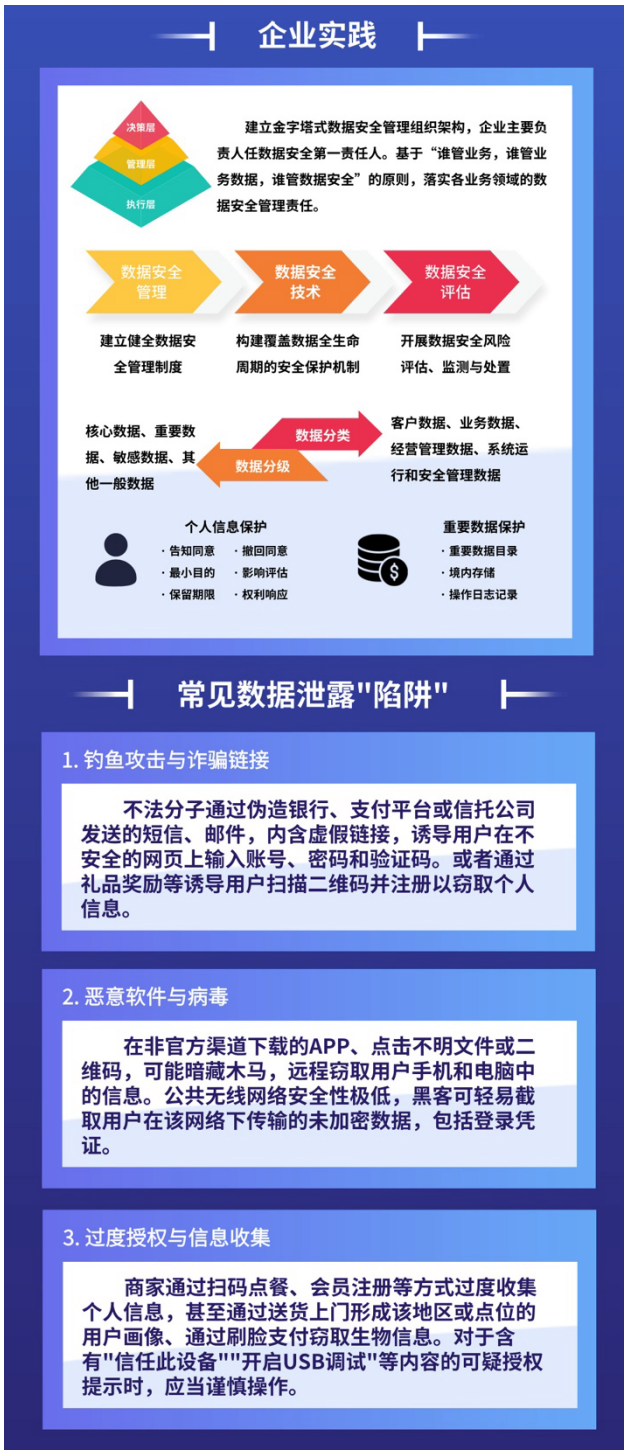
宝马汽车金融(中国)有限公司

守护数据安全，防范金融风险


企业实践
决策层
管理层
执行层
建立金字塔式数据安全管理组织架构，企业主要负责人任数据安全第一责任人。基于“谁管业务，谁管业务数据，谁管数据安全”的原则，落实各业务领域的数据安全管理责任。
数据安全管理
数据安全技术
数据安全评估
建立健全数据安全管理制度
构建覆盖数据全生命周期的安全保护机制
开展数据安全风险评估、监测与处置
核心数据、重要数据、敏感数据、其他一般数据
数据分类
数据分级
客户数据、业务数据、经营管理数据、系统运行和安全管理数据
个人信息保护
· 告知同意 · 撤回同意
· 最小目的 · 影响评估
· 保留期限 · 权利响应
重要数据保护
· 重要数据目录
· 境内存储
· 操作日志记录
常见数据泄露"陷阱"
1. 钓鱼攻击与诈骗链接
不法分子通过伪造银行、支付平台或信托公司发送的短信、邮件，内含虚假链接，诱导用户在不安全的网页上输入账号、密码和验证码。或者通过礼品奖励等诱导用户扫描二维码并注册以窃取个人信息。
2. 恶意软件与病毒
在非官方渠道下载的APP、点击不明文件或二维码，可能暗藏木马，远程窃取用户手机和电脑中的信息。公共无线网络安全性极低，黑客可轻易截取用户在该网络下传输的未加密数据，包括登录凭证。
3. 过度授权与信息收集
商家通过扫码点餐、会员注册等方式过度收集个人信息，甚至通过送货上门形成该地区或点位的用户画像、通过刷脸支付窃取生物信息。对于含有"信任此设备""开启USB调试"等内容的可疑授权提示时，应当谨慎操作。

实用防护建议

1. 强化信息保护意识

- 不向他人透露个人金融信息和财产状况，为金融账户设置高强度、无规律密码；
- 不透露自己收到的短信验证码，不轻信不明电话、短信和邮件；
- 不点击来历不明的短信、邮件、社交群中的链接和附件。

2. 认准官方渠道

- 通过官方应用下载App，扫描通过正规渠道发布的二维码；
- 尽量使用个人数据网络进行支付，避免在公共电脑上或连接公共网络进行网络交易；
- 启用电脑防火墙，定期查杀电脑病毒、及时为操作系统和各类应用软件安装官方发布的安全补丁。

3. 加强日常信息管理

- 妥善处理包含个人信息的单据，不得随意丢弃业务单据或凭证；
- 亲自办理金融业务，保管好个人身份证件、银行卡、银行账户等，不转借他人使用；
- 在社交媒体和朋友圈避免过度泄露个人身份信息、金融信息等敏感信息。

4. 审慎授权

在授权应用程序、小程序、网站权限时，仔细阅读授权协议，看清楚系统弹窗请求的权限内容，仅授予必要权限，及时解除不必要的授权。同时，关注金融机构发送的风险提示等。

紧急应对措施

一旦发现个人金融信息泄露迹象，要果断处置：

1.立即联系金融机构采取冻结账户(或卡)，修改密码、留存证据等措施；
2.及时联系公安机关报案，通过法律途径维权；
3.关注自身信用记录，若因诈骗导致个人信息被冒用产生不良信用，及时与相关机构沟通，采取措施消除影响。

数据安全不仅需要金融机构的努力，更需要每位金融消费者的参与。定期修改密码、谨慎授权应用、关注账户异常情况等简单的安全习惯，可能就是阻止数据泄露的最后屏障。