# 安全使用网上银行的八条温馨小提示

## 1 定期监控账户

确保所有的交易都由本人亲自授权。如果发现任何可疑的欺诈活动，请立即向银行报告

## 2 警惕奇怪的电子邮件！

如果您收到声称是银行（或其他公司）发出的电子邮件，并要求您提供帐户详细信息或密码，请千万不要回复。**银行不会通过电子邮件索取个人用户的帐户信息**

## 3 不要点击电子邮件中的链接

请尽量手动登录网上银行，以确保您所进入网站的安全性

## 4 定期更改银行密码

不要在多个网站使用相同的密码，并确保选择一个包含大小写字母、数字和特殊字符的高强度密码。不要使用包含个人姓名、首字母或出生日期的任何词语或短语

## 5 启用双重身份验证

多数金融机构为账户持有人提供额外的安全保护——双重身份验证，即要求用户在登录帐户之前进行额外验证

## 6 禁用自动登录

禁止网络浏览器保存网上银行的登录用户名和密码

## 7 尽量使用银行的官方APP

确保从可靠来源（如Apple Store或Google Play Store）下载APP

## 8 不确定某个事件是否合法?

对网银技术存在疑问？请致电工作人员，他们将乐意帮助您！

**信息由以下机构合作提供:**

THE STATE OF TEXAS DEPARTMENT OF BANKING

TexasBankers Association

# 加强网络安全的八条温馨小提示

## 1 电子邮件欺诈

如果邮件内容好得令人难以置信，比如说告诉您“中大奖了”或“外国王子联系您”，那很可能就是欺诈，千万不要相信！

## 2 欺诈性支付

如果您收到支票、本票、汇票或电子资金转账后，要求您退还部分金额，请谨慎处理，很可能是欺诈

## 3 主动提供的优惠

若收到“超值惊喜，欲购从速”等信息，要谨慎对待

## 4 保持更新

确保设备的操作系统（如Windows、Apple IOS、手机IOS（Apple、Android等））的安全设置更新到最新版本

## 5 警告和错误提示

不要相信弹出警告或错误提示的网站

## 6 小心电子邮件的附件

谨防点击来自未知来源的电邮附件或免费软件，否则可能面临在线欺诈和盗窃的风险

## 7 在线分享

注意在网上分享的内容。您在社交网站上发布的个人信息越多，就越有可能会有人利用这些信息来访问您的帐户、窃取您的身份。您需要通过加强隐私设置来保护个人信息

## 8 金融诈骗

注意与灾害事件相关的金融诈骗。骗子可能声称自己来自合法的慈善组织，在灾害事件后骗取人们的信任，而实际上是为了窃取金钱或有价值的个人信息

**更多有关在线安全的资源：**

**Texas Department of Banking – www.dob.texas.gov**
**Texas Bankers Association – www.texasbankers.com/BankingSafely**
**Better Business Bureau – www.bbb.org/council/for-businesses/cybersecurity/**