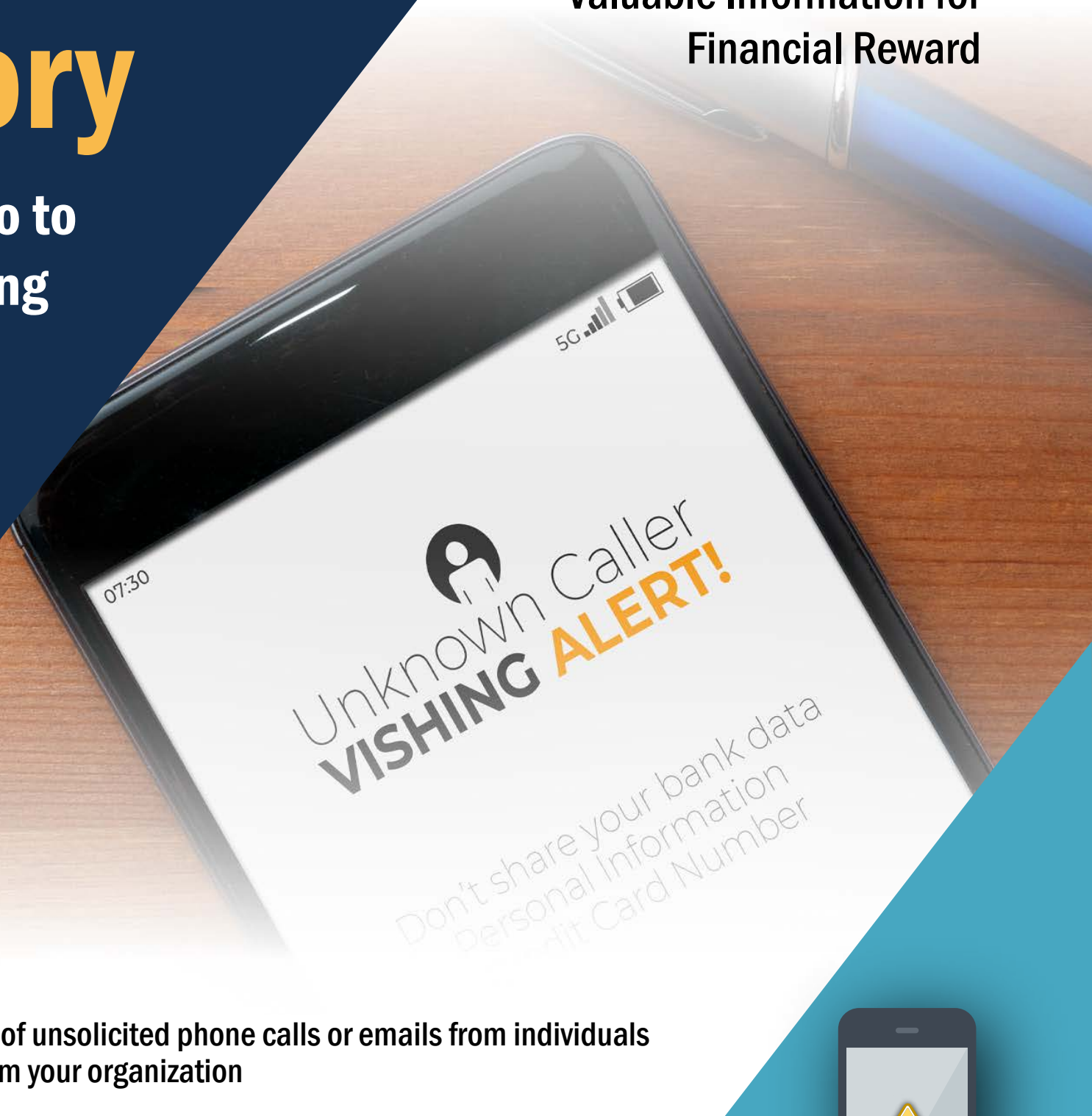
Vishing Threat Advisory

What You Can Do to Prevent Becoming a Victim

According to the FBI, **Vishing**, or Phone Phishing, is a Form of Criminal Phone Fraud using Social Engineering Over the Phone to Gain Access to Valuable Information for Financial Reward



TIPS

- Verify the identity of unsolicited phone calls or emails from individuals claiming to be from your organization
- Never share sensitive information, Personally Identifiable Information (PII), or Protected Health information (PHI) over the phone
- Only use your government furnished equipment (GFE) and always connect to a VPN
- Review and update your privacy settings on any personal or professional online accounts
- Limit the amount of information you share publicly, especially on social media
- Report security incidents to your Computer Security Incident Response Team (CSIRT); you may also contact the FBI's 24/7 Cyber Watch at cywatch@fbi.gov

Vishers can use Technology to Impersonate the Voices of their Victims

See Tips on what you can do to PREVENT yourself from becoming a victim