# National cybersikkerhedsmåned (NCSM): 4 uger 4 kampagner

Formålet med cybersikkerhedsmåneden er at sætte fokus på cyber- og informationssikkerhed. Måneden giver anledning til at sætte ekstra fokus på temaer inden for cyber- og informationssikkerhed.

For at udnytte cybersikkerhedsmåneden i sin fulde længde kan du med fordel bruge fire nyudviklede film som afsæt for fire kampagner om fire vigtige emner, nemlig:

* Phishing
* kodeordssikkerhed,
* at arbejde på farten
* følsomme oplysninger.

Link til alle fire film: <https://www.sikkerdigital.dk/myndighed/uddannelse-og-awareness/film-om-god-sikkerhedsadfaerd>. Bemærk, at filmene både kan tilgås fra linket og downloades, hvis din organisation ønsker at præsentere dem enkeltvis.

Indholdet nedenfor er et forslag til, hvordan filmene kan præsenteres i oktober måned. Det kan fx ske på fire mandage i oktober. Teksterne er konkrete forslag, du kan lade dig inspirere af og tage udgangspunkt i – fx i en mail til alle medarbejdere eller i form af en nyhed på intranettet. Link til analysen Danskernes informationssikkerhed: **[LINK].**

Du kan redigere, tilpasse eller skrive dine helt egne tekster.

|  |
| --- |
| **Uge 1: Phishing** |
| Kære kollega Oktober måned er national cybersikkerhedsmåned. Og i den anledning sætter vi i løbet af de næste fire uger fokus på fire vigtige emner inden for cyber- og informationssikkerhed. Første emne er phishing.**Hvad er phishing?**Phishing er en form for svindel, hvor svindlerne forsøger at narre personlige oplysninger, fx kodeord, fra offeret. Man kan fx blive bedt om at klikke på et link, som fører til en falsk login-side, hvor man bliver bedt om at indtaste sine login-oplysninger.**Hvor udbredt er phishing mod offentligt ansatte?**Analysen Danskernes informationssikkerhed 2024 viser, at phishing er den form for digital svindel, som flest offentligt ansatte møder. Næsten halvdelen af alle offentligt ansatte har i arbejdssammenhæng modtaget et phishing-link på mail, SMS eller chat-besked. Phishing kan være en trusselsform i sig selv, men kan også være en indgang for andre typer af digital kriminalitet.**Hvordan undgår jeg phishing-fælden?**Husk, at du aldrig skal svare på henvendelser, der beder om personlige oplysninger, som fx koder, login- eller bankoplysninger. Se denne korte film om phishing, som indeholder gode råd til, hvordan du undgår at gå i fælden. Den varer kun et par minutter.[LINK TIL FILM] |
| **Uge 2: Kodeordssikkerhed** |
| Kære kollegaHar du en god metode til at lave stærke kodeord, du kan huske? Vi går nu ind i 2. uge i oktober. Og i anledning af den nationale cybersikkerhedsmåned vil vi gerne sætte fokus på adgangskoder. **Hvad skal jeg være opmærksom på?**Et af problemerne med kodeordssikkerhed er, at man let kommer til at tage smuthuller for at gøre sin adgang til systemer lettere. Analysen Danskernes informationssikkerhed 2024 viser, at 26 % af medarbejdere i myndigheder bruger det samme kodeord til flere systemer, og at 23 % bruger samme kodeord i private og i arbejdsmæssige sammenhænge. **Hvorfor er det et problem?**Det er et problem, fordi genbrug af kodeord betyder, at et brud på sikkerheden lettere overføres fra et sted til et andet. **Hvordan kan jeg styrke mine kodeord?**Heldigvis er der metoder til at få orden på kodeordene: Du kan fx bruge passphrases (sætninger) til at lave stærke kodeord, du kan huske, eller du kan bruge en passwordmanager. Se denne korte film om kodeordssikkerhed, som indeholder tre gode råd til, hvordan du styrker dine kodeord. Filmen varer kun et par minutter.[LINK TIL FILM] |
| **Uge 3: Arbejde på farten** |
| Kære kollegaVed du, hvilke retningslinjer der gælder for hjemmearbejde i organisationen? Ved du, hvad du skal gøre for at holde styr på informationssikkerheden, når du arbejder hjemme, i toget eller på en café? **Ikke alle kender retningslinjer** Analysen Danskernes informationssikkerhed 2024 viser, at mere end halvdelen af offentligt ansatte arbejder hjemme en del af tiden. Dog ved ca. 1/3 ikke, om der i deres arbejde gælder retningslinjer for informationssikkerheden, når de arbejder hjemme eller i det offentlige rum. **Hvad skal jeg huske, når jeg arbejder hjemme eller på farten?**Der er nogle basale råd, som det er godt at få styr på og få ind i sine vaner. Det handler bl.a. om at bruge sikre netværk, hotspot fra telefonen og VPN. Det handler også om, hvordan man holder telefonmøder, virtuelle møder og bruger sine skærme, mens man fx arbejder i toget eller på en café. Det er bl.a. en rigtig god idé at bruge diskretionsskærm, når man arbejder steder, hvor andre mennesker potentielt kan se ens skærm. Det er der kun 11 % af offentligt ansatte, der gør, viser analysen.Se denne korte film om at arbejde på farten, som indeholder tre gode råd. Filmen varer kun et par minutter.[LINK TIL FILM]  |
| **Uge 4: Fortrolige og personfølsomme oplysninger** |
| Kære kollegaHar du styr på, hvordan du opbevarer og sender fortrolige og personfølsomme informationer? Vi runder den nationale cybersikkerhedsmåned af ved at rette blikket mod håndteringen af følsomme oplysninger.**Hvad skal jeg være opmærksom på?**Håndteringen af fortrolig og personfølsom information handler bl.a. om at beskytte informationer, når du printer og har papirer liggende på skrivebordet, og hvordan du sender og modtager informationer. Analysen Danskernes Informationssikkerhed viser, at 20 % af offentligt ansatte bryder GDPR-regler og har oplysninger, fx CPR-numre, liggende derhjemme. Heldigvis viser den også, at der er fremgang på mange fronter, fx er der flere, der husker at sende fortrolige oplysninger på krypteret mail. **Hvordan kan jeg styrke mine vaner?**Du kan starte med at lære dig selv en simpel vane, nemlig altid at låse skærmen, når du går væk fra din computer: Brug genvejstasterne Windows + L. Og så kan du se denne korte film med gode råd til at håndtere fortrolige og personfølsomme oplysninger. Den varer kun et par minutter.[LINK TIL FILM] |