FALSKA BANK E-POSTMEDDELANDE

Phishing är bedrägliga e-postmeddelanden som lurar mottagarna att dela med sig av sina personliga, ekonomiska eller säkerhetsinformation.

HUR GÅR DET TILL?

De här e-postmeddelandena:

ser ut som de meddelandena som banken brukar skicka ut.

innehåller logga och layout som är förvillande lika bankens egna.

ber att du laddar ned ett bifogat dokument eller klickar på en länk.

försöker förmå dig att agera fort.

VAD KAN DU GÖRA?

- **Håll din mjukvara uppdaterad**, såsom din webbläsare antivirusprogram och operativsystem.
- Var särskilt **vaksam** på om "bank" e-postmeddelanden ber dig om känslig information (tex. lösenordet till din internetbank).
- **Titta noga på e-postmeddelandet**: se upp för felstavningar och konstig grammatik.
- **Svara inte på ett misstänkt e-postmeddelande**, utan kontrollera med din bank att de är avsändare.
- **Klicka inte på länkar** eller ladda ner bifogade filer i e-postmeddelanden.
- Om du är tveksam **dubbelkolla** med banken.

Bedragarna utnyttjar att människor är stressade; då är det lätt att uppfatta e-postmeddelandena som äkta vid ett snabbt ögonkast.

#CyberScams

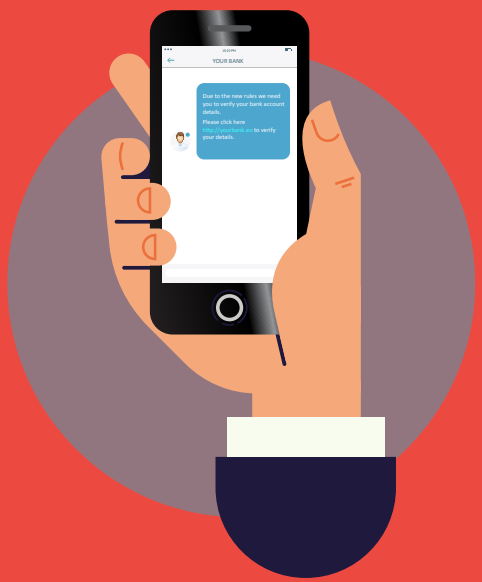
EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Polisen

FALSKA BANK SMS

Smishing (en kombination av orden SMS och Phishing) är att bedragaren försöker lura av dig personlig, finansiell eller säkerhetsinformation via sms.



HUR GÅR DET TILL?

Textmeddelandet kommer vanligtvis att be dig att klicka på en länk för att "verifiera", "uppdatera" eller "återaktivera" ditt konto. Men ... länken leder till en falsk webbplats där du vilseleds att lämna 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.
- **Aldrig svara på ett textmeddelande** som begär din PIN-kod eller dina lösenordsuppgifter.
- Om du tror att du kanske har svarat på en smishing-text och angett dina bankuppgifter, **kontakta din bank omedelbart**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Polisen

#CyberScams

FALSKA BANK SAMTAL

Vishing (en kombination av telefonsamtal och Phishing) är en telefonbluff där bedragare försöker lura offret för att avslöja personlig, finansiell eller säkerhetsinformation.

VAD KAN DU GÖRA?

- **Tänk på** att telefonsamtal kan komma från en bedragare.
- Motring till banken på ett telefonnummer som du säkert vet går dit.
- För att validera deras identitet, **kolla upp organisationens telefonnummer** och kontakta dem direkt.
- **Validera inte den som ringer med det telefonnummer de har gett dig** (det kan vara ett falskt nummer).
- Bedragare kan hitta information om dig på nätet. **Anta inte att en uppringare är äkta** bara för att de har personliga uppgifter om dig.
- **Lämna inte ut** bank-kortinformation eller ditt lösenord till internetbanken. Din bank skulle aldrig begära ut dessa uppgifter.
- **Banken skulle aldrig ringa** och begära att du överför pengar till annans konto.
- Om du misstänker att du är utsatt för vishing, **rapportera det till din bank.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

Polisen

#CyberScams