

# PÉNZÜGYI ADATHALÁSZ SMS-ek

A "smishing" (az SMS és a phishing szó kombinációja) azt jelenti, hogy a csalók személyes, pénzügyi vagy biztonsági információkat kérnek szöveges üzenetben.



## HOGYAN TÖRTÉNIK?

A csaló SMS-ek arra kérnek, hogy a benne lévő linkre kattintva, vagy telefonszám felhívásával 'hitelesítse', 'frissítse' vagy 'újra aktiválja' a bankszámláját. De... a link egy hamis weboldalra irányít, a telefonszámot pedig csalók használják, akik úgy tesznek, mintha egy törvényesen működő cég ügyintézői lennének.

## MIT TEHET?

- **Ne kattintson a linkre, mellékletre vagy képre**, amit a kéréstelen üzenetek tartalmaznak, csak miután ellenőrizte a feladót!
- **Ne kapkodjon!** Szánjon rá időt és ellenőrizze az üzenetet, mielőtt válaszol!
- **Soha ne válaszoljon olyan szöveges üzenetekre**, amiben PIN kódot, online banki jelszót vagy más bizalmas adatot kérnek!
- Ha úgy érzi csaló üzenetre válaszolt és megadta banki adatait, **azonnal értesítse a bankot!**