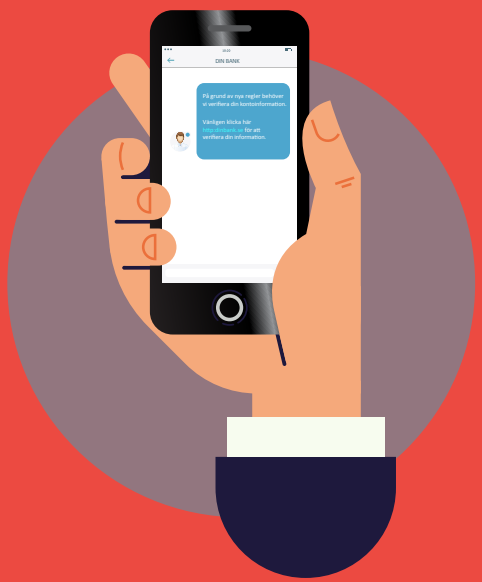
FALSKA SMS

Smishing (sms phising – kombination av orden SMS och falska e-postmeddelanden) innebär att bedragaren vis sms försöker få tillgång till personlig-, finansiell- eller säkerhetsinformation.



HUR GÅR DET TILL?

Textmeddelandet uppmanar oftast mottagaren att klicka på en länk för att "verifiera", "uppdatera" eller "återaktivera" sitt konto. Men istället leder länken till en falsk webbplats. Där uppmanas man lämna ut BankID eller kortuppgifter.

VAD KAN DU GÖRA?

- **Klicka inte på länkar,** bilagor eller bilder som du får i oönskade textmeddelanden utan att först verifiera avsändaren.
- Stressa inte. Ta dig tid att göra lämpliga kontroller innan du svarar avsändaren.
- **Svara aldrig på ett textmeddelande som begär din PIN-kod eller dina lösenordsuppgifter**.
- Om du misstänker att du svarat på ett smishing-textmeddelande och uppgett dina bankuppgifter, **kontakta din bank omedelbart.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | Polisen

#CyberScams