CYBERMISSION 1

CYBER AWARENESS

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR UNDERVISNING OG KVALITET

CYBER SKILLS

CYBERMISSION 1 - CYBER AWARENESS

Design:
Børne- og
Undervisningsministeriet

Børne- og Undervisningsministeriet
Styrelsen for It og Læring
Vester Voldgade 123
1552 København V

CYBERMISSION 1 - CYBER AWARENESS

Mange unge oplever, at de har godt styr på deres adfærd på nettet, at de ved, hvad de skal sige ja og nej til, hvad de skal undgå at klikke på og hvad de generelt skal undgå af fælder - måske tænker du det samme?

Men flere undersøgelser viser, at mange ikke altid gør det, de godt ved, de burde gøre i forhold til datasikkerhed.

Det er faktisk ikke kun unge, der mangler viden om datasikkerhed og har brug for en bedre digital adfærd. Det er også et af de områder, som er i fokus hos danske virksomheder: At styrke medarbejdernes viden om, hvordan man agerer sikkert på nettet.

Den udfordring skal I hjælpe med at løse!

IT-SIKKERHED ER MEGA COOL!

De it-løsninger, vi bruger til dagligt, skal helst bare virke, gerne hurtigt, allerhelst uden bøvl og alt for mange krav når man skal oprette konti, logge ind osv. Men sikkerhed betyder også, at det nogle gange bliver besværligt.

For mange er det svært at forstå, hvor stor faren er på nettet, når vi bruger digitale løsninger. Vi kan nemlig ikke altid se de konsekvenser, "små handlinger" kan lede til.

It-sikkerhed er et vigtigt område, der skal mere fokus på, og det er det, I skal arbejde med på denne mission. På denne mission bliver I mestre i god digital adfærd, og så skal I overbevise andre om, at de også skal være opmærksomme på deres it-sikkerhed!

JERES MISSION

I jeres gruppe skal I udvikle en kommunikationskampagne, der henvender sig til målgruppen unge i alderen 15-25 år. I må gerne snævre målgruppen endnu mere ind.

I det følgende finder I tre aktuelle temaer, som kan være omdrejningspunktet for jeres kommunikationskampagne. I kan bruge én eller flere eller selv komme på en tematik. Det vigtigste er, at kommunikationskampagnen kan forbedre målgruppens digitale adfærd - med fokus på it-sikkerhed. Når I har lavet en kampagne, skal I også forberede en kort præsentation, hvor I fortæller om tankerne bag.

TEMA 1

STYRK DIT PASSWORD

I skal få målgruppen til at lave bedre passwords og passe godt på dem.
De fleste laver forudsigelige passwords, der er lette at gætte/hacke, bruger det samme password til facebook og e-mail m.m. og deler det også med andre, når de eksempelvis låner deres Netflix-konto ud.

TEMA 2

HUSK AT LÅSE DIN COMPUTER

I skal få målgruppen til altid at låse deres computer, når de forlader den.
Hvor tit har I ikke forladt jeres plads uden at låse jeres computer? Det sker alt for tit, og I skal derfor gøre målgruppen opmærksom på, at de skal låse deres computer, så andre ikke får adgang til information, der ikke vedkommer dem.

TEMA 3

UNGÅ AT BIDE PÅ "PHISHING-KROGEN"

I skal lære målgruppen ikke at klikke på links i mails, som de ikke har tillid til.
En phishingmail er, hvor en hacker forsøger at franarre (fiske) éns personlige oplysninger som eksempelvis passwords. De prøver at lokke en til at klikke på et link i en mail, hvorefter de kan se de oplysninger, man indtaster. I skal derfor lære målgruppen at genkende phishingsmails, så de ikke ryger på krogen.

KAMPAGNENS FORMAT

I bestemmer selv, hvordan kommunikationskampagnen skal udformes. Den kan se ud på mange måder og I kan finde inspiration i listen her:

- SoMe-kampagne
- Informationsmail
- Film (el. et storyboard til en film)
- Podcast
- Et event (lav evt. en drejebog for et event)
- Quiz
- Plakat
- Pjecer

Overvej hvordan I kan lave budskabet sjovt, anderledes, kreativt og/eller nytænkende. Det er vigtigt, at kampagnen får målgruppen til at stoppe op en ekstra gang - og rent faktisk ændrer deres digitale adfærd. I kan med fordel tænke på situationer og scenarier, som målgruppen let kan relatere til.

Der forventes ikke et helt færdigudviklet produkt. Hvis I synes, I kommer bedst igennem med jeres budskab ved at lave et event, skal I ikke afholde et event, men I kan eksempelvis lave en drejebog for et event med et program, indholdspunkter mm.

GODE RÅD TIL KAMPAGNEUDFORMING

Når I skal i gang med at lave selve kampagnen, er det en god ide at starte med at finde ud af, hvilket budskab I vil kommunikere, hvilken adfærd I ønsker at ændre og hvem I kommunikerer til. Her kan I med fordel undersøge lidt mere om emnerne og måske også få inspiration fra andre.

Derudover kan I få hjælp i diverse kommunikationsmodeller. Hvis ikke I allerede har arbejdet med nogen i undervisningen, kan I bruge de to modeller, som er beskrevet i det følgende. Det er "Argumentationsanalysen" og "Kommunikationsmodellen".

Modellerne kan hjælpe jer i de valg, I træffer, når I udformer jeres kommunikationskampagne.

"OFTEST ER DET HELT BASALE MENNESKELIGE FEJL, DER GØR AT EN VIRKSOMHED UDSÆTTES FOR DATABRUD."

MODEL 1: ARGUMENTATIONSANALYSEN

I argumentationsanalyse skelner man mellem tre appelformer, der beskriver, hvordan man taler til modtageren på tre forskellige måder: Logos, etos og patos

Når man arbejder med budskaber, er det en god ide at overveje sin appelform.

I jeres præsentation skal I redegøre og argumentere for, hvordan I bruger de forskellige appelformer i jeres kommunikation. I kan sagtens anvende flere appelformer.

ETOS

Etos som appelform handler om at skabe troværdighed omkring afsenderen på baggrund af en person og hans eller hendes værdier. Hvis modtageren har tillid til afsenderen, er man oftest mere tilbøjelig til at give afsenderen ret i vedkommendes synspunkter og budskaber.

LOGOS

Denne appelform handler om at overbevise modtageren via en saglig og rationel argumentation. Man taler til modtagerens fornuft for at få dem til at indse rigtigheden af afsenderens synspunkter eller teorier. Logos bygger på fakta, tekstbelæg, statistikker og tal, altså dét som kan måles og dokumenteres.

PATOS

Denne appelform henvender sig til modtagerens følelser. Når afsenderen benytter patos som appelform, forsøger man at vække følelser som glæde, ophidselse, frygt, medlidenhed eller vrede hos modtageren for på den måde at overbevise ham eller hende om sit synspunkt.

MODEL 1

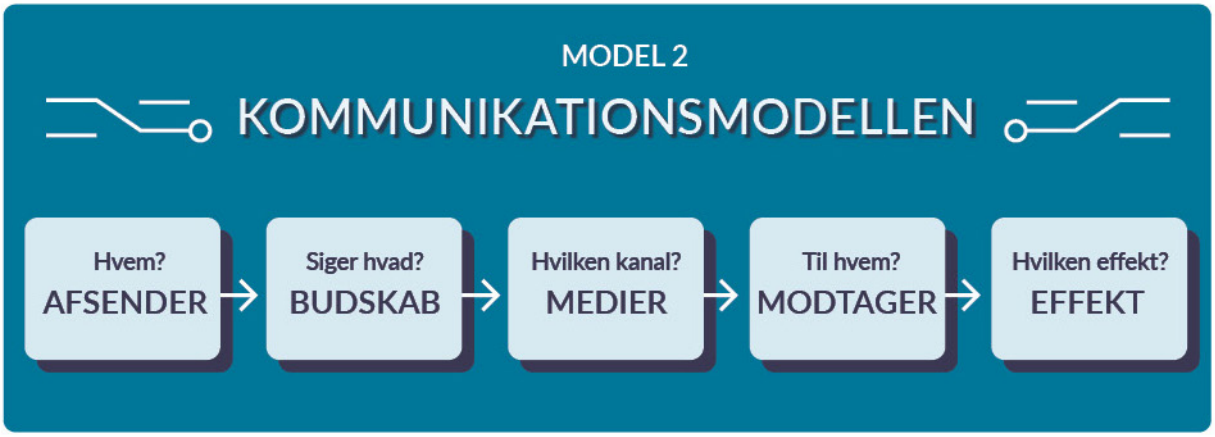
ETOS, LOGOS OG PATOS

TYPE	ETOS	LOGOS	PATOS
BETYDER	Når han/hun gør det, må det være godt	Tal, data, videnskabelige beviser Det logiske, det der tilsyneladende ikke kan sættes spørgsmålstegn ved	Gør det for min skyld Følelsestale
EKSEMPEL	"Fordi jeg siger det ..."	"Hvis du gør sådan sker der det og det ..." "70% af den danske befolkning ville gøre sådan..."	"Jeg bliver skuffet hvis du ikke gør det ..."

MODEL 2: KOMMUNIKATIONSMODELLEN

Kommunikationsmodellen, som I kan se herunder, består af fem faser, og kan hjælpe én, når man skal overveje sit budskab, udformning af budskabet, hvordan man vælger at kommunikere det samt om man via sine valg opnår den ønskede effekt.

I kan bruge kommunikationsmodellen til at beskrive jeres kampagne. I må gerne erstatte modellen med andre modeller, som I har kendskab til, og som I måske synes er bedre.



AFSENDER - Hvem?

"Hvem er det som siger noget?"
Afsender er den, der vil kommunikere et givent budskab.

BUDSKAB - Siger hvad?

"Hvad bliver der sagt?"
Afsenderens budskab er det, som han eller hun ønsker at kommunikere til modtageren.

MEDIE - I hvilken kanal?

"Hvordan og hvor bliver det sagt?"
Medie er den kanal, der bruges til at formidle budskabet (det kan være alt fra en fysisk plakat, et nyhedsbrev, en kampagne på sociale medier osv.).

MODTAGER - Til hvem?

"Hvem bliver det sagt til?"
Modtageren er den person, afsenderen vil sende sit budskab til.

EFFEKT - Med hvilken effekt?

"Hvad hører modtageren der bliver sagt?"
Modtagerens afkodning af budskabet og en analyse af, hvordan modtager bliver påvirket af afsenderens meninger/budskab.

INSPIRATION

Inden I går i gang med at lave kommunikationskampagnen, kan I starte med at se disse tre videoer, som er lavet sammen med nogle super dygtige folk, der arbejder med kommunikation og it-sikkerhed til daglig. De vil hjælpe jer til at forstå missionen, og I får nogle gode tips til stærke budskaber. Videoerne varer mellem 8-12 minutter.
Videoerne til **CYBERMISSION 1 - CYBER AWARENESS** finder I her: https://cybermissionen.cyberskills.dk/mission-1/

Video 1)
Cybersecurity Awareness - Hvem beskytter vi os mod?

Video 2)
Tips og tricks til gode cyber awareness kampagner

Video 3)
Når budskaber skal fange

JERES PRÆSENTATION

I skal forberede en præsentation af jeres kommunikationskampagne, hvor I redegør for missionen, fortæller om jeres proces med at finde frem til jeres løsning samt præsenterer selve løsningsforslaget.

I præsentationen skal I:

- Redegøre for jeres mission og den tematik, I har valgt at fokusere på
- Fortælle, hvordan I kom frem til jeres endelige løsningsforslag
- Præsentere jeres kommunikationskampagne (gerne med billeder, video m.m)
- Fortælle, hvordan I har anvendt analyseredskaber ex. argumentationsanalysen eller kommunikationsmodellen
- Argumentere for, hvilken effekt I tror, at jeres kampagne kan få hos jeres målgruppe.

Præsentationen skal have karakter af et kort pitch, ligesom det de laver i Løvens Hule, og må max tage 10 minutter.

DELTAG I EN NATIONAL KONKURRENCE

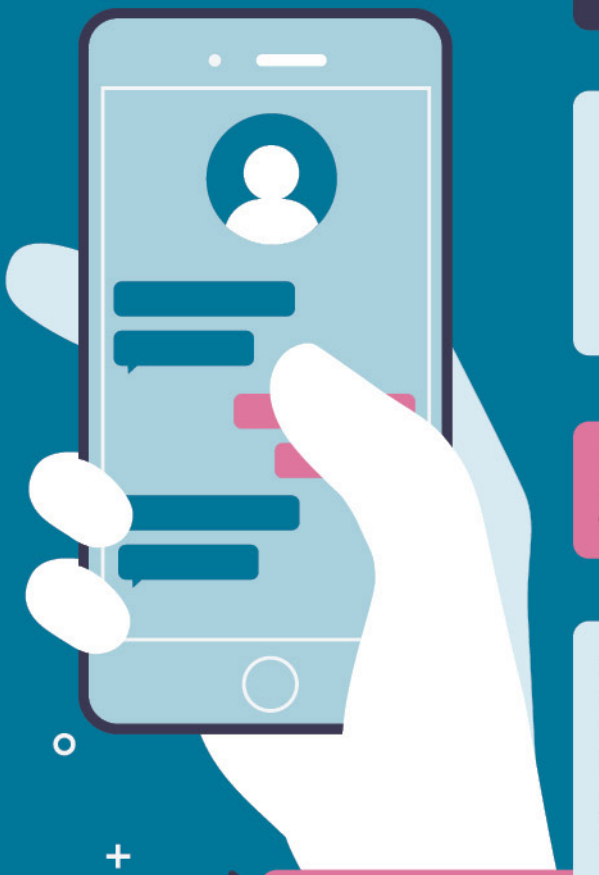
Cybermissionen er en national konkurrence, hvor alle ungdomsuddannelser har mulighed for at være med. Alle klasser må deltage i konkurrencen med ét løsningsforslag. Man deltager i konkurrencen ved at lave en videooptagelse af sin præsentation og sende den ind til Styrelsen for It og Læring. Alle videoer vurderes af Cybermissionens dommerpanel.

Videoen skal uploades af den underviser, som har tilmeldt jer Cybermissionen. I finder link til uploadfunktionen på konkurrencens hjemmeside: https://cybermissionen.cyberskills.dk, hvor I kan læse mere.

CYBERMISSIONEN

BEGREBSLISTE

Hvor mange begreber kender I?



INCOGNITO / PRIVAT BROWSER

Når du sætter din browser i 'inkognito' gemmes dine indtastninger ikke i din browser eller lokalt på din computer. Men hjemmesider, din skole eller internetudbyder kan stadig se din aktivitet.

COOKIES

En cookie er en fil, der bliver gemt på din computer, når du besøger en hjemmeside. Nogle cookies er nødvendige for at hjemmesiden virker, andre husker hvad du klikker på, så hjemmesiden kan sende reklamer, som passer til dig. Når du besøger en hjemmeside, kan du vælge hvilke cookies du vil acceptere.

CYBER AWARENESS

Mange virksomheder laver cyber awareness træning. Det kan eksempelvis være kommunikationsaktiviteter eller uddannelse, der skaber opmærksomhed om informationssikkerhed hos medarbejderne, så de får en mere sikker digital adfærd.

DIGITALE FODSPOR

Når du søger på Google, sender en snap eller uploader en video på TikTok efterlader du dig spor på nettet, som bliver gemt. Det kaldes digitale fodspor, og de kan være meget svære at slette igen.

HACKING

Hacking er, når nogen ulovligt skaffer sig adgang til andres data - eksempelvis via en computer. Hackere udnytter svagheder i systemer. En svaghed kan eksempelvis være passwords, der er nemme at gætte.

DDOS-ANGREB

DDos-angreb står for Distributed Denial of Service. Det er et digitalt angreb, hvor en hacker med vilje overbelaster en hjemmeside eller en it-service, så siden i en periode er utilgængelig eller bryder helt sammen. Angrebet udføres ved, at hackeren gennem et netværk af virusinficerede computere, et såkaldt botnet, sender en stor mængde forespørgsler til hjemmesiden og dermed får siden til at bryde sammen.

GDPR

GDPR står for General Data Protection Regulation og er en lov, som er indført af EU for at passe på dine og alle andres data og personoplysninger.

TO-FAKTOR LOGIN

To-faktor login er en dobbelt lås, som typisk består af dit password og en kode, du får tilsendt - ofte på sms. Hvis andre får fat i dit brugernavn og password og forsøger at logge ind på din konto, kan det derfor ikke lade sig gøre, fordi de mangler den anden kode, som er sendt til din mobil.

MALWARE

Malware bruges om ondsindet software - fx virus eller andet, der skader din computer.

RISIKOANALYSE

En risikoanalyse er et værktøj, som har til formål at afdække potentielle risici ved at kategorisere dem ift. den mulige konsekvens og sandsynlighed for, at de indtræffer. Risikoanalysen anvendes dernæst til at prioritere ressourcer og beslutte hvilken handling, der skal sættes ind for at sikre, at det ikke går galt.

PHISHING

'Phishing' er, når it-kriminelle bruger falske e-mails, links eller hjemmesider til at få fat i andres private oplysninger, eksempelvis til banken. Det er tit svært at se forskel på, hvad der er falske links, mails og hjemmesider, og hvad der er ægte.

Kan I finde flere ord?

BØRNE- OG UNDERVISNINGSMINISTERIET
STYRELSEN FOR IT OG LÆRING
CYBER SKILLS