Aktuella bedrägerimodus som i hög grad drabbar äldre medborgare i Lokalpolisområde Skärholmen

- **SMS från närstående** - Fortsatt stort inflöde av anmälningar gällande SMS från barn, både fullbordade och försök.

- **Postnord** – GM påstår sig ringa från Postnord om en påstådd beställning. Därefter slussas MÄ vidare till säkerhetsavdelning eller bank för identifiera sig med bank-id. I vissa fall har en annan GM kommit hem till MÄ för att hämta upp kort. I andra fall har bedrägeriet enbart skett via telefon.

- **Polis - modus**. Målsägande uppgav att hon fått ett samtal där det var en inspelad engelsk röst som uppgav att det var polisen. De sa hennes personnummer och att hon blivit ID--kapad. Den inspelade rösten bad henne sedan trycka 1 för att komma i kontakt med operatör på polisen.

- **Modus vårdcentral/sjukhus -** GM uppger sig för att ringa från sjukhus/ vårdcentral och erbjuder bl.a. covid-vaccin. Därefter vill GM att MÄ ska identifiera sig med bank-id eller bankdosa. GM har i flera fall lyckats förmå MÄ att föra över hundratusentals kronor.

- **Sms från elektronikföretag** - Om att MÄ gjort en beställning, vilket denne inte gjort. Om man undrar något så ska man ringa ett mobilnummer, måste sedan identifiera sig med bank-id.

- **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.

- **Fysisk vishing -** Ringer upp från Telia/Media Markt/Elgiganten, någon beställt varor, ”hjälper målsägande”, ”Securitas” eller ”polis” hämtar kort och ibland smycken. Man kan exempelvis få hjälp att lägga smycken i ett bankfack. I ett fall har målsägande via instruktioner gått till Tavex Smålandsgatan Stockholm och köpt guldtackor, därefter tagit en taxi till Kista centrum och där gjort ett bankomatuttag för att sedan möta upp en person och överlämna detta. Allt enligt instruktioner från den uppringande kvinnan (i det här fallet) som målsäganden hade kontakt med under hela händelseförloppet.

- **Mejl från mobilföretag** - En faktura betalats två gånger och en återbetalning ska göras. Uppmanas följa en länk, fylla i sina uppgifter och legitimera sig med bank-id.

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

- **Alektum/Svea inkasso ringer** - Meddelar att någon köpt en dator i MÄ företags namn och att man troligen blivit drabbad av bedrägeri, kopplar till banken och målsäganden för identifiera sig med bank-id. Bedragaren kommer i en del fall åt målsägandens företagskonton och stora belopp kan överföras

- **Annons Facebookgrupp -** Målsägande svarar på en annons via messenger, blir uppringd och upplyst om att en bakgrundskontroll (UC) behöver göras. Blir uppmanad att logga in med bank-id. Senare upptäcker målsäganden att antingen pengar försvunnit från kontot eller att en beställning av mobiltelefoner gjorts.