

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.



# व्यक्तिगत वित्त और साइबर धोखाधड़ी रोकथाम दिशानिर्देश

**W**

**Ã**

**1.    Ã**

-  
-                   -       Ã       W       A  
:       A                               }

**2.    W**

-  
-       "       -  
-   Ã       ¾

**3.**

-       -   A   A       -  
-                               "  
:       W                               "

**4.    W**

-                               -   A   A       W  
-                               A  
-                               -

**5.**

-                               W  
-                               X       A       A  
-

## **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.

## 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 فوراً 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 المرسله.

### 6. خصوصية البيانات

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

### 7. الاستعداد