SENIORERNA
Östgötadistriktet

Med anledning av en våg av falska mail där man I bland ber om att snabbt skicka pengar för att snabbt lösa en påhittad situation kommer här ett dokument som beskriver det vanligaste tillvägagångssätten.

Varning: Phishingmail

Detta dokument syftar till att varna för phishingmail och ge vägledning om hur man känner igen och undviker dem.

Vad är phishing?

Phishing är försök att lura dig att lämna ifrån dig känslig information, såsom lösenord, bankuppgifter, skicka pengar eller personliga data.

Tecken på phishingmail

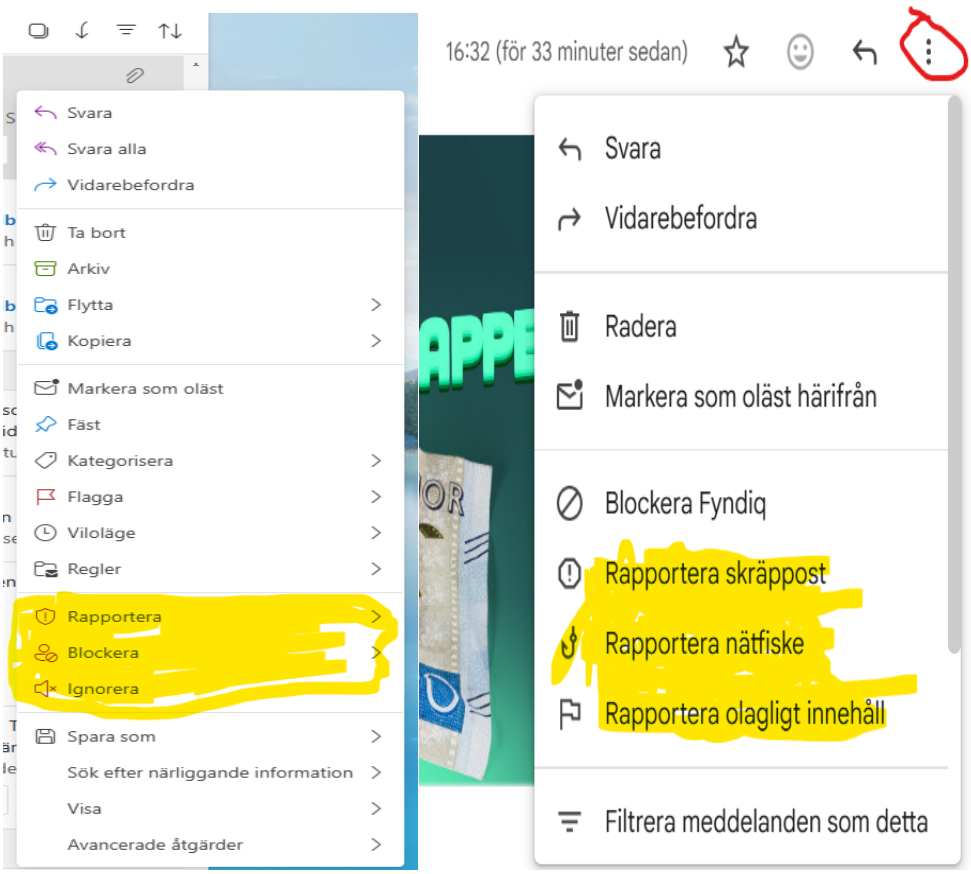
- Oväntade eller okända avsändare
- Stavfel och grammatiska fel i meddelandet
- Uppmaningar att "agera snabbt" eller hot om konsekvenser (ekonomiska)
- Länkar som inte går till en legitim webbplats
- Bilagor du inte förväntade dig

Så skyddar du dig

- Klicka inte på misstänkta länkar
- Öppna inte okända bilagor
- Kontrollera alltid avsändaradressen noga
- Använd tvåfaktorsautentisering när det är möjligt
- Rapportera phishingförsök till din epostleverantör. (Google Mail, Outlook, mm) Se nedan exempel på rapportering!

Exempel på tvåfaktorsautentisering (2FA)

- Engångskod via SMS: Du får en kod skickad till din mobiltelefon som du måste ange vid inloggning.
- Autentiseringsappar: Appar som Microsoft Authenticator eller Google Authenticator genererar tidsbegränsade engångskoder.
- Push-notiser: Du får en notis i en autentiseringsapp där du godkänner eller avvisar inloggningen.
- Fysiska säkerhetsnycklar: USB- eller NFC-enheter som YubiKey som kräver fysisk närvaro för inloggning.
- Biometrisk autentisering: Fingeravtryck eller ansiktsigenkänning som Windows Hello eller FaceID.
- Engångskod via e-post: En kod skickas till din e-postadress som en andra verifieringsfaktor.
- Smartcard-certifikat: Fysiska kort med certifikat som kräver PIN-kod, vanligt i företag.



Outlook, man högerklickar med musen på mailet. Välj Rapportera.
Google Mail: öppna mailet, klicka på de tre inringade prickarna. Välj Rapportera nätfiske.
Följ sedan det som kommer om rapportering.