Lærervejledning til ultra:bit-forløbet

CYBERTRUSLEN I DANMARK

Trin: 7.-9. klasse

Fag: Samfundsfag og teknologiforståelse

Antal lektioner: 4

INDHOLD

OBS. Inden du printer denne vejledning ud, så vær opmærksom på, at den indeholder hyperlinks, som kun kan tilgås digitalt.

LEKTIONSTABEL

	Delforløb 1	Delforløb 2	Delforløb 3	I alt
Antal lektioner	1 lektion	1 lektion	2 lektioner	4 lektioner

FÆLLES MÅL

Find Fælles Mål og læringsmål for samfundsfag HER.

Find Fælles Mål for forsøgsfaget teknologiforståelse HER.

OM FORLØBET

Danmark er et af de mest digitaliserede samfund i verden. Vi har effektiviseret mange processer for eksempel vores sundheds- og betalingssystem, men det har også gjort os sårbare overfor cyberangreb - både for os som privatpersoner og som land. I dette forløb skal I gå i dybden med, hvordan vi kan blive ramt af forskellige cybertrusler, og hvilke konsekvenser det har for borgerne og for samfundet.

Forløbet er henvendt til udskolingseleverne i samfundsfag, men det kan også bruges i forsøgsfaget teknologiforståelse.

'Cybertruslen i Danmark' består af tre delforløb. I kan arbejde med delforløbene i kronologisk rækkefølge eller udvælge de delforløb, der passer ind i jeres undervisning.

Her er en kort beskrivelse af hvert delforløb.

DELFORLØB 1 - HVORDAN FORSØGER HACKERNE AT ANGRIBE DIG?

Find elevsiden til delforløbet HER.

Nogle af dine elever ved sikkert allerede godt, at de ikke skal give deres kontooplysninger til ukendte arvinger eller klikke på links, de får tilsendt fra mystiske profiler på Instagram. Men hackernes metoder udvikler sige hele tiden. I dette delforløb skal I dykke ned i deres udspekulerede metoder.

Klasseaktivitet: Introduktion

- Video: 'Hacker smadrer 7.B's telefoner' (varighed 06:21 min.).
- Gruppearbejde: Arbejdsspørgsmål til videoen.
- På klassen: Saml op på gruppeopgave.

NOTE: Om I vælger at tage arbejdsspørgsmålene til videoen i grupper eller på klassen er op til dig.

Tip til gruppeopgave

Du kan med fordel dreje samtalen ind på, om eleverne har fået mere eller mindre tillid til at færdes på nettet. Om de selv har haft lignende oplevelser, som har lært dem noget, og som eventuelt har fået dem til at ændre adfærd og være mere på vagt. Sådan en samtale kan give dem et godt udgangspunkt, når de senere hen skal arbejde med cyberangrebenes konsekvenser for samfundet i delforløb 3.

Elevopgave: Hackernes metoder

- Tekst: Kort intro om cyberangreb mod danske borgere.
- Billedserie: Hackernes metoder.
- Quiz: 'Klik eller klik ikke'

NOTE: Find mere viden om hackernes metoder HER.

Ekstra elevopgave: Lav et quizspørgsmål

- Produkt: Eleverne laver en grafisk fremstilling af et quizspørgsmål til deres målgruppe.

DELFORLØB 2 - DE FEM CYBERTRUSLER DER KAN RAMME DANMARK

Find elevsiden til delforløbet HER.

I delforløb 2 bliver eleverne klogere på de fem forskellige typer af cybertrusler, som kan ramme Danmark.

Delforløbet indeholder:

Elevopgave: Læs om de fem cybertrusler

- Tekst: Kort intro om cybertruslen i Danmark.
- Billedserie: De fem forskellige cybertrusler.
- På klassen: Spørgsmål til billedserien.

Billedserie

I billedserien fremgår det aktuelle trusselsniveau anno 2021 for de fem forskellige typer af cybertrusler. Her kan du se en uddybning af trusselsniveauerne:

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

Kilde: Cybertruslen mod Danmark 2021, Center for Cybersikkerhed (side 21)

Elevopgave: Fem eksempler

- Klipsamling: Fem klip der viser, hvordan danske virksomheder og myndigheder er blevet ramt af cyberangreb (varighed i alt 08:06 min).
- Gruppeopgave: Arbejdsspørgsmål til klipsamlingen.
- På klassen: Opsamling og fremlæggelse.

NOTE: Det er op til jer selv, om I vælger at tage arbejdsspørgsmålene til klipsamlingen i grupper eller på klassen.

Find svaret på arbejdsspørgsmålene til hvert klip HER.

Tip til gruppeopgave:

I det sidste arbejdsspørgsmål kan du med fordel dreje samtalen ind på, om eleverne har tillid til, at de offentlige myndigheder er rustet godt nok til at kunne passe på vores samfundsvigtige funktioner og borgernes personlige data. Sådan en samtale kan give dem et godt udgangspunkt, når de senere hen skal arbejde med cybertruslernes konsekvenser for samfundet i delforløb 3.

Forslag til lektie inden delforløb 3:

Genstart: Afsnittet 'The DarkSide' (varighed: 23 min.) giver en god fælles referenceramme, inden i påbegynder delforløb 3. Genstart er DR's nyhedspodcast.

Om afsnittet:
Podcastafsnittet handler om et stort cyberangreb på USA's største olieledning begået af hackergruppen 'The DarkSide'. Afsnittet giver et godt indtryk af, hvilke konsekvenser et stort hackerangreb kan have for borgerne og samfundet.

Find den HER.

DELFORLØB 3 - HVORDAN KAN SAMFUNDET BLIVE RAMT?

Find elevsiden til delforløbet HER.

Delforløb 3 sparkes i gang med en video, hvor eleverne møder professor i cybersikkerhed Jens Myrup Pedersen fra Aalborg Universitet. Han fortæller om, hvilke konsekvenser cyberangrebene kan have i dag ('økonomiske' og 'politiske') og i fremtiden ('et samfund der går i stå' og 'mistillid'). Videoen indeholder svære ord og sammenhænge, så derfor kan eleverne støtte sig op af ordbogen på elevsiden, der uddyber nogle af de svære begreber.

Delforløbet indeholder:

Klasseaktivitet: Cyberangrebenes konsekvenser

- Video: Cyberangrebenes konsekvenser (varighed 04:08 min.).
- Ordbog: Find ordforklaringer på svære ord fra videoen
- På klassen: Spørgsmål til videoen

Video: Didaktisk tip

Du kan overveje at gøre følgende:

1. Start med at se videoen i sin helhed første gang.
2. Del herefter eleverne op i grupper.
3. Eleverne snakker i gruppen om, hvad de forstod, og hvad de ikke forstod og derfor godt kunne tænke sig at få uddybet lidt mere.
4. Hver gruppe vælger en elev. Elevens opgave bliver at række en hånd i vejret under anden afspilning af videoen ved de steder, hvor gruppen gerne vil have noget uddybet.
5. Se videoen igennem for anden gang
6. Stop videoen, når en elev rækker hånden i vejret.
7. Uddyb og opklar misforståelser. Støt dig eventuelt op af ordbogen på elevsiden.

Elevopgave: En fiktiv case

- Gruppearbejde: Arbejd med to cases (find dem sidst i lærervejledningen)
- Klipsamling: Hjælpeklip
- På klassen: Opsamling og fremlæggelse.

NOTE: Sidst i lærervejledningen finder du de to printbare-cases. 'Hospitalet der gik i sort' og 'Banken der gik i stå'. Det er op til dig, om I vælger at tage en eller to cases på klassen eller i grupper. Bemærk, at der til hver case er to hjælpeklip. Du finder hjælpeklippene på elevsiden.

Afrundende elevopgave: Tre gode råd

- Video: Gense videoklippet 'Hackere smadrer 7.B's telefoner' (delforløb 1)
- Produkt: Lav en fysisk plakat med tre gode råd om cybersikkerhed

Case 1: Hospitalet der gik i stå

LÆS: I 2026 er det lykkedes en gruppe kriminelle hackere at hacke et stort dansk hospital. Lægerne kan nu ikke længere få adgang til patienternes sundhedsoplysninger. Der opstår kaos på hospitalet. Dagens patienter strømmer ind, men hvem skal opereres for hvad, og hvem skal tale med hvilken læge? Alle ikke akutte operationer og konsultationer bliver derfor aflyst på ubestemt tid. Hackerne kræver 100 millioner kroner for at stoppe angrebet. De truer sågar med at lække patientjournaler offentligt, hvis de ikke snart får deres penge.

SE de to hjælpe-klip i klipsamlingen:

- CASE 1 – Britiske hospitaler hacket (01:11 min)
- CASE 1 - Hospitalspatienter reagerer på hackerangreb (00:56 min)

SVAR på spørgsmålene:

1. Hvordan vil det påvirke din hverdag, hvis det skete i virkeligheden?
2. Hvordan vil det ramme borgerne, virksomhederne og de danske myndigheder?
3. Hvilke konsekvenser vil sådan et cyberangreb have? (I kan bruge de fire konsekvenser, I kender fra videoen med Jens Myrup Pedersen)

Case 2: Banken der gik i stå

LÆS: I 2028 er det lykkedes en gruppe kriminelle hackere at hacke alle banker i Danmark. Alle kontoer og hæveautomater bliver låst, og det er nu ikke muligt at lave digitale overførelser ind og ud af bankerne. Kunderne kan altså ikke længere hæve penge, bruge deres betalingskort eller mobilepay i butikkerne eller på nettet. Kun kontantbetaling virker. Hackerne kræver 100 millioner kroner for at stoppe angrebet. De truer sågar med at bytte rundt på bankkundernes kontoer, så der ikke er længere, er styr på, hvem der har hvor mange penge på hvilken konto.

SE de to hjælpe-klip i klipsamlingen:

- CASE 2 – Danske banker ruster sig mod hackerangreb (01:44 min)
- CASE 2 – Danskerne bruger færre kontanter (01:15 min)

SVAR på spørgsmålene:

1. Hvordan vil det påvirke din hverdag, hvis det skete i virkeligheden?
2. Hvordan vil det ramme borgerne, virksomhederne og de danske myndigheder?
3. Hvilke konsekvenser vil sådan et cyberangreb have? (I kan bruge de fire konsekvenser, I kender fra videoen med Jens Myrup Pedersen)