Vanligaste tillvägagångssätten i Sthlms län nu under sommaren.
De två översta vanligast förekommande i Huddinge just nu.
Flera äldre i 85-98 årsåldern blivit drabbade senaste veckan av fysisk vishing

SMS från ”barn” – OM du får ett SMS där ditt barn uppger att de har ny telefon och bytt nummer, ring alltid och dubbelkolla till det nummer du har sedan tidigare
– swisha aldrig pengar till ett nytt nummer du inte har kontrollerat vem det går till!

Fysisk vishing. Ringer upp från Telia/ Media Mark/ Elgiganten etc, någon ska ha beställt varor i ditt namn och de erbjuder sig att hjälpa till då de förstår att du blivit utsatt för ett bedrägeri.
”Securitas” hämtar kort och ibland även smycken för att förvara dem på säker plats åt dig.
Eller
Säger att de ringer från din bank eller från polisen, att du blivit utsatt för ett bedrägeri och att de måste få ditt bankkort och koder för att kunna hjälpa dig. En person från ”banken” kommer och hämtar dina saker och de tömmer sen snabbt ditt konto.
- Inget seriöst företag eller bank kommer ringa dig och komma och hämta kontokort, koder, smycken eller andra värdesaker!

Postnord, en person påstår sig ringa från Postnord om en påstådd beställning. Därefter slussas du vidare till säkerhetsavdelning eller bank för identifiering med bank-id. I vissa fall har en person även kommit hem till den utsatta personen för att hämta upp kort. I andra fall har bedrägeriet enbart skett via telefon
– Identifiera dig aldrig med BankID när någon ringer upp dig, enbart om du själv ringer en bank/myndighet på ett nummer som du själv har tagit fram!

Modus vårdcentral/sjukhus. GM uppger sig för att ringa från sjukhus/ vårdcentral och erbjuder bla covid-vaccin. Därefter vill personen att du ska identifiera sig med bank-id eller bankdosa. Under tiden har de förberett transaktioner på stora summor från ditt konto som du godkänner med ditt BankID
– Använd ALDRIG Mobilt BankID eller bankdosa på uppdrag av någon som ringer upp dig!!

Sms från elektronikföretag som du ska ha gjort en beställning från, vilket du inte har gjort. Om man undrar något så ska man ringa ett mobilnummer. Måste sedan identifiera sig med Bank-ID.
– Använd ALDRIG Mobilt BankID eller bankdosa på uppdrag av någon

Kapade Snapchatkonton. Kontaktad av en vän vars konto blivit hackat som ber om hjälp med en snabb swishbetalning (5000-6500 kronor), tex en ”Blocketaffär” då vännens bank/swish ligger nere.
– Ring alltid din vän och dubbelkolla först!

Byta bankdosa. Ringer från banken och uppger att målsägandens bankdosa behöver uppdateras/bytas ut och uppmanar målsäganden att logga in med bankdosan och skriva in kontrollkoder och på detta sätt lyckas med överföringar
– Banken ringer ALDRIG upp och ber dig logga in. Kontakta din bank på ett nummer du känner till om du är osäker!

Fysisk vishing. Ringer upp från Telia/ Media Mark/ Elgiganten etc, någon beställt varor i ditt namn och de erbjuder sig att hjälpa till då de förstår att du blivit utsatt för ett bedrägeri. ”Securitas” hämtar kort och ibland även smycken för att förvara dem på säker plats åt dig.
– Inget seriöst företag kommer ringa dig och komma och hämta

- Inget seriöst företag kommer ringa dig och komma och hämta bankkort, koder, smycken eller andra värdesaker!

Mejl från mobilföretag. En faktura har betalats två gånger och en återbetalning ska göras till dig. Du uppmanas följa en länk, fylla i dina uppgifter och legitimera dig med bank-id.
- Använd ALDRIG Mobilt BankID eller bankdosa på uppdrag av någon som ringer upp dig, oavsett ärende!

Olika former av investeringsbedrägerier. Målsäganden kan komma i kontakt med uppringande personer på olika sätt, *bla annonser på Facebook, kapade Instagram- och Facebook-konton* där ”vännen” skriver att denna lyckats så bra och tipsar om hur man kan göra detsamma.