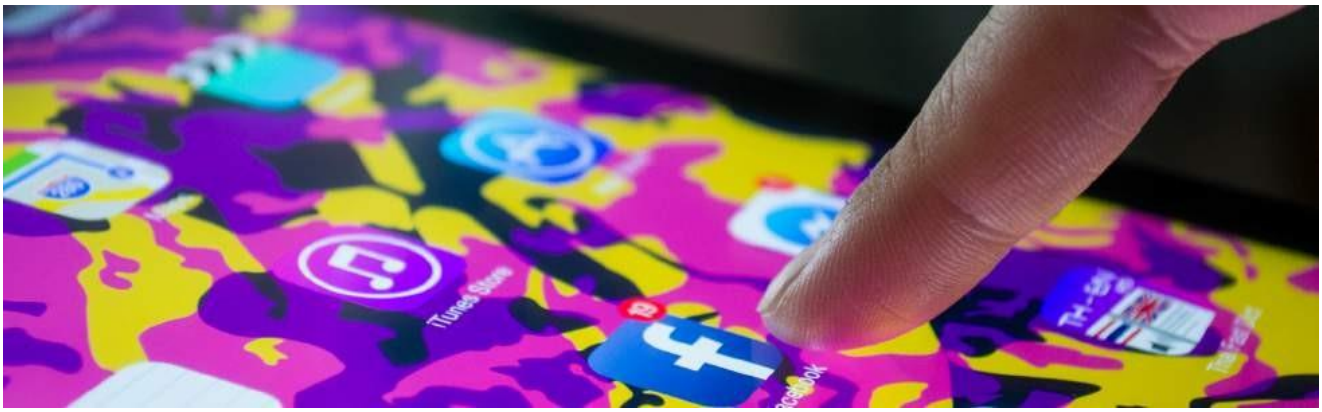
在网上购物之后，可能在用户账户中已经存储了诸如姓名，送货地址和账单，购买历史，电话号码等数据。 但也有关于使用的付款方式的信息，在大多数情况下是信用卡：卡的类型，号码，到期日期和CVV。 如果是这样的话，有必要评估将财务数据存储在账户中为了之后购买，反言之，最好删除它们。

使用账户的注意事项

如果在线商店的帐户在安全性（密码，双重验证）方面配置不正确，那么强烈建议不要保存银行账户信息。 特别是如果它是一个信用卡并且帐户有足够的钱付其他的费用。

最好在每次网上购物时重新输入银行资料，用户在进行在线购买时会有被其他人捕获密码的风险访问该账户并继续进行在线购买。

而且我们必须时刻记住，无论这些信息是否存储在用户帐户中，最后都必须在购买结束时关闭会话以防其他人进行访问。



2.2.5.通过应用程序购买的具体考虑事项

在通过应用程序在线购买时，重要的是还要考虑一些其他的预防措施，以防止任何人出于某种原因，可以进入设置网上购物的财政和银行信息的App非法进行购买。

通过手机应用程序购买额外的安全措施

- 设置一个最短的屏幕锁定时间，以限制对包括应用程序在内的功能的访问。 可以配置一个模式，PIN或密码是最安全的两种选择。

- 保护对特定应用程序的访问权限，以便没有人可以启动它们。 对于许多在线购物那样的应用程序来说，这是一个非常有趣的选项，它允许访问提供有关用户信息的服务，并且默认保存会话，并且每次他们不需要输入访问代码。 有些应用程序包含了这种安全措施，但对于那些不是这种情况的应用程序，可以安装一个“应用程序锁定器”，因为它们是已知的，可以提供此功能。

- 此外，建议配置设备以便在从应用程序存储库下载应用程序之前，无论是否付款都要输入PIN码。 通过这种方式，未经许可的人未经设备所有者的同意，就可以避免安装或使用应用程序。

3. 1. 实行取消的权利

消费者和使用者有权取消所签订的合同，并在确定的期限内通知另一方，无需为其决定作出解释，消费者和用户无需付额外款项.

消费者和使用者将有14个自然日的时间来行使这一权利，这将从合同中的收到货物时或，若不是寄出实际货物（比如某项服务）则从请求发出时开始计算。 如果用户没有被告知这项权利的存在，则该时间延长至十二个月。这项措施不应向消费者或用户索取任何费用。

在自其发生之日起14个自然日内，无论在任何情况下，当消费者和用户行使取消购买权时，网上商业将有义务退还其所支付的款项而不能扣留费用。

在线商业必须以清晰，可理解和准确的方式，以书面形式通知消费者这一权利及其行使的要求和后果，包括退还所收到商品或服务的方式。 还必须提供一份明确的使用取消权说明，写明收件人的姓名和地址，以及提及的合同和缔约方的相关信息。

无法执行撤回权的一些例外情况

特定日期的航空公司和火车票，音乐会门票，酒店和汽车租赁预订以及送餐服务。
通常送货上门食品和饮料（例如超市分销）。
对已经打开的音频，视频或计算机软件（例如DVD）进行密封的定制或定制项目（量身定制的套装等）。
在线数字内容，如果下载或实时播放已经开始。
从个人购买而不是从公司购买的产品。
一旦价格达成一致，保修和紧急维修工作的服务合同。

更多信息请见:

Links
- *消费者权利*
- *消费者冲突解决方案*

3. 2. 保修

通过网上商店购买的产品将受到消费品销售保修制度的约束。

不论购买渠道是什么，购买新产品的保修期限为两年。两年保修是最基本的权利；国家法律有可能提供时间更长的保修时间。

消费者有权享有的担保既适用于新产品，也适用于二手产品，但后者有一些特殊性，既买卖双方之间协议保修的最长期限为一年。无论任何一种情况，消费者有权获得没有质量问题的优质产品。

对消费者提供的维修和更换是完全免费的。 包括更换有缺陷的货物，特别是在合理的时间内进行的运输费用以及与劳动和材料有关的费用。 只要产品滞留在卖方的技术人员手中（制造商方），则保修时间计算将不被计算在内。

3.3. 有缺陷的产品：运输和转运支出

有缺陷的产品是：考虑到所有可能发生的情况下，不能在合理预期内提供其安全性，尤其是其介绍、使用情况和出厂时间。

供货商将对产品在生产或进口过程中造成的损害负责。

根据欧盟的规定，如果所购买的产品有缺陷或对所宣称的特征（包括价格，所用税和交货成本）不符，消费者可以选择：

- 货物的修理
- 其更换
- 降价
- 退还合同已付款项，除非要求退还不合乎常理的款项，原则上不合理的情况是指强制商家缴付的，较之前的可能性相比，无理的请求。
- 含退还款项的合同决议，除非其中一个是不可能的或不相称的。 原则上，对卖方的成本加以衡量是不相称的，与其他可能性相比，是不合理的。

3.4. 个人信息的权利

在网上商店进行联系，购买或订购后，会保留已经提供的个人资料，并可能默认已获得您同意来处理信息。

即使我们的个人信息在电子商务的计算机系统里，ARCO权利使我们能够对其数据进行操控。

权利的行使必须出自本人或其法定代表人。

14岁以下未成年人若要履行权利必须由法定代理人行使。 “数据保护组织法”草案规定年龄为13岁。

如果在请求行使这些权利时没有得到网上商店的回应，或者对其答复不满意，用户可以向西班牙数据保护局提出控诉。

访问权

- 允许用户了解在线商店掌握的其个人资料情况并有权访问它。

- 在线商家从接收数据，或者从生成拒绝请求起必须在一个月内回复请求。

纠正权

- 允许纠正错误，修改错误或缺失信息，并确保网上商家所持有的信息是准确无误的。例如，更新发票地址或联系电话。
- 网上商家应收到申请后的10天内进行回复。

撤销或清除权

- 允许删除不合理或多余的信息。
- 删除权将其信息封锁，因此网上商家无法对这些信息进行任何操作。

- 在可能需要承担法律责任期间，网上商家将保存公共管理，法官和法院的数据副本。 一旦过了这段时间必须将其删除。

- 在线商家需在收到申请后的10日内做出回应。

- 与在线商店保持合同关系所必需的数据在购物行为仍然存在时不能被取消，例如订阅付款服务。

反对权

- 允许申请并获得继续处理或停止处理数据的权利。一个很常见的例子就是让网上商家停止以广告目的处理个人数据。
- 网上交易必须在收到通知后的10日内回复，排除处理消费者信息或矢口否认消费者提出的请求的情况。

2018年5月25日在这些权利基础上，又加上三条

处理限制权

- 通过这一权利，消费者可以申请，在交易中行使个人数据纠正权的时，停止在线商店对数据的处理。
- 若您需要使用您的个人信息来执行某法律行为，或若网上商家违法处理您的个人信息，您可以申请停止删除您的个人信息。在处理数据暂停期间，在消费者同意的情况下数据只能用于储存，或公共利益目的项目。

数据可移植性的权利

- 允许用户获得涉及他们个人数据的副本，并且促进了在线商务，以便能够将其传输，被用于另一项服务。
- 如果技术上可实现的情况，用户有权让在线商店将他们的个人数据用于所指定的服务，并且商家必须执行此操作。

拒绝个人决定自动化的权利

- 在线商务的用户有权拒绝自动化行使个人权利的行为，例如，通过拟定购买属性时使用此权利，它有着至关重要的影响。
- 在线商务可以根据与用户有关的合同或法律明确允许的情况下做出这样的决定。 您也可以请求用户同意采取此决定。 在这种情况下，利害关系方可以拒绝授权他来作此类决定。

更多信息请见:

Links

- *LOPD权利*
- *新法规适用时，我有什么权利?*
- *保护权利的索赔*

3.5. 保密义务和数据发布

网上贸易以及以其名义收集或处理个人资料的任何人都有职业保密义务。 即使在与他的商业或合同关系结束之后，这一义务仍在存在。

任何情况下，网上商店的访问者和客户的个人数据都不得在未经其同意的情况下被公布。在互联网上公布数据并开放访问，这触犯了目前的法律并可能遭到AEPD起诉。

提出申诉:

- *在网上AEPD进行申诉*

3.6. 安全性措施和安全风险提示

网上商店有义务采取技术措施或管理方法来保证用户安全。 从2018年5月25日起，将颁布“通用数据保护条例”，存在安全漏洞，影响其用户个人资料的网上商家:

_ 您必须在72小时内通知西班牙数据保护局，详细说明漏洞细节和采取或提出的纠正及预防措施。

_ 在安全漏洞可能对用户造成高风险的情况下，网上商家必须告知:

- 数据保护代表处的详细联系信息
- 安全漏洞的后果
- 为降低不利影响并防止新的漏洞而采取或提出的相关措施

3. 7. 广告

在线商家可以将商业信息发送给被授权的客户和访问者。

但是，当您联系、购买或与在线商店签订合同时，商家必须向用户提供拒绝接收广告的选择。

以电子方式进行的商业通讯必须遵守一般广告法规，其中包括禁止进行误导性广告，广告需可被辨认以及禁止发送可信度低的广告。 同样，它也必须符合适用于推广产品或服务的具体广告规定。 如果在线商店提供您有关产品或服务的促销信息，则必须说明适用于此促销活动的相关条件。如果您举办比赛或抽奖活动，您必须使用户方便的看到活动规则。

请记住，您可以免费自愿通过广告系统拒绝在不需要的广告中输入您的信息。 目前只有一个名为*罗宾逊名单*的文件，是由西班牙数字经济协会（ADIGITAL）进行管理的。

通过注册罗宾逊名单，您可以选择不希望接收的宣传媒介或渠道（邮寄、联系电话、电子邮件或其他方式）。

若您想了解更多信息:

Links

如何避免不需要的广告?

4. 如何申诉

如果最终认定违反了某种规定，那么可以通过以下途径申诉：

在处理消费者投诉时，这个问题的主管机构在国家或地区管辖范围内，在违反消费者和使用者的一般防卫规则的情况下采取行动（见“消费冲突解决办法”）。

也可以通过附属于西班牙消费者事务，食品安全与营养机构（AECOSAN）的欧洲消费者中心，在总部对其他欧盟成员国的公司进行干预 -CEC由欧盟委员会创建。 该网络包括挪威和冰岛，提供有关在欧洲国家购买商品或使用服务的信息或协助，这些信息或协助与居住地不同。

如果是处理关于保护个人资料的申诉，主管部门是西班牙数据保护局（AEPD）。 可以通过其电子方式向总部提交。 在提供很多证据的情况下，处理更为敏捷。

但是，当我们通过电子手段获得远程的服务时，作为消费者和用户的权利的保护受到提供这些商品或服务的地点的限制。 因此，我们要知道什么时候可以去西班牙欧洲当局，我们必须考虑到以下几点：

至2018年5月24日

- 如果商人在西班牙成立，或者在西班牙境内的企业在其活动范围内要处理个人资料，则西班牙法律适用。任何关于数据保护的声明必须在AEPD之前提出。

- 如果商人在西班牙没有设立机构，但是在欧盟的另一个成员国设立，那么他所在的成员国的立法适用于他所指定的公司的活动。 在这些情况下，有关数据保护的声明可以向成员国的数据保护机构提交（清单在本指南的末尾），或与AEPD一起提交给主管当局。

- 如果商家在西班牙或欧盟的任何其他成员国都没有设立机构，商家使用他的报价，并且与位于我国的潜在西班牙买家的关系，那么AEPD只能在数据保护方面采取行动。 例如，当您在西班牙居民的终端设备（如电脑，平板电脑，智能手机等）上安装存储和数据恢复设备（通常称为cookie）时。

从2018年5月25日起

- 如果商家在欧盟有营业机构，或者没有在欧盟境内设立，他向欧盟消费者提供商品或服务时，指南中指出的内容是有效的。 关于数据保护的声明可以提交给AEPD，AEPD将提供给他们适当的课程。

--- 最后，就属于犯罪的行为而言，其调查和起诉对应于各自的安全部队，财政部和相应的司法机构。

5. 安全网购的10个基本建议

- **1.** 在值得信任的网上页面进行购物
- **2.** 确保可以识别网上商店的负责人及其位置
- **3.** 检查网上商店是否安全，并要求提供有关个人消费数据和处理所需的所有信息
- **4.** 如果可以，使用专用卡进行在线支付
- **5.** 不要相信过于吸引人的优惠，因为您可能会在欺诈性网站里面
- **6.** 在提供您的个人数据或付款信息之前，请不要忘记检查您的设备配置是否正确以及互联网连接是否安全
- **7.** 不要用现金完成在线购买。 请仔细选择付款方式。
- **8.** 请记住有信任的图标商家会提供更大的保证
- **9.** 您可以在14天内无理由取消购买或取消合同。
- **10.** 如果您取消或使用保修，他们不应该像您收取任何费用，包括运输成本。

当局网络安全，消费和数据保护

欧洲网络安全机构和实体

- 欧洲刑警组织 EUROPOL
- 由欧洲网络认证的信息安全事件响应中心 TF-CSIRT *Centros de Respuesta ante Incidentes de Seguridad de la Información acreditados por la red europea*
  TF-CSIRT. Trusted Indroducer.
- 欧盟网络和信息安全局 *European Union Agency for Network and Information Security* (ENISA)

国家网络安全机构和实体

- 国家警察 - 技术研究大队 *Policía Nacional - Brigada de Investigación Tecnológica* (BIT)
- 民警卫队 - 远程信息处理犯罪组织 *Guardia Civil - Grupo de Delitos Telemáticos* (GDT)
- 国家重点基础设施保护中心 *Centro Nacional de Protección de Infraestructuras Críticas* (CNPIC)
- 国家网络安全研究所 *Instituto Nacional de Ciberseguridad* (INCIBE) y 安全和行业事件响应中心 *el CERT de Seguridad e Industria* (CERTSI)
- 国家密码中心 *Centro Criptológico Nacional* (CCN-CERT)

欧洲消费者当局

- 欧洲替代性纠纷解决机构 *Organismo europeos para la Resolución alternativa de litigios* (RAL)

欧洲数据保护机构

- 西班牙
https://www.agpd.es
- 奥地利
http://www.dsb.gv.at
- 比利时
http://www.privacycommission.be
- 保加利亚
http://www.cpdp.bg
- 克罗地亚
http://www.azop.hr
- 塞浦路斯
http://www.dataprotection.gov.cy
- 捷克共和国
http://www.uoou.cz
- 丹麦
http://www.datatilsynet.dk
- 爱沙尼亚
http://www.aki.ee/en
- 芬兰
http://www.tietosuoja.fi/en
- 法国
http://www.cnil.fr
- 德国
http://www.bfdi.bund.de
- 希腊
http://www.dpa.gr
- 匈牙利
http://www.naih.hu
- 爱尔兰

http://www.dataprotection.ie

· 意大利
http://www.garanteprivacy.it
· 拉脱维亚
http://www.dvi.gov.lv
· 立陶宛
http://www.ada.lt
卢森堡
http://www.cnpd.lu
· 马耳他
http://www.dataprotection.gov.mt
· 荷兰
https://autoriteitpersoonsgegevens.nl
· 波兰
http://www.giodo.gov.pl
· 葡萄牙
http://www.cnpd.pt
· 罗马尼亚
http://www.dataprotection.ro
· 斯洛伐克
http://www.dataprotection.gov.sk
· 斯洛文尼亚
https://www.ip-rs.si
· 瑞典
http://www.datainspektionen.se
· 英国
https://ico.org.uk

欧洲机构

· 欧洲数据保护主管
http://www.edps.europa.eu

安全网购

实用指南


AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
aecosan
Policía Nacional