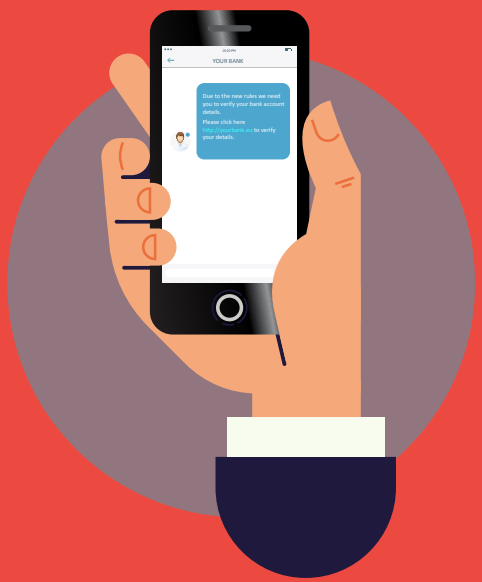
BANK PHISHING SMS

Smishing (eine Kombination der Wörter SMS und Phishing) ist der Versuch von Betrügern, persönliche, finanzielle oder sicherheitsrelevante Informationen mittels Textnachricht zu erlangen.



WIE FUNKTIONIERT ES?

Die Textnachricht wird Sie typischerweise auffordern, einen Link anzuklicken oder eine Telefonnummer anzurufen, um ihr Konto zu 'prüfen', 'aktualisieren' oder 'reaktivieren'. Aber...der Link führt zu einer gefälschten Webseite und die Telefonnummer zu einem Betrüger, der vorgibt das echte Unternehmen zu sein.

WAS KÖNNEN SIE TUN?

- **Klicken Sie nicht auf Links, Anhänge oder Bilder,** die Sie in unerbetenen Textnachrichten erhalten, ohne vorher den Absender zu überprüfen.
- **Keine Hast.** Nehmen Sie sich Zeit, die notwendigen Überprüfungen vorzunehmen, bevor Sie antworten.
- **Beantworten Sie nie Textnachrichten,** die die Eingabe Ihrer PIN, Ihres E-Banking Passwortes oder anderer Sicherheitsmerkmale verlangt.
- Wenn Sie vermuten, dass Sie einen Smishing-Text beantwortet und Ihre Bankdaten preisgegeben haben, **kontaktieren Sie sofort Ihre Bank.**

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG Ministry of the Economy
ABBL
SECURITY MADE IN.LU
BEE SECURE