

5 anbefalinger til tryk kunde- kommunikation

Den digitale kriminalitet er stigende. Med udbredelsen af AI-baserede værktøjer har kriminelle fået endnu bedre muligheder for at udføre digital svindel i større skala, bedre kvalitet og endnu mere målrettet end hidtil. Både borgere, forbrugere og virksomheder taber på den omfattende digitale kriminalitet, hvor virksomheder og myndigheders navn, brand og troværdighed misbruges til at svindle borgerne.

Mange virksomheder gør allerede en stor indsats for at forebygge og håndtere digital svindel. Og mange vil gerne gøre mere for at hjælpe forbrugerne og deres kunder.

Derfor har Forbrugerrådet Tænk og TrygFonden, som står bag varslingsappen Mit Digitale Selvforsvar, samarbejdet med partnere bag appen om at formulere fem overordnede anbefalinger til, hvordan man som virksomhed kan kommunikere med sine kunder, medlemmer og omverdenen på måder, som gør livet sværere for svindlerne.

Anbefalingerne har til formål at øge tilliden til virksomheders digitale kommunikation og sætte en fælles højere standard for kommunikation, som styrker forbrugernes robusthed over for digital kriminalitet og gør det sværere for de kriminelle at få succes.

Anbefalingerne kan bruges til at rammesætte en intern dialog i en virksomhed eller organisation om, hvorvidt ens kommunikationspraksisser og -procedurer harmonerer med anbefalingerne, eller om der er behov for at ændre noget. Anbefalingerne skal ikke ses som en fyldestgørende eller absolut tjekliste, men som vejledende.

Vigtigst er det, at man bruger anbefalingerne til at undersøge og gøre sig bevidst om egen praksis, valg og fravalg, og på den baggrund lave en samlet vurdering af, hvordan kommunikationen påvirker risikoen for svindel mod egne kunder og forbrugere generelt.

5 anbefalinger:

1. Vær varsom med, hvordan du beder om kunders oplysninger
2. Kunder skal altid kunne verificere, hvem de kommunikerer med
3. Informér jeres kunder om aktuel svindel
4. Hjælp kunder, der kontakter jer om svindel
5. Forebyg svindel ved at reagere hurtigt og effektivt

1: Vær varsom med, hvordan du beder om kunders oplysninger

- Vær meget varsom med at udsende aktive links i jeres eksterne kommunikation, fx mail og sms'er, som kunder skal klikke på. Kunden kan ikke afkode, om linket fører til en legitim webside. Svindlerne bruger ofte aktive links til phishing.
- Vær meget varsom med at anvende QR-koder i jeres kommunikation i det åbne offentlige rum. Svindlere bruger QR-koder til phishing, fx på falske parkeringsbøder eller elbilladestandere.
- Anvis kunder en lukket kommunikationskanal fx en app eller et login-beskyttet site, som de selv kan gå ind på og administrere deres oplysninger.

Eksempel på god praksis:



2: Kunder skal altid kunne verificere, hvem de kommunikerer med

- Råd altid kunder til selv at verificere afsender. Hvis de kontakter jer med tvivl om en henvendelse, forsøg ikke at overbevise dem, men råd dem til at være sikker ved at 'bruge fordøren', dvs. selv søge jeres website frem og/eller selv finde og ringe op til jeres hovednummer for at verificere, om henvendelsen kommer fra jer. Hav et setup, så kunden bliver hjulpet igennem verifikationsprocessen.
- Hav genkendelige og retvisende tekster på de digitale transaktioner, kunder skal foretage eller godkende. Fx bør det være virksomhedens navn, som kunden kender det, der vises som Mobile-pay-modtager, på kontoudtog og lignende. Væn på den måde jeres kunder til, at det skal være muligt at verificere en transaktion.
- Kommuniker proaktivt og synligt til jeres kunder, hvordan de kan forvente, at I kommunikerer med dem – og hvordan I aldrig vil kommunikere til dem. Oplys fx om, hvilke mailadresser og telefonnumre I kontakter dem fra, hvordan I anmoder om betalingsinformation, i hvilke tilfælde I ringer jeres kunder op etc. Det gør at kunden kan forholde sig skeptisk over for kommunikation, der ikke stemmer overens med jeres praksis.
- Beskyt jer mod, at svindlere misbruger jeres afsenderID eller telefonnummer og kan udgive sig for at være jer på mail, sms eller i telefonopkald. Undersøg muligheden for spoofingbeskyttelse af jeres telefonnumre hos jeres teleselskab, og aktiver protokollen DMARC på emails. Læs mere på www.teleindu.dk og på www.sikkerdigital.dk.
- Beskyt jer mod, at svindlere misbruger jeres digitale identitet og domænenavn. Aktiver DNSSEC og benyt fx en professionel brand protection service. Læs mere www.sikkerdigital.dk og www.unikpaanettet.dk.

Eksempel på god praksis:

Gode råd til en bedre digital sikkerhed

Husk, log altid ind på sygeforsikring.dk med MitID, hvis du skal have udbetalt tilskud, opdatere dine personlige oplysninger mm.

1 Vær obs på links i mails og sms'er
Del aldrig personlige oplysninger over mail eller via links. Log i stedet ind på sygeforsikring.dk med MitID, så er du bedst sikret mod svindel.

2 Ingen beløb i sms'er eller mails
Der er ikke beløb i sms'er eller mails fra "danmark". De er blot notifikationer om, at der er nyt på selvbetjeningen til dig. Vi har fjernet beløbet for at passe bedst muligt på vores medlemmer. Mange svindlere bruger nemlig beløb som lokkemad til at franske personlige oplysninger.

3 Ingen personlige oplysninger uopfordret over telefonen
Sygeforsikringen "danmark" ringer aldrig uopfordret og beder om bank- eller personoplysninger. Log ind med MitID på sygeforsikring.dk for at foretage ændringer eller opdateringer.

4 Beskyt dine personlige oplysninger
Log altid ind med MitID på sygeforsikring.dk, hvis du vil foretage ændringer i dit medlemskab, vil opdatere dine oplysninger mm.

5 Tjek afsenderen
Åben kun mails, hvor du kender afsenderen. Mails fra "danmark" vil altid være afsendt fra domænet @sygeforsikring.dk. Vær dog opmærksom på, at svindlere kan være kreative med navngivning, og det derfor kan se ud, som om mailen er sendt fra @sygeforsikring.dk.

[Log ind](#)

3: Informér jeres kunder om aktuel svindel

- Advar jeres kunder om aktuel svindel i jeres navn for at forebygge, at flere bliver ofre for samme type svindel. Det kan I gøre via Mit digitale selvforsvar samt på jeres egne kanaler – fx på forsiden af jeres hjemmeside eller app. Vis gerne eksempler på den svindel, der aktuelt udsendes i jeres navn.
- Henvis til en side med gode råd og hjælpsomme redskaber, kunden kan bruge. Læg jer eventuelt op ad myndighedernes gode råd, som findes på www.sikkerdigital.dk/borger.

Eksempel på god praksis:



4: Hjælp kunder, der kontakter jer om svindel

- Kunder, der mistænker svindel, vil ofte kontakte den virksomhed, som beskeden eller opkaldet (tilsyneladende) kommer fra. Vær tydelig i jeres eksterne kommunikation om, at I er tilgængelige på mail eller telefon for hjælp ved mistanke om svindel.
- Tag enhver henvendelse om svindelforsøg alvorligt. Berolig kunden og udvis forståelse for deres situation. Svindlerne er blevet så dygtige, at alle kan blive ramt. Der er ikke noget at skamme sig over, og det er legitimt at kunden er skeptisk.
- Undersøg, om kunden faktisk har modtaget en henvendelse fra enten jer, jeres telemarketing eller andre eksterne samarbejdspartnere. Hvis ikke, kan der være tale om svindel.
- Ved mistanke om svindel, henvis til myndighedernes Cyberhotline for digital sikkerhed på www.sikkerdigital.dk/cyberhotline. De kan rådgive kunden og hjælpe med at spærre MitID. Kunden vil desuden ofte være nødt til at kontakte banken og Politiet.

5: Forebyg svindel ved at reagere hurtigt og effektivt

- Hav klare interne procedurer for håndtering af mulig svindel, herunder håndtering af henvendelser fra kunder herom. Hav også klare procedurer for, hvornår og hvem der anmelder svindelforsøg til politiet, samt til andre nødvendige aktører såsom webhost, teleoperatører og myndigheder.
- Vær opmærksom på, at I kan have behov for at indhente dokumentation til politi eller myndigheder for at de kan efterforske sagen, samt for at kunne håndhæve jeres rettigheder, hvis nogen misbruger jeres navn, domæne mv.
- Husk at advare eksternt om aktuelle svindelforsøg via Mit Digitale Selvforsvar. Flere end 500.000 danskere har appen, og advarsler udbredes ofte fra appen til andre medier.

