A picture containing diagram

Description automatically generatedImmagine che contiene testo, clipart

Descrizione generata automaticamenteLogo

Description automatically generated

Text

Description automatically generated



**DIGITALT MEDBORGERSKAP**

**MODUL**

**ENHET 10: DIGITAL SIKKERHET**

|  |
| --- |
| ***SAMMENDRAG AV MODULEN*** |
| I løpet av denne modulen vil elevene bli introdusert fordigital sikkerhet. Elevene vil kunne absorbere viktigheten av digital bevissthet i våre liv og også i utdanning. De vil kort vite om **digital sikkerhetstips hjemme og på skolen.** |

INNHOLDSFORTEGNELSE

* Definisjon av digital sikkerhet 3
* Eksempler på hensiktsmessig og upassende digital sikkerhet 3
* Hvorfor er digital sikkerhet viktig i utdanning? 4
* Hva er digital sikkerhetsbevissthet for studenter? 5
* Hvorfor er bevissthet om digital sikkerhet viktig?
* **12 digitale sikkerhetstips for elever hjemme og på skolen 7,8,9**
* Evaluation spørsmål 10
* Referanser 11

DEFINISJON

**Digital sikkerhet er de elektroniske forholdsreglene for å garantere sikkerhet.**

**Etter hvert som flere og flere personlige opplysninger blir lagret elektronisk, er en strategi for å beskytte informasjonenavgjørende.  Folk trenger å lære å beskytte seg selv når de fortsetter å bruke teknologiske enheter. I likhet med å beskytte seg selv hjemme, må enkeltpersoner finne måter å sikre personlige elektroniske data (for eksempel ved hjelp av virusbeskyttelsesprogramvare, opprette brannmurer og lage sikkerhetskopier**)  **(weebly.com)**

**Eksempler på upassende digital sikkerhet**  
**- Brukere klarer ikke å opprettholde gjeldende programvareoppdateringer eller oppdateringer som beskytter datamaskinene mot  
  
virus og forklaring.**  **Brukere klarer ikke å beskytte sin identitet når de bruker e-post, sosiale nettverk eller tekstmeldinger.**



**EKSEMPLER PÅ PASSENDE DIGITAL SIKKERHET -   
  
Brukere tar seg tid til å sørge for at virusbeskyttelsen og brannmurene er riktig udatert og konfigurert for å beskytte personlig informasjon.-Lærere og foreldre snakker med elevene om farene ved å gi informasjon til alle over internett.**  **(weebly.com)**

**HVORFOR ER DIGITAL SIKKERHET VIKTIG I UTDANNING?**

Betydningen av [digital sikkerhet i utdanning](https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/) Institusjoner øker stadig. Utviklingen av datamaskiner og internett har gjort livet enklere for folk i utdanningsinstitusjoner så vel som i andre institusjoner.

Det har også gitt utdanningsinstitusjoner mulighet til å være mer effektive i sin virksomhet.

Men det er også et faktum at den samme teknologien som gjør livet enklere for folk, også kan gjøre livet surt hvis det misbrukes.

Internett og datamaskiner har blitt en viktig del av hverdagen vår, uansett om vi jobber eller studerer hjemme eller på skolen eller høyskolen eller til og med på arbeidsplassen.

Det er derfor veldig viktig å holde datamaskinene sikre mot hackere, slik at personopplysningene til studenter, ansatte og lærere ikke blir misbrukt av skruppelløse mennesker som kan være interessert i å skaffe seg konfidensiell informasjon om studenter / ansatte / lærere uten deres viten for å bruke den mot dem senere. (James K., 2022)





[Betydningen av digital sikkerhet](https://cybersecurityforme.com/importance-of-cybersecurity-in-the-us/) i utdanningsinstitusjoner kan ikke overvurderes fordi informasjonsteknologi spiller en viktig rolle i utdanningsinstitusjoner.

Det er derfor svært [viktig å sikre datamaskiner og internett](https://cybersecurityforme.com/importance-of-cybersecurity-in-the-internet-age/) fra uautoriserte personer, slik at informasjonen som er en verdifull ressurs for enhver utdanningsinstitusjon, forblir sikker.

Vi bør ikke glemme at informasjonsteknologi har gjort utdanningsinstitusjoner mer effektive og effektive i sin virksomhet.

Derfor er det veldig viktig å sikre cybersikkerhet i utdanningsinstitusjoner slik at vi kan dra full nytte av denne teknologien. (James K., 2022)

**HVA ER DIGITAL SIKKERHETSBEVISSTHET FOR STUDENTER?**



[Digital sikkerhet er et voksende felt](https://cybersecurityforme.com/women-in-cybersecurity-field/) i utdanningsverdenen. Med så mange studenter som får tilgang til internett på daglig basis, er det mange muligheter for nettkriminelle å stjele passord eller personlig informasjon.

Digital opplæring i sikkerhetsbevissthet er viktig fordi den lærer elevene hvordan de kan beskytte seg mot cyberangrep. Studentene vil lære om phishing-svindel, skadelig programvare, ransomware og andre datamaskintrusler.

Dette er helt nødvendig for at skolene skal holde elevene trygge. Skoler må beskytte seg mot hackere ved å installere [brannmurer](https://cybersecurityforme.com/firewall-security/), beskyttelse mot skadelig programvare og annen beskyttelse.

Skolen må sørge for at alle enhetene som er koblet til Wi-Fi-nettverket, er sikret med sterke passord.

Lærere kan undervise i digital sikkerhet i klasserommet, eller foreldre kan undervise i det hjemme.

Digital sikkerhetsbevissthet for studenter inkluderer også å lære dem å være klar over truslene og risikoene som følger med bruk av teknologi. Det lærer dem også hvordan de skal bruke teknologi trygt og ansvarlig.

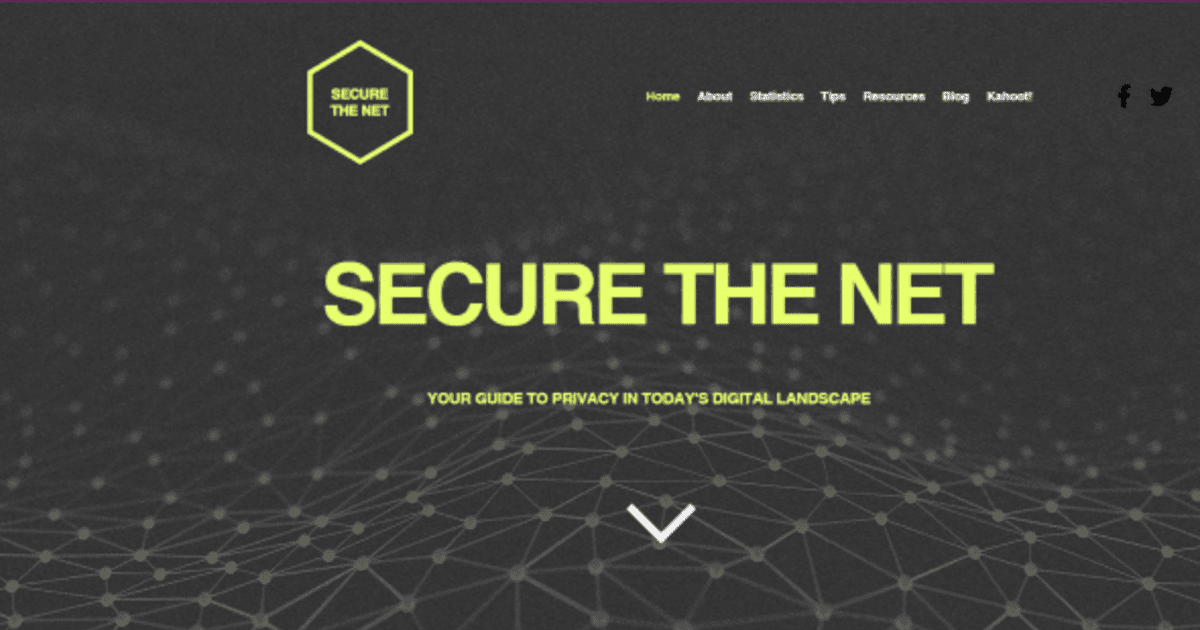
Det er viktig at barn får en trygg måte å utforske verden på uten frykt for å bli angrepet på nettet. (James K., 2022)

### HVORFOR ER DIGITAL SIKKERHETSBEVISSTHET VIKTIG?

Internett har gjort informasjon allment tilgjengelig for publikum til enhver tid, noe som både er en velsignelse og en forbannelse. Det er avgjørende for alle typer virksomheter, inkludert utdanningsinstitusjoner.

Personvernlovgivningen har definert personlig informasjon som en viktig ressurs som ikke kan handles eller selges uten samtykke. Hvis denne informasjonen faller i feil hender, kan det føre til identitetstyveri som skaper alvorlige langsiktige konsekvenser.

Når det gjelder utdanning, betyr dette at det er mange muligheter for studenter å få tilgang til kursmateriell på nettet - men også flere farer.

Bevissthet om cybersikkerhet er av avgjørende betydning fordi det kan hjelpe oss med å identifisere potensielle trusler før de skjer. Det gir oss også den kunnskapen som er nødvendig for å beskytte oss mot ondsinnede nettsteder eller angrep. På grunn av det er det den eneste måten å [beskytte utdanningsinstitusjoner mot](https://cybersecurityforme.com/measures-to-protect-your-network-from-cyber-criminals/) cybertrusler. En av de viktigste aspektene ved å beskytte en institusjon mot cyberangrep er bevissthet, slik at studenter og ansatte vet hva de trenger å gjøre for å beskytte seg selv.

Programmer for bevissthet om digital sikkerhet bør være obligatorisk i skolen, slik at alle kan lære å holde seg trygge på nettet. De fleste hackere er motivert av utfordringen og ikke den økonomiske belønningen.

Hvis en hacker kan få oppmerksomheten din, kan de komme inn i systemet ditt. Det finnes også terrorgrupper som hacker seg av ideologiske grunner.

Disse gruppene har vært kjent for å målrette eller i det minste vise interesse for skoler og høyskoler. Ved å være klar over hvordan hackere fungerer, kan du unngå fellene deres og beskytte dataene dine mot dem.

Når det gjelder cybertrusler, kan det du ikke vet skade deg. Skoler er et av de mest sårbare målene for cyberangrep fordi de har store nettverk av datamaskiner og ofte ikke håndhever nødvendige protokoller.

Utdanningsinstitusjoner må håndheve strengere retningslinjer for å sikre studentenes sikkerhet.

Å utdanne deg selv og dine ansatte om farene ved skadelig programvare, phishing-svindel, ransomware-angrep og mer gir deg kunnskapen og verktøyene som trengs for å unngå å [bli en annen](https://cybersecurityforme.com/how-to-become-a-cybercrime-investigator/) nettkriminalitetsstatistikk. (James K., 2022)

## ****12 DIGITALE SIKKERHETSTIPS FOR ELEVER HJEMME OG PÅ SKOLEN****

### ****1. Sikre dine sosiale medier****

Instagram, Twitter og Facebook lar deg oppdatere foreldre og elever på en morsom og engasjerende måte. For å fortsette trygt må du imidlertid gå gjennom personverninnstillingene for hver konto for å beskytte personvernrettighetene til studentene dine. Vit hvem som kan se hva og hvilken plattform som deler hvilke data og med hvem. Noen eksempler:

**Twitter**: Sett klasserommet Twitter-kontoen din til "beskyttet" slik at bare folk du følger kan se tweets.

**Facebook**: Gjør kontoen «Synlig for venner bare» i innstillingene for personvernkontroll.

**Gjør elevenes ansikter uskarpe**: Med mindre du har forhåndstillatelse til å bruke bildene deres i innleggene dine, kan det hende du bryter personvernrettighetene til elever og foreldre. Bruk en gratisapp til å gjøre elevenes ansikter uskarpe og annen informasjon som kan avsløre identiteten deres.

### ****2. Bruk apper, verktøy og nettsteder som krypterer data****

Kryptering sikrer og beskytter alle data du sender på nettet fra hackere, nettverkssnokere og tredjeparter.

**Bruk krypterte nettsteder**: Bruk bare nettsteder med 'http**s**' i nettadressen og et hengelåsikon ved siden av. 'S' står for 'sikker' (kryptert), noe som betyr at data lekket eller innhentet av uautoriserte parter er ubrukelige.

**Sjekk personvernreglene for apper**: iOS-apper tvinger alle brukere til å kommunisere via https, men det samme kan ikke garanteres for Android-apper. Det er best å enten sjekke personvernreglene for hvert verktøy eller inspisere nettstedet for et offisielt stempel fra en databeskyttelsesorganisasjon.

Classtime, for eksempel, har signert California Student Privacy Alliance-avtalen. Hvis en app eller et nettsted er dekket av **COPPA** (Children's Online Privacy Protection Act), vil strenge datasikkerhetstiltak allerede være på plass.

### ****3. Ha en gjenopprettingsplan****

**Informere foreldre**: Feil skjer. Du kan ved et uhell ha fanget en elevs navn eller adresse i et bilde du har lagt ut på sosiale medier, eller det kan være et utbredt brudd på personlig eller sensitiv informasjon. La foreldrene få vite om de vil bli informert via post eller e-post, og hvem vil gjøre det: vil det være noen fra IT-avdelingen eller andre ledende ansatte?

**Hva er planen?**Gi en klar oversikt over trinnene som vil bli tatt hvis et datainnbrudd noen gang oppstår. Vil studentene bli registrert i en identitetstyveritjeneste? Vil du hjelpe studentene med å sikre kontoene sine og tilbakestille passordene sine i etterkant (se trinn 5)? I tilfelle et brudd på selskapets data, kan skolen, distriktet eller studenten be om å få dataene sine slettet fra selskapets servere. Ulike typer brudd på personvernet vil kreve ulike løsninger.

## ****4. Bruk en VPN****

**For alle utdanningsrelaterte oppgaver:** Tilgang til institusjonens nettverk bør kreve en privat VPN-tilkobling. Den krypterer og beskytter dermed studentenes internettrafikk mot avskjærere som kanskje vil stjele passord. [Surfshark](https://surfshark.com/surfshark-review) er et eksempel på en VPN du kan vurdere.

**På offentlig Wi-Fi:** Offentlig Wi-Fi er usikret, noe som gjør det til et arnested for hackere. Et VPN sikrer offentlig Wi-Fi ved å kryptere tilkoblingen din. Dette gjør det mulig for eksterne studenter å jobbe fra kaffebarer, hjemme eller på hybelen uten å bekymre seg for at hackere fanger opp dataene deres.

### ****5. Bruk sterke og unike passord****

**Bruk en passordbehandling:** Det er millioner av stjålne brukernavn og passord som selges av nettkriminelle på det mørke nettet. Svake passord kan gjettes eller knekkes i millisekunder, og utsetter elevenes sensitive data. En passordbehandling er en app som genererer passord som ikke kan knekkes og fyller dem ut automatisk når du trenger dem. Mange passordholdere lagrer all legitimasjon i et kryptert hvelv, som bare du har tilgang til.

#### ****Hvordan lage et sikkert passord****

Råde elevene til å lage passord som er lange, komplekse og blandede. De skal nemlig være minst 8 tegn lange, ha en blanding av bokstaver, tall og spesialtegn, og være så meningsløse som mulig. I et brute-force-angrep prøver hackere kombinasjoner av millioner av ordbokord og tall per sekund til man får dem inn.

### ****6. Vær årvåken når det gjelder phishing-svindel****

**Skoler og universiteter som mål**: Studentdatabaser er en gullgruve av personlig studentinformasjon. En phishing-svindel er avhengig av at en medarbeider blir lurt til å svare eller klikke på en lenke i en falsk e-post eller tekstmelding for å spre skadelig programvare, stjele legitimasjon eller verre. Nettkriminelle har brukt student-e-post til å søke om falske lån, stjele identiteter og infisere hele nettverk, og krasje dem fullstendig.

**Forebygging**: Du kan vanligvis oppdage phishing-svindel ved å lese avsenderens adresse. For eksempel kan California Student Aid Commissions nettadresse www.csac.ca.gov vises som www.csac.ca. **com,** og de fleste av oss ville ikke være noe klokere. For å være på den sikre siden, be elevene sende en egen e-post til den aktuelle myndigheten og aldri klikke på lenker i COVID-19-tema e-post. Årvåkenhet er nøkkelen.

### ****7. Kjenn vilkårene****

Når du blir med på et nettsted, registrerer deg for en sosial mediekonto, laster ned en app - eller til og med bruker en app du allerede eier - vær oppmerksom på vilkårene du godtar ved å laste ned og / eller bruke den appen. En app du bruker til å skanne ansiktet ditt, kan for eksempel dele disse dataene kombinert med navn, nettleserlogg, kontaktinformasjon og mer for å representere en betydelig sikkerhetsrisiko for deg i fremtiden.

### ****8. Ikke del personlig informasjon****

Denne er ganske åpenbar, men den må gjentas: Ikke del personlig informasjon - eller i det minste være klar over nøyaktig hvem som kan lese (eller til slutt "finne ut") om hva. Det tar ikke mye av et informasjonsbrudd - en e-postadresse med et svakt passord eller ditt fulle navn og adresse - for å gjøre det mulig for noen som er villige til å bruke litt deduktiv resonnement og internettsøkferdigheter for å skape en trussel mot din identitet, økonomisk sikkerhet og mer.

Dette betyr også at det er usikkert å dele kontoer med venner - en Netflix-konto, for eksempel.

## ****Andre datasikkerhetstips for studenter og skoler****

### ****9. Oppdater apper og enhetsoperativsystemer****

### ****10. Behold (sikre) sikkerhetskopier av viktige filer eller databaser****

### ****11. Ikke bruk usikrede WiFi-kilder****

### ****12. Kjenn din kontekst og "nettverk" (fysisk og digital)****

For eksempel studenter: Kjenn dine spesifikke risikoer og sårbarheter (basert på bruk, alder, karrieremål osv.) Skoler: lære opp ansatte i skole- og distriktspolitikk. (Nordpass, 2022)





EVALUERING SPØRSMÅL

1. Hva betyr «digital sikkerhet» for deg?
2. Hva er eksempler på upassende digital sikkerhet?
3. Hvorfor er digital sikkerhet viktig i utdanning?
4. Kan du fortelle meg 2 måter å være trygg på nettet?
5. Er du klar over digital sikkerhet nok?

**Referanser**

<https://www.simplilearn.com/what-is-digital-security-article>

<https://mwhitmoredigitalcitizenship.weebly.com/digital-security.html>

<https://cybersecurityforme.com/importance-of-cybersecurity-in-education/#:~:text=Cybersecurity%20awareness%20training%20is%20important,schools%20to%20keep%20students%20safe>.

<https://www.teachthought.com/technology/cybersecurity-tips-for-students/>