数据泄露事件

****Instagram**** 4900万条数据曝光，影响人数达数百万

影响人数：4900万条记录

泄露目标：Instagram用户

泄露内容：用户资料、图片、粉丝数据、以及验证过的国家/地区、私人联系信息（包括电话、电子邮件等），甚至还有用户已删除信息内容。

事件经过: 据TechCrunch网站报道，Instagram的一个大型数据库由于在AWS存储桶上没有受到保护，导致任何人都可以在没有身份验证的情况下访问它。该数据库首先由安全研究人员Anurag Sen发现，并立即报告给了TechCrunch网站。

该数据库包含从有影响力的Instagram帐户中抓取的公共数据，包括其个人资料，个人资料图片，关注者数量，如果经过验证，则具有按城市和国家/地区划分的位置，私人联系信息，电子邮件的地址和电话号码Instagram帐户所有者。数据库中的每个记录还包含一个计算每个帐户价值的字段。档案中的影响者名单包括著名的美食博客，名人和其他社交媒体影响者。

****优衣库**** 遭到黑客攻击，超过46万用户数据泄漏

影响人数：46万用户

泄露目标：用户

大致时间：2019年5月

泄露内容：个人信息、电子邮件、地址以及部分信用卡资料

事件经过：日本最大的服装零售商迅销集团发布消息称，旗下优衣库以及GU品牌的在线商城遭到黑客攻击，约46万用户的数据泄漏，包括用户个人信息、电子邮件、地址以及部分信用卡资料等。迅销称，此事件仅限于日本网站，发生在4月23日至5月10日期间，是一次基于列表的攻击。当客户在多个网站上使用相同的用户名和密码组合时，可能会遭受此类攻击，建议用户更改密码。

**Facebook** 再被指泄漏用户数据，至少5.4亿用户资料任由下载

影响人数：至少5.4亿名用户

泄露目标：Facebook 用户

大致时间：2019年4月

事件经过：据《彭博社》报导，网络保安公司 UpGuard 在亚马逊云端数据库上发现大量 Facebook 用户的个人资料，涉及至少5.4亿名用户，且数据开放予任何人下载。报导指出，墨西哥城媒体公司 Cultura Colectiva 的数据库储存了5.4亿名 Facebook 用户的个人资料，包括身份证号码、帐号称谓、网上评论及回应记录等。Cultura Colectiva 专门发布拉丁美洲娱乐及文化消息，在 Facebook、Instagram、Twitter、YouTube 等开设专页，拥有逾4500万用户追踪。《彭博社》向 Facebook 查询，Facebook 随后通报亚马逊，相关数据库已被封锁。Facebook 发言人表示，公司政策禁止将用户资料储存于公开数据库，此次发现事件后即时通知亚马逊处理；发言人称，公司致力与平台开发商合作保障用户私隐。

****华硕**** 内网密码在 GitHub 上泄露

泄露内容：企业内网密码

事件经过：北京时间3月28日早间消息，据美国科技媒体TechCrunch报道，一名信息安全研究员两个月前向华硕发出警告称，有华硕员工在GitHub代码库中错误地发布了密码。这些密码可以被用于访问该公司的企业内网。其中一个密码出现在一名员工分享的代码库中。通过该密码，研究员可以访问内部开发者和工程师使用的电子邮件帐号，从而与计算机的使用者分享夜间构建的应用、驱动和工具。有问题的代码库来自华硕的一名工程师，他将电子邮件帐号密码公开已有至少一年时间。目前，尽管GitHub帐号仍然存在，但这个代码库已被清理。

个人对于数据泄露的防范

1. **设置复杂的密码**

建议用户可采用“大小写+数字+特殊符号”这样的形式来设置账户密码。需要注意的是，众多账户尽可能不要使用同一个密码。

**2、 定期更改密码**

定期修改密码，会增加账户的安全度，3个月更改一次密码最佳。

**3、 不要轻易出售个人信息**

目前很多平台或APP为了拉动新用户注册率，会以各种优惠的活动吸引用户，诱导用户进行注册甚至是信息绑定，当有APP或平台需要获得你的各项信息权限的时候，可千万要注意了，别薅羊毛不成反被羊咬。

**日常生活中的防范网络诈骗的方法**

不点击短信、邮件中的陌生链接，

不登录陌生网站，定期为电脑查杀病毒，木马；

智能手机安装杀毒软件；

保留有关单据、信息记录，发生利益受损情况时，用法律手段维权；

不轻易相信“订单处理异常”等反馈，不下载来历不明的手机应用；

密码使用不涉及自己姓名、生日等信息，定期修改密码。