



مكافحة الاحتيال والتوعية بالمخاطر الإلكترونية

فرنسبك سورية

Version: 1.0

Date: 5-12-2025



أولاً: التزام المصرف

يلتزم مصرف فرنسبك سورية بما يلي:

- تطبيق ضوابط رقابية وتقنية لرصد ومنع محاولات الاحتيال.
- حماية القنوات المصرفية الإلكترونية من الاستغلال غير المشروع.
- الاستجابة الفورية لحوادث الاحتيال والإبلاغ عنها أصولاً.
- نشر التوعية المستمرة للموظفين والعملاء حول أساليب الاحتيال.

ثانياً: إرشادات الموظفين

على جميع الموظفين الالتزام بما يلي:

1. التقيد الكامل بسياسات وإجراءات مكافحة الاحتيال المعتمدة.
2. التحقق من هوية العملاء وعدم تجاوز إجراءات التدقيق لأي سبب.
3. عدم طلب أو مشاركة أي معلومات سرية (كلمات مرور – رموز تحقق).
4. عدم التعامل مع أي طلب غير رسمي أو خارج القنوات المعتمدة.
5. الإبلاغ الفوري عن أي حالة مشتبها بها أو محاولة احتيال.
6. المشاركة الإلزامية في برامج التوعية والتدريب ذات الصلة.

ثالثاً: إرشادات العملاء

يهيب المصرف بعملائه الالتزام بما يلي:

- عدم مشاركة الرقم السري أو رمز التحقق (OTP) أو بيانات البطاقة.
- عدم الضغط على أي روابط غير موثوقة.
- استخدام تطبيق المصرف والموقع الرسمي فقط.
- تحديث التطبيق بشكل دوري.
- الإبلاغ فوراً عن أي عملية أو رسالة أو اتصال مشبوه.

رابعاً: أمثلة شائعة لأساليب الاحتيال

1. رسائل نصية (SMS)

- رسالة تدّعي إيقاف الحساب وتطلب تحديث البيانات.
- رسالة تحتوي على رابط شبيه بموقع المصرف.
- رسالة تطلب إدخال رمز التحقق لأسباب "طارئة".
- ⚠️ **تنبيه:** المصرف لا يطلب أي بيانات سرية عبر الرسائل النصية.

2. مكالمات هاتفية

- اتصال يدّعي أنه من موظف المصرف أو جهة رقابية.
- طلب معلومات البطاقة أو الرمز السري بحجة حل مشكلة.
- تهديد بإيقاف الحساب في حال عدم التعاون.
- ⚠️ **تنبيه:** المصرف لا يطلب معلومات سرية عبر الهاتف.

3. روابط ومواقع مزيفة

- مواقع مشابهة لواجهة المصرف مع اختلاف بسيط في الرابط.
- روابط تُرسل عبر WhatsApp أو Telegram أو البريد الإلكتروني.
- صفحات تطلب إدخال اسم المستخدم وكلمة المرور.
- ⚠️ **تنبيه:** يجب التأكد دائماً من الرابط الرسمي للمصرف.

خامساً: الإبلاغ عن الاحتيال

في حال الاشتباه بأي عملية احتيال، يرجى الإبلاغ فوراً عبر:

- مركز خدمة العملاء
- أقرب فرع
- القنوات الرسمية المعتمدة لدى المصرف