Gør din hverdag mere sikker

Et undervisningsmateriale til ældre borgere

Undervisningsvejledning

Udviklet af LCIK, Nordjyllands Politi og Midt- og Vestjyllands Politi

Velkommen

Den fysiske verden er ikke det eneste sted hvor ældre borgere færdes i dag. En del af hverdagen foregår for mange ældre også i den digitale verden. Det gør dem sårbare på nye og uvante måder.

Og det gør dig og dit møde med de ældre vigtigt. Du kan gøre en stor forskel ved at tale med de ældre om at de skal sikre sig i både den fysiske og den digitale verden.

I tillæg til at tale om de typiske temaer – indbrud og tricktyveri – lægger undervisningsmaterialet derfor også op til dialog om stærke adgangskoder der skal sikre de ældres "digitale hjem", fuphenvendelser på mail eller sms og fupopkald.

Undervisningsmaterialet skal gøre det nemmere at forstå den digitale verden. Derfor bruger vi paralleller til den fysiske verden til at fortælle om it-kriminalitet og sikkerhed, fx sammenligner vi adgangskoder med husnøgler.

Vi taler – ganske enkelt – om *hverdagen*, og hvordan den ældre selv kan gøre netop *hverdagen* mere sikker.

Du skal derfor heller ikke være ekspert i it-sikkerhed for at bruge materialet eller gennemføre oplægget.

Materialet giver mulighed for tryghedsskabende dialog med de ældre i centrum. Formålet er at vise de ældre at de selv kan gøre noget for at øge deres sikkerhed i hverdagen – både fysisk og digitalt. Det gør vi med dialog og udvalgte råd om, hvordan de kan gøre hverdagen mere sikker.

Den primære målgruppe er borgere i alderen 65+, men du er også velkommen til at bruge materialet til andre borgergrupper. Materialet kan bruges hvis fx foreninger, organisationer eller grupper af borgere ønsker at få politiet ud og fortælle om kriminalitet og hvad man som borger selv kan gøre. Materialet kan også bruges som et aktivt tilbud, hvis I i politikredsen selv igangsætter en forebyggende indsats hvor I vil nå borgere gennem undervisning.

Materialet er udviklet af LCIK, Nordjyllands Politi og Midt- og Vestjyllands Politi. Illustrationer er udarbejdet af Tanke-streger v/ Mette Jepsen.

Denne vejledning indeholder detaljerede instruktioner til materialet.

Vil du have mere information, er du velkommen til at kontakte LCIK eller din kreds' tovholder.

Rigtig god fornøjelse.

Hvordan skal undervisningsmaterialet bruges?

Undervisningsmaterialet skal få ældre borgere til at dele erfaringer og give dem viden om hvordan de kan gøre deres hverdag mere sikker – både i den fysiske og den digitale verden.

Materialet består af en præsentation med to overordnede temaer 1) Indbrud og 2) Snyd og bedrag. De to temaer fletter kriminalitet fra den fysiske og digitale verden sammen.

Der er vedlagt to korte film som du selv skal sætte ind i PowerPoint-præsentationen. Korrekt indsat fremstår de som sorte billeder, og du skal blot klikke på dem for at afspille filmene. Tjek at højtalere og lyd virker inden dit oplæg. Filmene er en vigtig del af oplægget, og vi anbefaler at du ser dem igennem flere gange, så du kan fortælle, hvad der sker hvis lyden skulle drille.

Hvert kapitel i præsentationen indeholder overordnet tre elementer:

- Introduktion til temaet med film, illustrationer eller eksempler fra virkeligheden.
- Dialog
- Gode råd

Din rolle er at præsentere de ældre for materialet og få dem til at dele deres egne erfaringer og idéer til at gøre hverdagen mere sikker. Husk derfor at aftale med deltagerne at personlige oplevelser deles i fortrolighed. Afhængigt af publikumsstørrelsen vil du kunne skabe mere eller mindre dialog.

Dit udgangspunkt er at fortælle om en sikker *hverdag* – ikke kompleks information om it-sikkerhed eller tekniske detaljer om indbrudssikring. Det vigtigste er at formidle tre overordnede budskaber:

1) Vælg en stærk lås både til din bolig og dit digitale hjem. Gør det svært at bryde ind.

2) Opbevar penge, koder og personlige oplysninger med omtanke. De er som underbukser og skal ikke ligge og flyde men holdes tæt til kroppen eller gemmes godt væk.

3) Du er ikke forpligtet til at tale med fremmede. Vær skeptisk ved uopfordrede henvendelser: stop kontakten, tænk dig om og tag evt. selv kontakt efterfølgende.

Undervisningsmaterialet består af:

Vigtigt: Al materiale til undervisningen er samlet på et USB-stik. Dette stik skal medbringes til undervisningen sammen med en internet-pc til visning af præsentationen. Brug IKKE din personlige arbejdscomputer og rediger IKKE i indholdet på stikket. Du risikerer at filmene ikke kan afspilles og at din kollega ikke kan bruge materialet efterfølgende. Kontakt LCIK hvis stikket er bortkommet.

POWERPOINT-PRÆSENTATION

Præsentationen vises under dit oplæg. Det er vigtigt at du viser præsentationen fra det tildelte USB-stik sammen med en internet-pc. Ellers kan filmene ikke afspilles.

HANDOUT OG PLAKAT

På USB-stikket finder du også et handout med en opsummering af de bedste råd. Dem kan du printe og dele ud til deltagerne efter mødet. Print på begge sider så der bliver en forside og en bagside. Handoutet kan også printes i A3 format og hænges op som plakat under oplægget.

TALEKORT

Talekortene kan bruges under oplægget og indeholder de vigtigste budskaber og forslag til spørgsmål til de ældre der kan skabe dialog. Medbring et print af talekortene. Har du brug for at tilpasse dem, skal du gemme og redigere dem på din egen computer og ikke USB-stikket.

EKSTRA SLIDES

Her finder du slides med samme gode råd som i præsentationen dog i større format. Disse slides kan klippes ind i præsentationen såfremt der ikke er et stort lærred ved præsentationen. Så kan deltagerne bedre læse teksterne.

Baggrundsinfo om oplæggets temaer

Materialet består af to overordnede temaer: 1) Indbrud og 2) Snyd og bedrag.

De to temaer har hver både fysiske og digitale aspekter. Det er relevant og vigtigt at formidle begge temaers aspekter til ældre borgere så de kan gøre deres hverdag mere sikker. De vil typisk selv efterspørge råd til hvordan de kan sikre sig i den fysiske verden, men det er præcis lige så vigtigt at de gør deres digitale verden mere sikker. Det gælder også de ældre som ikke selv opfatter sig som digitale.

Som supplement til talekortene, kan du her læse lidt mere om hvert tema så du har tilstrækkelig baggrunds-viden til holde oplægget og til at skabe en god dialog med dit publikum.

TEMAERNE ER:

1. Indbrud – i din bolig
2. Indbrud – i dit digitale hjem
3. Snyd og bedrag – Tricktyveri i hjemmet og på indkøbsturen
4. Snyd og bedrag – Fuphenvendelser på mail og sms
5. Snyd og bedrag – Fupopkald

1. Indbrud i din bolig

Indbrud i hjemmet er attraktivt for en tyv, fordi det er forholdsvis nemt, relativt risikofrit og giver et acceptabelt udbytte! Det kan der heldigvis gøres noget ved.

Forskning viser at en indbrudstyv ofte giver op hvis han skal bruge mere end 3 minutter på at bryde ind i en ejendom uden at larme fordi risikoen for at blive opdaget stiger. Derfor gælder det om, at gøre det så svært for tyven at han skal bruge mere end 3 minutter.

Man kan reducere risikoen for indbrud ganske betragteligt ved at gøre nogle få ting. Tyven kommer oftest ind i huset ved at bryde et vindue op der er "skjult for nysgerrige blikke".

Huse fra 1960'erne og godt op i nullerne er for en stor dels vedkommende forsynet med ældre vinduer i trærammer og som oftest uden sikringsforanstaltninger. Hvis ruden i vinduet er listet udefra, kan listerne fjernes helt lydløst med fx en bredbladet skruetrækker eller spaden der står frit tilgængelig i haven eller i det ulåste haveskur. Når listen er fjernet, kan ruden løftes ud og sættes på jorden. Det tager under 1 minut. Det samme gør sig gældende for en dør med f.eks. små ruder. Der kan man "afmontere" en rude og herefter åbne døren.

Det er derfor vigtigt at se på om ruderne i både vinduer og døre er listet udefra. Er de det, kan de sikres forholdsvis nemt med envejsskruer (sikringsskruer). De holder nemlig på ruden selvom tyven fjerner listerne. Alternativt kan man lime ruden fast til rammen. (Det skal være speciallim, og ruden skal afmonteres helt).

Hvis vinduerne er sikrede og haveredskaberne er låst inde, er det svært for en indbrudstyv at komme ind i huset lydløst. Men det kræver selvfølgelig også at der er nogen til at reagere på larmen. Derfor bør det kombineres med f.eks. Nabohjælp og en "synlig" bolig i form af god belysning og en trimmet hæk samt evt. alarm.

Disse tiltag vil reducere risikoen for indbrud ganske betydeligt, men det er ikke en garanti. Det er derfor altid en god ide at gemme eller sikre ting der har stor værdi og som vanskeligt kan erstattes (fx arvesmykkerne), så tyven ikke umiddelbart kan finde dem – og jo, en garvet indbrudstyv kender godt de sædvanlige gemmesteder.

Kort sagt: Man skal gøre sådan at tyven allerede inden selve indbruddet bliver stresset fx ved sensorstyret lys eller en "nysgerrig nabo" så han ikke kan arbejde uset. Dernæst må indbruddet ikke kunne ske lydløst, og man skal ikke "forære" ham værktøjet. Husk at sætte en god lås på haveskuret og at komme værktøjet derind. En glemt spade i haven er en gave til en indbrudstyv!

VINDUER OG DØRE

- Hvis vinduerne ikke i forvejen er forsynet med gode låse-/sikringsbeslag så kan det gøres med 1-2 beslag pr. vindue.
- Er dørene forsynet med ældre låse, er det altid en god ide at udskifte låsene til en ny model – og gerne uden indvendig vrider.
- Særlig opmærksomhed på terrasse-, kælder- og bagdøre der ikke kan ses fra vejen.

HÆK, LYS OG NABOHJÆLP

- Trim hækken: Trim hække, buske og træer, som kan give dække. På den måde bliver det sværere for tyven at komme uset ind.
- Sensorstyret eller automatisk lys: Tænd lys ude. Lys med sensor øger chancen for, at tyven bliver set af naboen og forstyrret i sit arbejde.
- Tilmed dig Nabohjælp og vær en aktiv nabohjælper: Hils på dem du møder på din vej. Godt naboskab og fælles opmærksomhed øger tyvens risiko for at blive opdaget. Det gør nabolaget mindre attraktivt for tyven og mere trygt for dig.

Præsentationens indhold om indbrud i din bolig

- Forside
- Illustration til introduktion af temaet
- Film om Nabohjælp
- Film hvor en tidligere indbrudstyv fortæller, hvad han kigger efter.
- Dialogslide
- Råd til at sikre boligen

Præsenter kort temaet og se de to film med deltagerne. Tal med dem om hvordan man kan sikre sin bolig og gemme sine værdigenstande. Saml op på dialogen og gentag til sidst de vigtigste budskaber.

2. Indbrud i dit digitale hjem

Adgang til de ældres fysiske hjem er ikke det eneste tyvene er ude efter. De forsøger også at få adgang til deres digitale hjem hvor de kan stjæle penge og personoplysninger.

Adgangskoder er nøglerne til det digitale hjem. De er derfor vigtige og bør være af høj kvalitet - præcis som nøgler og låse i det fysiske hjem. Hvis adgangskoden er let at gætte, er det som at have en ulåst dør der inviterer tyven ind i stuen.

Det vil være nyt for mange at tale om et digitalt hjem og derfor bør denne del af oplægget indledes med at definere hvad det omfatter. Det digitale hjem er alle de steder på nettet hvor man bruger adgangskoder eller indtaster personlige oplysninger og/eller betalingsoplysninger. Disse oplysninger har høj værdi, og skal derfor beskyttes med en solid lås – altså en stærk adgangskode.

Dialogen med de ældre kan derfor tage udgangspunkt i hvordan de laver den stærkeste adgangskode til de vigtigste steder dvs. mail, NEMID og sociale medier.

På samme måde som man gemmer sine værdigenstande, bør man også beskytte sine adgangskoder. Brug derfor også dialogen til at tale om hvordan de sikkert kan gemme deres adgangskoder i fx e-Boks og at det er vigtigt at de finder et sikkert sted i hjemmet hvis de gemmer deres adgangskoder i en lille notesbog. Et sted tyvene ikke kender og hvor det er synligt for dem hvis nogen har haft adgang.

NemID bruges af 98% af de 60+ årige, og ni ud af ti 65+ årige bruger e-Boks eller netbank.* Herfra kender de til totrinsgodkendelse. Brug NemID til simpelt at forklare hvad totrinsgodkendelse er og hvorfor det er vigtigt også at bruge totrinsgodkendelse til andre webtjenester, fx mail og sociale medier. Totrinsgodkendelse kan også sammenlignes med at de ældre ud over nøgler også har et alarmsystem til hjemmet der skal deaktiveres, inden man får adgang.

PASSWORD MANAGER

Hvis det passer til dit publikum, kan du også komme ind på brugen af en password manager.

ADGANGSKODE

En stærk adgangskode er:
1. brugt maks. 1 sted
2. min. 12 tegn langt
3. indeholder tal, symboler, store og små bogstaver, samt specialtegn
4. upersonligt (ingen personlige oplysninger, fx dit barnebarns navn)
5. ikke en tidligere anvendt kode
6. ukendt for alle andre end dig selv

Brug en linje du kan huske fra en sang fx titlen eller første vers kombineret med fire cifre, dit lykketal og et specialtegn. Eksemplet vises i præsentationen.

TOTRINSGODKENDELSE

Totrinsgodkendelse er en ekstra beskyttelse, der gør, at tricktyve ikke kan bruge dit brugernavn og adgangskode til at komme ind på din konto. De mangler den engangskode, der sendes som sms til din telefon.

Du kender det fra NemID, hvor du sammen med dit brugernavn og adgangskode også skal bruge en nøgle fra nøglekortet eller NemID nøgleappen.

Du kan tilvælge totrinsgodkendelse i de fleste web-tjenester fx Gmail og Facebook.

Totrinsgodkendelse omtales også som tofaktorgodkendelse.

PASSWORD MANAGER

Har du mange adgangskoder, kan en password manager være en hjælp.

Med en password manager skal du kun huske én kode, som er adgangen til din konto, hvor du samler alle dine brugernavne og adgangskoder.

Kontoen kan du få adgang til via en app på telefonen eller på internettet.

Der findes mange forskellige password managere. Søg derfor på internettet efter én, der passer til dine behov.

Politiet anbefaler ikke en specifik password manager.

Præsentationens indhold om indbrud i dit digitale hjem

- Forside
- Illustration til præsentation af temaet med eksempler på, hvad der indgår i "det digitale hjem"
- De 10 mest brugte adgangskoder
- Eksempel på en stærk adgangskode
- Dialogslide
- Råd til at sikre dit digitale hjem

Præsenter kort temaet ved at fortælle hvad det digitale hjem består af. Brug metaforer for en fysisk bolig. Vis de 10 mest brugte adgangskoder og lad deltagerne byde ind med hvad de tror det er og spørg evt. om de selv bruger et af dem. Fortæl hvordan man kan lave en stærk adgangskode, om totrinsgodkendelse og sikker opbevaring. Tal med dem om hvilke adgangskoder der er vigtigst og hvorfor, og hvordan man kan opbevare adgangskoder sikkert. Saml op på dialogen og gentag til sidst de vigtigste budskaber.

*Se "It-anvendelse i befolkningen 2017" fra Danmarks Statistik og "NemID imagemåling 2017" fra Digitaliseringsstyrelsen.

3. Snyd og bedrag: Tricktyveri

Tricktyveri sker både i og uden for hjemmet. Ved tricktyveri er der et fysisk møde mellem offer og gerningsperson. Det adskiller sig fra fuphenvendelser som kan ses som den digitale version af tricktyveri.

I størstedelen af sagerne om tricktyveri i hjemmet er formålet for gerningspersonen at snyde sig indenfor for derefter at stjæle kontanter, smykker mv.

Gerningspersonen henvender sig typisk ved hoveddøren hos en ældre borger og udgiver sig for at være fx hjemmehjælper, vicevært eller håndværker. Målet er at skabe så meget forvirring for den ældre at gerningspersonen og/eller medgerningspersoner uset kan komme ind i boligen. Her kan de i løbet af meget kort tid finde smykker, kontanter og andre værdigenstande og forlade boligen igen.

TRICKTYVERI UDEN FOR HJEMMET

Tricktyveri uden for hjemmet adskiller sig fra lommetyveri ved, at en eller flere gerningspersoner

skaber en situation der forvirrer offeret så meget, at de kan stjæle kontanter eller kreditkort. Tricktyvene går typisk efter en ældre person der færdes alene. De er især ude efter betalingskort da de med rette PIN-kode efterfølgende kan hæve endda meget store beløb.

Ved tyveri af kreditkortet har gerningspersonen forinden afluret PIN-koden. Det sker typisk når forurettede hæver kontanter i en hæveautomat eller betaler indkøb med betalingskortet. Efterfølgende bliver forurettede kontaktet på fx gaden eller p-pladsen hvor en eller flere gerningspersoner fx spørger om vej og breder et stort kort ud. Denne afledningsmanøvre giver mulighed for at en medgerningsperson kan stjæle forurettedes kreditkort.

Det ses i flere og flere tilfælde at kreditkortet tages ud af pungen hvorefter pungen lægges tilbage i forurettedes taske. Forurettede opdager derfor ikke med det samme at kreditkortet er stjålet. Der kan derfor hæves mange penge over flere dage – indtil kortet bliver spærret.

BETALING OG KONTANTER

Brug trådløs betaling så vidt muligt.

Beskyt pinkoden når du betaler, så ingen kan se den mens du taster.

Undgå at have mange kontanter på dig og i dit hjem.

SIKKER OPBEVARING

Opbevar ikke betalingskort og kode samme sted.

Læg altid dine værdigenstande i inderlommen. Brug aldrig yderlommer eller baglommer.

Hold altid din taske lynet og under opsyn og bær den gerne tæt ind til kroppen.

Lad aldrig værdigenstande ligge fremme i hverken entre eller bryggers. Det gælder punge, nøgler, penge, smartphones, smykker mv.

SUND SKEPSIS

Udvis skepsis, hvis en person pludselig går ind i dig, stopper op og spærrer vejen for dig eller spørger dig om hjælp.

Bed altid fremmede personer om at fremvise legitimation, hvis de banker på din dør. Fx hvis nogen udgiver sig for at være fra hjemmeplejen eller politiet.

Præsentationens indhold om snyd og bedrag: Tricktyveri i hjemmet og på indkøbsturen

- Forside
- Illustration af tricktyveri på indkøbsturen
- Eksempler på tricktyveri i hjemmet
- Dialogslide
- Råd til at beskytte sig mod tricktyveri ude og hjemme

Fortæl om tricktyveri ude, og giv derefter to eksempler på tricktyveri i hjemmet. Tal med dem om deres erfaringer med tricktyveri og hvordan man kan beskytte sig både hjemme og ude. Saml op på dialogen og gentag til sidst de vigtigste budskaber.

4. Snyd og bedrag: Fuphenvendelser på mail og sms

De fleste danskere modtager fra tid til anden en fupmail. Ofte bliver de fanget i spamfilteret, men enkelte slipper igennem og havner i vores indbakke på mailkontoen.

Med mobilen i hånden er vi mindre årvågne over for det vi modtager. Vi reagerer hurtigt, og det udnytter tricktyvene.

Formålet med både fupmails og fupsms'er er at få modtageren til at klikke på et link for at bekræfte eller opdatere personfølsomme oplysninger. På den måde får svindlerne adgang til fx adgangskoder, kort- og kontooplysninger, NemID og personnummer – altså nøglerne til vores digitale hjem.

Klikker man på linket, bliver man typisk ført til en hjemmeside der ligner en tro kopi af en hjemmeside som borgeren kender. Svindleren får adgang til alle de oplysninger der indtastes på siden, og indtaster man fx sine kortoplysninger i den tro at man betaler porto for at få tilsendt en gevinst, kan det sammenlignes med at man udleverer både kort og koder til svindleren.

Omfanget af fupmails og fupsms'er er stort, og de fleste er heldigvis til at gennemskue. Svindlerne bliver dog bedre og bedre til at lave en troværdig tekst. Samtidig virker henvendelsen ofte så lokkende, truende, hjælpende eller hastende, at vi sættes i en situation, hvor vores sunde fornuft slår fra.

I politiet oplever vi endda at fuphenvendelserne kommer samtidig med at man fx gør et online køb eller omkring tidspunktet for offentlige myndigheders henvendelse til borgere, fx Skats årsopgørelse. Det gør troværdigheden og risikoen for at blive snydt større.

STOP, TÆNK, KONTAKT

Så længe man ikke reagerer på en fuphenvendelse, sker der ikke noget. Vi kan derfor hjælpe os selv ved at være kritiske.

Du kan tage udgangspunkt i eksemplerne i oplægget når du sammen med de ældre taler om hvad man skal kigge efter når man modtager en mail der efterspørger ens personoplysninger. Mind de ældre om at eksemplerne kan være nogle andre i morgen, og det derfor er vigtigt at holde fast i rådene. De gælder både i dag og i morgen.

Brug eksemplerne til at vise det væld af forskellige fuphenvendelser der florerer. Det kan være alt fra at man har vundet i en konkurrence, advarsler om hackingforsøg til opdatering af oplysninger hos banken. Inddrag publikum ved at tale om hvilke fupmails og fupsms'er de har modtaget, og hvordan de reagerede i situationen.

Det vigtigste råd er at man aldrig skal udlevere følsomme oplysninger når man kontaktes uopfordret. Det gælder både i dag, i morgen og dagen efter. Hvis henvendelsen er reel, er der altid tid til at tænke sig om. Hvis man derefter tror at den er god nok, anbefaler vi at man for en sikkerheds skyld søger virksomhedens telefonnummer frem og ringer til dem. *Stop, tænk, kontakt.*

Har man ignoreret en reel henvendelse? Bare rolig – de skal nok forsøge at få kontakt igen. Og så er det forfra med *stop, tænk, kontakt.*

Når man får en mail, bør man overveje følgende:

- Kender jeg afsenderen?
- Har jeg gjort noget der gør at afsenderen retter henvendelse til mig? Fx deltaget i en konkurrence.
- Forventer jeg at modtage noget fra afsenderen – på dette tidspunkt og i dag?
- Giver det mening at afsenderen efterspørger mine oplysninger, eller bør afsenderen allerede have dem?

Man bør også se efter dette:

- En lang eller mærkelig adresse på afsenderen, dvs. det der står efter @.
- Dårlig dansk og stavefejl.
- Fejl i logoer fx farver, former, tekst.

Husk! Så længe man ikke klikker på noget, kan der ikke ske noget. Så tag dig god tid.

KLIK IKK'

Klik aldrig på links der beder om personfølsomme oplysninger.

Klik aldrig på links i mails fra offentlige myndigheder. Myndigheder sender som udgangspunkt ikke links.

STOP, TÆNK, KONTAKT

Giver det mening, at afsenderen kontakter mig?

Tag dig tid til at tænke og kontakt evt. afsenderen på telefon.

Søg selv nummeret frem, så du er sikker på at ringe til den rigtige virksomhed/myndighed.

SIKKER OPBEVARING

Undgå personfølsomme oplysninger på din telefon. Så risikerer du ikke ved en fejl at give adgang til dem.

Præsentationens indhold om snyd og bedrag: Fuphenvendelser på mail og sms

- Forside
- Illustration af fupmails og fupsms'er
- Eksempel på fupmail
- Eksempel på tre fupsms'er
- Dialogslide
- Råd til at beskytte sig mod fupmails og fupsms'er

Fortæl med udgangspunkt i eksemplerne på fupmails og fupsms'er hvad man skal være opmærksom på for at gennemskue fup, herunder at det ofte haster. Fortæl også at uheldig timing har stor betydning. Tal med dem om deres erfaringer med fuphenvendelser og hvordan man kan beskytte mod dem. Saml op på dialogen og gentag de vigtigste budskaber.

5. Snyd og bedrag: Fupopkald

De fleste ældre har sikkert hørt om eller selv modtaget opkald fra dårligt engelsktalende personer, der siger, at de ringer fra Microsoft IT support og vil hjælpe med at fjerne virus på computeren.

Desværre bliver fupopkald mere og mere troværdige. Der er fupopkald hvor de taler dansk, er velformulerede og udgiver sig for at ringe fra en offentlig myndighed eller en virksomhed hvor modtageren er kunde, fx bank eller forsikringsselskab. Svindlerene er dygtige til at skabe en stressende situation hvor det haster og man skal reagere NU hvis man ikke vil miste en masse penge.

Modtagerne fatter ofte mistanke allerede ved opkaldets begyndelse og forsøger at holde fast i deres overbevisning og afvise svindleren. Problemet opstår fordi svindleren har masser af tålmodighed og gerne bruger timer på at overbevise borgeren om opkaldets rigtighed. Svindlerne forsøger at gøre det umuligt at afslutte opkaldet på en ordentlig måde. I stedet for at stille spørgsmål og tale med personen, er man derfor nødt til at lægge høfligheden fra sig og afvise personen i røret ved at lægge på.

SPOOFING

Spoofing er når svindlere overtager et eksisterende telefonnummer. Det betyder at telefonnummeret du ser på din mobilskærm, vises som det faktiske telefonnummer på virksomheden eller den offentlige myndighed du kender, selvom det er svindlere der ringer eller sms'er.

Det er ikke alle svindlere der er så smarte, og du kan derfor også tjekke, om andre har oplyst at telefonnummeret er falsk. Det kan du gøre på fx ukendtnummer.dk eller 180.dk.

STOP, TÆNK, KONTAKT

Ved uopfordrede opkald fra fx banker eller myndigheder, er det altid en god idé at bede om navnet på personen der ringer, og meddele at man ringer tilbage 5 minutter senere. Søg selv nummeret frem – ring op til omstillingen og bed om at blive stillet igennem.

Er der modstand mod, at man selv ringer op, skal man blot lægge på.

SVÆRE ETISKE DILEMMAER.

Nogle fupopkald er ekstra grove, og kan sætte modtageren i et svært etisk dilemma. Det kan fx være opkald om at modtagerens barnebarn er i knibe og at der er akut brug for en pengeoverførsel for at hjælpe barnebarnet. En historie kunne fx være at barnebarnet er involveret i en trafikulykke på en ferie og at det koster penge at tilkalde en ambulance.

Det kan også være dobbeltopkald hvor modtageren i første omgang afværger et fupopkald og derefter bliver ringet op af en falsk betjent der under påstand af at kende til opkaldet beder om informationer. Brug gerne dialogen til at tale om, hvordan man i disse situationer kan holde fast i sin sunde fornuft og afvise opkaldet.

ET EKSTRA TIP

Afslutningsvis kan du tale med de ældre om det gamle kneb med at bruge en telefonsvarer og undlade at tage telefonen når de ikke kender nummeret. Er det ikke et fupopkald, vil personen typisk lægge en besked, og den ældre kan så selv ringe tilbage.

STOP, TÆNK, KONTAKT

Giver det mening, at afsenderen kontakter dig?

Bed om et navn du kan ringe tilbage til, hvis du uventet bliver ringet op af en virksomhed eller offentlig myndighed.

LÆG PÅ

Læg på, når fremmede ringer – eller lad være med at tage telefonen.

Du behøver ikke at være høflig. Er det et reelt opkald, lægger personen en besked eller kontakter dig på anden vis.

SIKKER OPBEVARING

Udlever aldrig bekræftelseskoder, personfølsomme oplysninger eller kort- og kontooplysninger over telefonen.

Præsentationens indhold om snyd og bedrag: Fupopkald

- Forside
- Illustration af fupopkald
- Dialogslide om fupopkald
- Råd til at beskytte sig mod fupopkald

Fortæl om fupopkald. Læg fokus på de svære situationer, hvor opkaldet handler om private forhold eller ”dobbeltopkald” hvor man først afværger et fupopkald og derefter kontaktes af en fuppolitibetjent. Tal med dem om deres erfaringer og gode strategier til at afslutte opkaldene. Saml op på dialogen og gentag de vigtigste budskaber.

Opsamling og afslutning

Det er en god ide at afslutte oplægget med en opsamling så de vigtigste pointer gentages. Derudover kan du fortælle de ældre hvor de kan finde mere information og hvordan de kan kontakte politiet hvis det skulle blive nødvendigt.

FREMHÆV DE VIGTIGSTE POINTER

- Indbrud i både bolig og digitalt hjem: I begge tilfælde handler det om at sikre sig med en stærk lås/adgangskode og gøre både fysisk og digitalt hjem mindre tilgængelige ved fx at låse haveredskaber inde og bruge totrinsgodkendelse.

- Sikker opbevaring af både fysiske værdigenstande og koder: Penge, værdier og adgangskoder bør ikke ligge synligt fremme – eller være gemt på fx telefonen. Pinkoden bør skærmes ved betaling, og tegnebog bør holdes tæt til kroppen. Penge og passwords er lige så private som underbukser, og bør ikke vises frem.

- Sund skepsis over for fremmede: Bed om dokumentation og vær ikke for høflig til at afvise og holde afstand til fremmede. Vær på vagt over for uopfordrede henvendelser fra virksomheder og offentlige myndigheder.

- Stop, tænk, kontakt: Ved den mindste tvivl eller usikkerhed, bør man afbryde kontakten og tage sig tid til at tænke, og derefter selv tage kontakt til virksomheden eller den offentlige myndigheds hovednummer. Har de rent mel i posen, skal I nok finde ud af det.

FORTÆL HVOR DE ÆLDRE KAN FINDE MERE INFORMATION

- Nabohjælp: Nævn igen at de første to film er produceret af Bo Trygt, som står bag Nabohjælp, og fortæl, at de kan finde flere gode tips til indbrudssikring på deres hjemmeside.

- Mit digitale Selvforsvar: Du kan med fordel opfordre de ældre til at downloade app'en. Politiet, andre offentlige myndigheder, banker og private virksomheder bruger den til at udsende aktuelle advarsler om fuphenvendelser. Der er også god information om, hvad man skal gøre, hvis man bliver snydt. App'en drives af Forbrugerrådet Tænk i samarbejde med Trygfonden.

- Børn og børnebørn: Hvis deltagerne er meget usikre, kan du evt. tale med dem om at få børn og børnebørn til at hjælpe med at få foretaget de foreslåede sikkerhedsforanstaltninger. Dette frarådes dog hvis deltagerne overvejende er aktive ældre.

FORTÆL HVORDAN MAN ANMELDER

Mødet med de ældre er en oplagt mulighed for at fortælle de ældre, hvordan de skal kontakte politiet, hvis uheldet er ude. Fortæl dem om forskellene på 112 og 114 og om den digitale anmeldelsesplatform til it-kriminalitet. Fortæl evt. også at de skal spærre NemID og kontokor, hvis de har mistanke o, at det er blevet misbrugt eller hvis andre er kommet i besiddelse af deres oplysninger.

SPØRGSMÅL FRA DELTAGERNE

Afsæt 5 minutter til de allersidste spørgsmål. Da oplægget er dialogbaseret, har der være rig spørgemulighed undervejs men en ekstra spørgemulighed kan give de ældre den sidste tryghed i forhold til råd og anbefalinger.

UDDELING AF HANDOUT

Uddel til sidst flyeren med de vigtigste råd. Når du gør det efter oplægget, undgår du at miste dit publikums opmærksomhed.