

SEPTEMBER 1, 2025

NR 10, 2025

Skellefteå Strokeförening

E-post
skelleftea@strokeforening.se**www.strokeforening.se**

Påminner om caféträffarnas uppstart för hösten

Den 4 september är det dags för den första caféträffen för hösten 2025. Vi träffas på Stora Coop Söder, Anderstorp i Skellefteå. kl. 14.00- ca 15.30

Surströmmings festen 19 september

Vi skickar ut en separat inbjudan kring hur ni anmäler er och vad det kommer att kosta för dig som medlem och vad det kostar för ej medlemmar.

Det förekommer bedrägeriförsök kring falska e-postmeddelanden och sms som utger sig för att komma från föreningen

En av föreningen okänd person har försökt få ut pengar genom att utge sig för att vara en medlem av styrelsen.

Föreningen vill härmed varna sina medlemmar. Med några råd från Polisen kring Vishing och Phising. Källa: <https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/>

Så skyddar du dig mot telefonbedrägeri även kallat vishing

1.) Lägg på luren

Om någon ringer upp dig och du blir osäker ska du avsluta samtalet. Det gäller oavsett om personen säger sig vara en släkting eller någon från din bank, ett företag eller en myndighet.

Förbered något du kan säga för att avsluta samtalet snabbt, eller lägg på direkt. Du behöver inte vara artig.

2.) Logga inte in

Identifiera dig aldrig med bank-id och lämna aldrig ut koder från din bankdosa eller till ditt betalkort om någon frågar efter det.

Seriösa företag, organisationer och myndigheter tar aldrig kontakt och ber dig logga in eller lämna ut personliga uppgifter på det sättet.

3.) Lita inte på den som ringer

Bedragaren kan försöka stressa dig genom att säga att du är på väg att förlora pengar eller att någon anhörig har råkat illa ut.

Lita inte på personen som ringer även om den verkar trovärdig och har personlig information om dig.

Så skyddar du dig mot nätfiske, även kallat phishing

1.) Lämna aldrig ut kortuppgifter eller personliga uppgifter.

2.) Var misstänksam om du får mejl eller sms när du uppmanas klicka på en länk och lämna känsliga uppgifter, som koder och personuppgifter. Följ aldrig sådana instruktioner. Inga banker eller seriösa företag skickar sådana meddelanden. Är du osäker, ring din bank eller företaget.

3.) Ha unika lösenord för dina viktigaste tjänster, som din mejl, banken och e-legitimationen.

4.) Godkänn aldrig att någon fjärrstyr din dator eller telefon.

Rapportera misstänkta bluff-sms till 7726

Har du fått ett misstänkt bluff-sms? Vidarebefordra meddelandet till 7726. Siffrorna motsvarar ordet SPAM på knappsatsen i telefonen och är globalt etablerat för att rapportera bluff-sms.

Det är ett operatörsberoende nummer som alla kan använda. På så sätt får teleoperatörerna veta vilka bluff-sms du får.

Du kan hjälpa till att sprida brottsförebyggande råd

Du kan hjälpa till att sprida brottsförebyggande råd till personer i din närhet. Prata med en mamma, en mormor, en granne eller kompis. Tillsammans kan vi stå emot bedragarna.

Vid tangentbordet denna gång: Camilla Stenmark kassör i föreningen