

# **Personal Finance & Cyber-Fraud Prevention Guidelines**

To safeguard your finances and reduce the risk of cyber fraud, adopt these best practices.

## **1. Strong Authentication**

- Use strong, unique passwords for all financial accounts.
- Enable multi-factor authentication wherever possible.
- Change passwords regularly and avoid reusing them.

## **2. Secure Online Banking**

- Access banking services only through official websites or apps.
- Avoid using public Wi-Fi for financial transactions.
- Log out after each banking session.

## **3. Monitoring and Alerts**

- Check bank and credit card statements frequently.
- Set up alerts for unusual transactions.
- Report suspicious activity immediately to your bank.

## **4. Safe Payment Practices**

- Use credit cards or secure payment services for online shopping.
- Do not share card details via email or phone.
- Verify seller credibility before making payments.

## **5. Protection from Phishing and Scams**

- Be cautious of emails or messages requesting personal data.
- Avoid clicking on suspicious links or downloading unknown attachments.
- Confirm any unusual request with the source directly.

## **6. Data Privacy**

- Store sensitive documents in encrypted or secure locations.
- Shred physical documents containing financial information.
- Limit sharing of personal financial details on social networks.

## **7. Emergency Preparedness**

- Maintain an updated list of bank and credit card contacts.
- Have a financial recovery plan for potential fraud incidents.
- Consider insurance or identity theft protection services.

These habits help protect your financial stability and guard against cyber threats.

## 个人理财与网络诈骗防范指南

为保护财务安全并降低网络诈骗风险，请遵循以下最佳实践。

### 1. 强身份认证

- 为所有金融账户使用强而独特的密码。
- 尽可能启用多因素认证。
- 定期更换密码并避免重复使用。

### 2. 安全网上银行

- 仅通过官方网站或官方应用访问银行服务。
- 避免在公共 Wi-Fi 下进行金融交易。
- 每次银行操作后都要退出登录。

### 3. 监控与提醒

- 经常检查银行和信用卡账单。
- 启用异常交易提醒。
- 发现可疑交易立即通知银行。

### 4. 安全支付

- 网上购物时使用信用卡或安全支付平台。
- 不要通过邮件或电话分享卡片信息。
- 在付款前核实卖家信誉。

### 5. 防范钓鱼与诈骗

- 谨慎对待索取个人信息的邮件或消息。
- 避免点击可疑链接或下载未知附件。
- 直接向来源确认异常请求。

### 6. 数据隐私

- 将敏感文件加密或存放在安全位置。
- 粉碎含有金融信息的纸质文件。
- 限制在社交网络上分享个人财务细节。

### 7. 应急准备

- 保留最新的银行和信用卡联系方式。
- 制定财务应急恢复计划。
- 考虑购买保险或身份盗用防护服务。

**遵守这些习惯可有效保障财务安全并防范网络威胁。**

व्यक्तिगत वित्त और साइबर धोखाधड़ी रोकथाम दिशानिर्देश

अपने वित्त की सुरक्षा और साइबर धोखाधड़ी के जोखिम को कम करने के लिए इन सर्वोत्तम प्रथाओं का पालन करें।

**1. मजबूत प्रमाणीकरण**

- सभी वित्तीय खातों के लिए मजबूत और अद्वितीय पासवर्ड का उपयोग करें।
- जहां संभव हो बहु-कारक प्रमाणीकरण सक्षम करें।
- पासवर्ड को नियमित रूप से बदलें और दोबारा उपयोग से बचें।

**2. सुरक्षित ऑनलाइन बैंकिंग**

- केवल आधिकारिक वेबसाइटों या ऐप्स के माध्यम से बैंकिंग सेवाओं का उपयोग करें।
- सार्वजनिक वाई-फाई पर वित्तीय लेनदेन से बचें।
- प्रत्येक सत्र के बाद लॉग आउट करें।

**3. निगरानी और अलर्ट**

- बैंक और क्रेडिट कार्ड विवरण बार-बार जांचें।
- असामान्य लेनदेन के लिए अलर्ट सेट करें।
- संदिग्ध गतिविधि की तुरंत बैंक को रिपोर्ट करें।

**4. सुरक्षित भुगतान**

- ऑनलाइन खरीदारी के लिए क्रेडिट कार्ड या सुरक्षित भुगतान सेवाओं का उपयोग करें।
- ईमेल या फोन पर कार्ड विवरण साझा न करें।
- भुगतान से पहले विक्रेता की विश्वसनीयता सत्यापित करें।

**5. फ़िशिंग और धोखाधड़ी से सुरक्षा**

- व्यक्तिगत जानकारी मांगने वाले ईमेल या संदेशों से सावधान रहें।
- संदिग्ध लिंक पर क्लिक करने या अज्ञात फ़ाइल डाउनलोड करने से बचें।
- किसी भी असामान्य अनुरोध की सीधे पुष्टि करें।

**6. डेटा गोपनीयता**

- संवेदनशील दस्तावेजों को एन्क्रिप्टेड या सुरक्षित स्थानों में रखें।
- वित्तीय जानकारी वाले कागज़ी दस्तावेज़ नष्ट करें।
- सोशल मीडिया पर व्यक्तिगत वित्तीय विवरण साझा करने से बचें।

**7. आपातकालीन तैयारी**

- बैंक और क्रेडिट कार्ड संपर्कों की अद्यतन सूची रखें।
- संभावित धोखाधड़ी के लिए वित्तीय पुनर्प्राप्ति योजना तैयार करें।
- बीमा या पहचान चोरी सुरक्षा सेवाओं पर विचार करें।

इन आदतों से वित्तीय स्थिरता और साइबर खतरों से सुरक्षा में मदद मिलती है।

# Guía de Finanzas Personales y Prevención de Fraudes Cibernéticos

Para proteger sus finanzas y reducir el riesgo de fraude en línea, siga estas buenas prácticas.

## 1. Autenticación Segura

- Utilice contraseñas fuertes y únicas para cada cuenta financiera.
- Active la autenticación multifactor cuando sea posible.
- Cambie las contraseñas con regularidad y no las reutilice.

## 2. Banca en Línea Segura

- Acceda a los servicios bancarios solo a través de sitios o aplicaciones oficiales.
- Evite usar Wi-Fi público para transacciones financieras.
- Cierre la sesión después de cada operación bancaria.

## 3. Monitoreo y Alertas

- Revise con frecuencia los estados de cuenta bancarios y de tarjetas.
- Configure alertas para movimientos inusuales.
- Informe de inmediato cualquier actividad sospechosa a su banco.

## 4. Pagos Seguros

- Use tarjetas de crédito o servicios de pago seguros para compras en línea.
- No comparta los datos de su tarjeta por correo electrónico o teléfono.
- Verifique la confiabilidad del vendedor antes de pagar.

## 5. Protección contra Phishing y Estafas

- Sea precavido con correos o mensajes que pidan datos personales.
- No haga clic en enlaces sospechosos ni descargue archivos desconocidos.
- Confirme directamente cualquier solicitud extraña.

## 6. Privacidad de Datos

- Guarde documentos sensibles en lugares cifrados o seguros.
- Destruya los documentos físicos con información financiera.
- Limite la publicación de detalles financieros en redes sociales.

## 7. Preparación para Emergencias

- Mantenga una lista actualizada de contactos bancarios y de tarjetas.
- Establezca un plan de recuperación financiera ante fraudes.
- Considere seguros o servicios de protección de identidad.

**Estas prácticas protegen su estabilidad financiera y reducen los riesgos de fraude en línea.**

## Guide de Finances Personnelles et de Prévention de la Fraude en Ligne

*Pour protéger vos finances et réduire les risques de fraude en ligne, suivez ces bonnes pratiques.*

### 1. Authentification Sécurisée

- Utilisez des mots de passe forts et uniques pour chaque compte financier.
- Activez l'authentification multifactorielle si possible.
- Changez régulièrement vos mots de passe et ne les réutilisez pas.

### 2. Banque en Ligne Sécurisée

- Accédez uniquement aux services bancaires via des sites ou applications officiels.
- Évitez le Wi-Fi public pour les transactions financières.
- Déconnectez-vous après chaque session.

### 3. Surveillance et Alertes

- Vérifiez fréquemment vos relevés bancaires et de cartes.
- Configurez des alertes pour toute transaction inhabituelle.
- Signalez immédiatement toute activité suspecte à votre banque.

### 4. Paiements Sécurisés

- Utilisez des cartes de crédit ou des services de paiement sécurisés.
- Ne partagez jamais les informations de carte par e-mail ou téléphone.
- Vérifiez la fiabilité du vendeur avant tout paiement.

### 5. Protection contre le Phishing et les Arnaques

- Soyez prudent avec les e-mails ou messages demandant des données personnelles.
- Ne cliquez pas sur des liens suspects et n'ouvrez pas de pièces jointes inconnues.
- Confirmez directement toute demande inhabituelle.

### 6. Confidentialité des Données

- Conservez les documents sensibles dans des emplacements chiffrés ou sécurisés.
- Détruisez les documents papier contenant des informations financières.
- Limitez le partage d'informations financières sur les réseaux sociaux.

### 7. Préparation aux Urgences

- Tenez une liste à jour des contacts bancaires et de cartes.
- Élaborez un plan de récupération en cas de fraude.
- Envisagez une assurance ou un service de protection d'identité.

CES MESURES RENFORCENT LA SÉCURITÉ FINANCIÈRE ET PROTÈGENT CONTRE LA FRAUDE EN LIGNE.

# إرشادات الإدارة المالية الشخصية ومنع الاحتيال الإلكتروني

لحماية أموالك وتقليل مخاطر الاحتيال عبر الإنترنت، اتبع هذه الممارسات المثلى.

## 1. مصادقة قوية

- استخدم كلمات مرور قوية وفريدة لكل حساب مالي -
- فعّل المصادقة متعددة العوامل كلما أمكن -
- غيّر كلمات المرور بانتظام وتجنب إعادة استخدامها -

## 2. الخدمات المصرفية عبر الإنترنت الآمنة

- استخدم فقط المواقع أو التطبيقات الرسمية للوصول إلى الخدمات المصرفية -
- العامة للمعاملات المالية Wi-Fi تجنب استخدام شبكات -
- سجّل الخروج بعد كل جلسة مصرفية -

## 3. المراقبة والتنبيهات

- راجع بيانات الحسابات المصرفية وبطاقات الائتمان بانتظام -
- قم بإعداد تنبيهات للمعاملات غير المعتادة -
- أبلغ البنك فورًا عن أي نشاط مريب -

## 4. ممارسات دفع آمنة

- استخدم بطاقات الائتمان أو خدمات الدفع الآمنة للتسوق عبر الإنترنت -
- لا تشارك بيانات البطاقة عبر البريد الإلكتروني أو الهاتف -
- تحقق من موثوقية البائع قبل الدفع -

## 5. الحماية من التصيد والاحتيال

- احذر الرسائل أو البريد الإلكتروني التي تطلب بيانات شخصية -
- لا تنقر على الروابط المشبوهة أو تفتح مرفقات غير معروفة -
- تأكد مباشرة من أي طلب غير معتاد مع الجهة المرسل -

## 6. خصوصية البيانات

- خزّن المستندات الحساسة في أماكن مشفرة أو آمنة -
- أُلّف المستندات الورقية التي تحتوي على معلومات مالية -
- قلل من مشاركة تفاصيلك المالية على الشبكات الاجتماعية -

## 7. الاستعداد للطوارئ

- احتفظ بقائمة محدثة لجهات الاتصال المصرفية وبطاقات الائتمان -
- ضع خطة للتعافي المالي في حالة الاحتيال -
- فكر في الحصول على تأمين أو خدمة حماية الهوية -

اتباع هذه الإرشادات يحمي استقرارك المالي ويقلل من مخاطر الاحتيال الإلكتروني.