sphero BOLT™

CYBERSECURITY LABS

Pædagogveileder

INNHOLD

INTRODUKSJON

Vårt stadig mer digitale samfunn gir verden til fingerspissene, og lar oss lære praktisk talt hva som helst, kommunisere og samarbeide med mennesker på den andre siden av kloden, og innovere løsninger på våre største utfordringer. Dessverre åpner den digitale verden oss for et helt nytt og skummelt sett med trusler. Etterspørselen har aldri vært større etter en robust cybersikkerhetsarbeidsstyrke og innbyggere med en sterk forståelse av dataetikk og hvordan de kan beskytte sine digitale liv.

Sphero BOLT Cybersecurity Labs har som mål å møte denne utfordringen ved å bringe cybersikkerhetskonsepter til live gjennom praktiske læringsopplevelser. BOLT simulerer og modellerer konsepter som ofte er skjult dypt inne i datamaskiner, nettverk og kode, slik at ungdomsskoleelever kan visualisere, diskutere og fullt ut forstå dem.

Labene er utviklet i samarbeid med **Dr. Pauline Mosley** , professor og førsteamanuensis for informasjonsteknologi ved Pace University. Dr. Mosleys fagekspertise sikrer at læringen i laboratoriene er både nøyaktig og aktuell. Samtidig som direktør for **Camp Cryptobot** , hennes entusiasme for å engasjere flere ungdomsskoleelever i karriereveier for nettsikkerhet sikrer at laboratoriene er relevante, høyinteresserte og, viktigst av alt, morsomme!

Mål

Ved slutten av enheten vil studentene kunne:

- forklare hvordan datamaskiner bruker private og offentlige nettverk til å overføre informasjon
- skille mellom etisk og uetisk bruk av teknologi
- vurdere risikoen og fordelene ved ulike databehandlingsmetoder
- identifisere ulike typer hackere og forklare deres motiver
- identifisere og forklare vanlige cyberangrep inkludert phishing, skadelig programvare, distribuerte denial of service-angrep og mer
- forklare teknikker som cybersikkerhetsprofesjonelle bruker for å beskytte Internett-tilkoblede enheter og databrukere
- dele strategier for å holde seg selv og enhetene deres trygge mot vanlige cyberangrep
- beskrive potensielle karriereveier innen cybersikkerhet

SPHERO MISJONEN

Sphero forvandler PK-12-utdanning med tilgjengelige verktøy som oppmuntrer til utforskning, fantasi og utholdenhet gjennom STEAM og informatikk. Ved hjelp av lærere over hele verden styrker vi elever med alle bakgrunner og evner til å oppdage interessene og lidenskapene deres, samtidig som vi utstyrer dem med ferdighetene de trenger for å være verdens fremtidige forandringsskapere.

KJÆRE LÆRERE,

VELKOMMEN TIL CYBERSECURITY LABS!

Cybersikkerhet blir raskt en prioritet ettersom unge hjerner lærer STEM og forbereder seg på å bli med i arbeidsstyrken i denne tidsalderen av informasjon og rask globalisering. I følge data samlet inn av US Bureau of Labor Statics (BLS), vil etterspørselen etter cybersikkerhetsjobber som informasjonssikkerhetsanalytikere vokse med så mye som 33 % i løpet av de neste ti årene. Likevel, data fra National Center for Women and Information Technology (NCWIT, 2010), vil bare rundt 3 % av den tilgjengelige mengden av minoritetsutdannede videregående skoler oppnå databehandlingsgrader fra amerikanske høyskoler og universiteter, og mangler dermed kvalifikasjonene til å fylle disse jobbene.

Sphero BOLT Cybersecurity Labs er et standardjustert sett med guidede praktiske erfaringer som introduserer studentene til cybersikkerhetsprinsipper, etikk og teknikker. Laboratoriene, som bruker flere inngangspunkter og koblinger til relevante emner i studentenes hverdag, vil bidra til å skape et sterkt cybersikkerhetsgrunnlag for studenter som kan brukes til å forbedre deres digitale hygiene og starte dem på veien til en cybersikkerhetskarriere. En stor styrke ved denne læreplanen er differensieringen av aktiviteter for ulike ferdighetssett, unge kvinner og minoriteter. Labs kan enkelt modifiseres for disse studentene med ulike ferdighetssett, slik at leveringen av innholdet er inkluderende og engasjerende samtidig som man dyrker selveffektivitet – en kritisk faktor for elevenes suksess.

Det er vårt ønske at studenter som samhandler med disse laboratoriene vil føle seg bemyndiget med kunnskap, teknologiske ferdigheter og en tankegang om at det ikke er noe du ikke kan gjøre hvis du setter tankene dine på det. Kos deg, still spørsmål, gjør feil, få venner, og viktigst av alt – vi krever at du har det gøy!!

Vennlig hilsen,
Dr. Pauline Mosley
Pace University
Full professor og førsteamanuensis for informasjonsteknologi
Direktør for Camp CryptoBot

LAB FUNKSJONER

Designet for ungdomsskoleelever

Laboratoriene er designet spesielt for å introdusere ungdomsskoleelever til feltet cybersikkerhet med to hovedmål. For det første lærer og forsterker laboratoriene prinsippene for digital hygiene og etisk databruk slik at studentene vet hvordan de skal holde seg selv og samfunnet trygt. For det andre viser laboratoriene hvordan ulovlige hackere ofte angriper nettverk og enheter, samt trinnene som cybersikkerhetsprofesjonelle tar for å stoppe angrep slik at studentene bygger et grunnlag for å gå dypere inn i cybersikkerhetsutdanning og -karrierer.

Fokusert på cybersikkerhet

Fokuset til laboratoriene er på cybersikkerhet, ikke på undervisning i dataprogrammeringsferdigheter. Forutsatt forhåndslagrede programmer lar studentene samhandle med cybersikkerhetskonseptene rett ut av esken uten tidligere programmeringserfaring. Studentene vil imidlertid få mer ut av laboratoriene hvis de har litt tidligere erfaring med blokkkoding og med BOLT-roboter. Vi anbefaler på det sterkeste å fullføre Intro to Blocks-aktivitetene i Sphero Edu-appen før du fullfører cybersikkerhetslaboratoriene.

Enkel å differensiere og utvide

Bruk ideene og ressursene i lærernotatene for å hjelpe deg med å tilpasse laboratoriene til elevenes erfaringer og behov. Du finner lenker til instruksjonsideer, ressurser og videoer samt ideer for å ta elevenes læring videre.

Knyttet til karriereveier

Laboratoriene fremhever hvordan cybersikkerhetseksperter jobber for å holde oss og dataenhetene våre trygge mot cybertrusler og utvider studentenes horisont for å vurdere fremtidige cybersikkerhetskarrierer. I den avsluttende laboratoriet utforsker studentene ulike karrierealternativer og forsker og presenterer funnene sine for jevnaldrende.

Justert til cybersikkerhetsstandarder

Laboratoriene er på linje med K-12 Cybersecurity læringsstandarder – utviklet i 2021 av Cyber.org og lærere over hele USA – for å "øke studentenes cybersikkerhetskunnskap og bygge en robust pipeline av fremtidig cybersikkerhetstalent." Standardene er organisert i tre kjernetemaer: Computing Systems (CS), Digital Citizenship (DC) og Security (SEC).

Tema: Datasystemer (CS)

- **6-8.CS.APPS** Diskuter rollen som programvare spiller i beskyttelsen av et sikkert system.
- **6-8.CS.CC** Identifiser fordeler og ulemper med ulike cloud computing-modeller.
- **6-8.CS.COMM.1** Sammenlign og kontrast nettverkstopologier.
- **6-8.CS.COMM.2** Skille mellom en nettverksenhets MAC- og IP-adresser.
- **6-8.CS.COMP** Identifiser rollen til tilkoblede nettverkskomponenter.
- **6-8.CS.HARD** Utvikle strategier for å øke bevisstheten om maskinvaresårbarheter.
- **6-8.CS.IOT** Vurder risikoene og fordelene ved tingenes internett-enheter.
- **6-8.CS.TAP** Forklar rollen og viktigheten av sikkerhetskopier.
- **6-8.CS.OS** Diskuter risikoen ved utdaterte operativsystemer.
- **6-8.CS.PROG** Forklar rollen til skripting i cyberangrep.
- **6-8.CS.PROT** Identifiser protokolltilkoblingstypene som brukes for forskjellige tjenester tilgjengelig på nettet.
- **6-8.CS.SOFT** Identifiser eksempler på sårbarheter som finnes i programvare.

Tema: Digitalt medborgerskap (DC)

- **6-8.DC.AUP** Forstå de ulike avtalene og hvordan de beskytter brukere og eiere av teknologi.
- **6-8.DC.CYBL** Utvikle strategier for å øke bevisstheten om effekten av, og metoder for å identifisere og forebygge nettmobbing.
- **6-8.DC.ETH** Skille mellom etisk og ondsinnet hacking.
- **6-8.DC.FOT1** Gjenkjenne de mange datakildene som utgjør et digitalt fotavtrykk.
- **6-8.DC.FOOT2** Gjenkjenne varigheten av et digitalt fotavtrykk.
- **6-8.DC.IP** Forklar hvordan åndsverk og opphavsrett relaterer seg til rimelig bruk.
- **6-8.DC.LOV** Analyser spesifikke føderale, statlige og lokale lover når det gjelder nettsikkerhet og personvern.
- **6-8.DC.PP.1** Diskuter risikoene og fordelene ved å dele PII.
- **6-8.DC.PP.2** Undersøk teknikker for å oppdage, korrigere og forhindre avsløring av PII.
- **6-8.DC.THRT** Beskriv ulike typer trusselaktører.

Tema: Sikkerhet (SEC)

- **6-8.SEC.ACC** Forklar konseptet med tilgangskontroll og hvordan du begrenser tilgang til autoriserte brukere.
- **6-8.SEK.AUTH** Forklar hvordan autentiserings- og autorisasjonsmetoder kan beskytte autoriserte brukere.
- **6-8.SEC.CIA** Forklar virkningene av en fiasko i CIA-triaden.
- **6-8.SEC.COMP** Beskriv Defence in Depth-strategier for å beskytte enkle nettverk.
- **6-8.SEK.GRÅT** Diskuter metoder og behovet for kryptering av informasjon når den utveksles, f.eks. http vs. https.
- **6-8.SEC.CTRL** Beskriv Defence in Depth og hvordan fysiske tilgangskontroller fungerer sammen.
- **6-8.SEK.DATA** Beskriv data i de tre statene og potensielle trusler mot hver stat.
- **6-8.SEK.INFO** Analyser trusler og sårbarheter for informasjonssikkerhet for enkeltpersoner og organisasjoner.
- **6-8.SEC.NET** Forklar hvordan ondsinnede handlinger truer nettverkssikkerheten.
- **6-8.SEC.PHYS** Forklar hvordan ondsinnede handlinger truer fysisk sikkerhet.

LAB STRUKTUR

Hvert laboratorium bruker følgende struktur for å engasjere studentene og utvikle en dypere forståelse av cybersikkerhetskonsepter:

Aktiver

I **Aktiver trinn** , laboratorier knytter til forkunnskaper som studentene kanskje allerede har om emnet og engasjerer studentenes interesse.

Lære

I **Lær trinn** , gir laboratoriene kjernelæringsvokabular og konsepter for å gjøre det mulig for studentene å øke forståelsen av cybersikkerhet. Bruk ideene og informasjonen i lærerens notater for å ta denne læringen videre.

Undersøk

I **Undersøk trinn** , studenter åpner og kjører et BOLT-program for å begynne å utforske emnene på en praktisk måte.

Hack

I **Hack Steps** , endrer studentene programmet for å utvide modellen gjennom flere scenarier og spilling.

Sikre din forståelse

I **Sikre dine forståelsestrinn** , studenter kobler BOLT-modellen tilbake til databehandling i hverdagen og diskuterer læring om nettsikkerhet med klassekameratene sine.

TILRETTINGSTIPS

Før undervisning:

- Les gjennom elevinstruksjonene for aktiviteten, prøv ut programmeringen og forutse hindringer som elevene dine kan møte.
- Les lærernotatene i Lab Steps og vurder punkter der du vil sette elevene på pause for undervisning og diskusjon i hele klassen.
- Forbered klasserommet for laboratoriets behov i henhold til elevinstruksjoner og lærernotater.
- Bestem om laboratoriet bruker IR-kommunikasjon mellom to eller flere grupper og, om nødvendig, planlegg for større studentgrupper med to eller flere BOLTER og programmeringsenheter.
- Sørg for at alle roboter og programmeringsenheter er fulladet.
- Plan for to elever per BOLT-robot.

Under undervisningen:

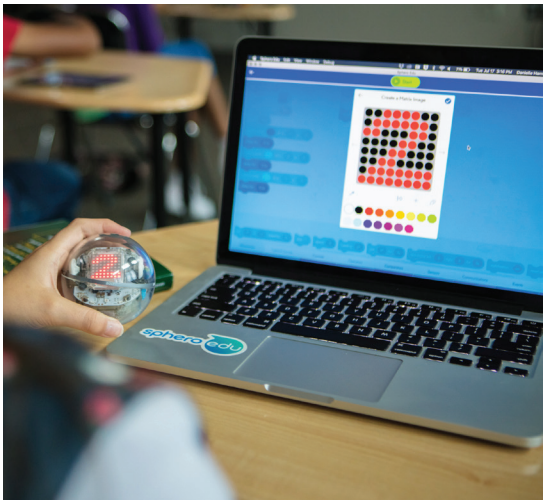
- Sirkuler klasserommet ditt for å feilsøke utfordringer med elevene. Hvis flere grupper sliter med det samme problemet, feilsøk det som en hel klasse.
- Bruk lærernotatene for potensielle elevløsninger samt ideer om hvordan du kan utvide utfordringer og læring.
- Tenk på tid. Hvis mulig, reserver 5–10 minutter på slutten av instruksjonsperioden for trinnet Sikre din forståelse.

Etter undervisning:

- Reflekter over elevenes læring. Hva var lett for elevene? Hva var vanskelig? Var det en artefakt av elevlæring som du kan dele med hele klassen for å løse en felles utfordring eller vise frem et programmeringskonsept eller problemløsningsstrategi?
- Utforsk hvordan du kan bruke ideer og ressurser i laboratoriet og/eller lærernotater for å utdype elevenes læring.
- Vurder hvordan du kan bygge emnet inn i et uavhengig prosjekt eller gruppeprosjekt. Elevene kan for eksempel forske på et annet eksempel på et phishing-opplegg og presentere læringen for jevnaldrende.

LAB GRUPPER

Cybersikkerhetslaboratoriene er delt inn i **fire nivåer** —rød, gul, blå og grønn — hver med **fem laboratorier** . Laboratoriene er presentert i en løs **sekvensiell rekkefølge** , som starter med de mest innledende cybersikkerhetskonseptene og slutter med noen av de mest avanserte. Du kan begynne på Rød 1 og undervise helt til Grønn 5. Hver lab er imidlertid også ment å **stå alene** . Du kan **velg og velg** emner som er mest relevante for elevenes behov og pensum. Vær nøye med på **koding forutsetninger** , hvis noen, oppført i beskrivelsen av laboratoriet ved planlegging.



RØDT NIVÅ
ETIKK OG NETTVERK

Studentene starter sin cybersikkerhetsreise ved å lære om etiske kontra uetiske databehandlingspraksis og vurdere en dataetisk kode. Deretter lærer elevene det grunnleggende om hvordan datamaskiner kommuniserer via internett og på private nettverk. De digitale fotavtrykkslaboratoriene sporer elevenes veier gjennom internett og introduserer måter som deres digitale handlinger spores (og brukes) av andre.

Klikk på hver tittel eller aktivitetsnavn for å se aktiviteten i Sphero Edu-appen

RØD 1 *Databehandlingens etikk: Rett vs. galt*

En sterk etikkkodeks utgjør hjertet av cybersikkerhet, og påvirker valgene vi tar når vi bruker dataenhetene våre, samt hvordan vi beskytter oss selv og andre mot cybertrusler.

Ved slutten av denne laboratoriet vil studentene kunne:

- forklare etiske retningslinjer for datafagfolk.
- skille mellom en etisk og uetisk beslutning.

RØD 2 *Hvordan Internett fungerer: Det store bildet*

De fleste av oss bruker internett daglig til jobb, skole og livet. Men hva er egentlig internett og hvordan fungerer det?

Ved slutten av denne laboratoriet vil studentene kunne:

- beskrive IP- og TCP-protokoller.
- bruk BOLT-roboter for å forklare hvordan internett fungerer.
- sammenligne og kontrastere nettsteder som bruker HTTP og HTTP.

RØD 3 *Private nettverk: Holde det privat*

Internett er et stort, offentlig rom, men oddsen er at du bruker mesteparten av tiden din på å få tilgang til internett fra et privat nettverk kalt et lokalnettverk (LAN), enten du er hjemme, på biblioteket eller på skolen.

Ved slutten av denne laboratoriet vil studentene kunne:

- definere og skissere et lokalt nettverk (LAN).
- beskrive rollen til et modem og en ruter.
- forklare hvordan brannmurer beskytter enheter på et LAN fra det offentlige internett.

RØD 4 *Digitale fotspor: Våre Internett-spor*

Akkurat som et fotavtrykk i bakken, kan digitale fotavtrykk brukes til å spore beslutninger og bevegelser på nettet. Det er viktig for deg å begynne å tenke på dette så snart du begynner å bruke internett.

Ved slutten av denne laboratoriet vil studentene kunne:

- Identifiser hva et digitalt fotavtrykk er.
- Lag en modell av et digitalt fotavtrykk som klasse.
- Se på hva som for tiden er i deres digitale fotavtrykk.

RØD 5 *Administrere ditt digitale fotavtrykk*

Å forstå hvordan ditt digitale fotavtrykk skapes og hva det brukes til er avgjørende for å beskytte deg selv og informasjonen din. Mens mange deler av ditt digitale fotavtrykk kan være ufarlige – og til og med nyttige – uten riktig oppmerksomhet, kan det raskt bli til mye informasjon du ikke vil at noen skal ha tilgang til.

Ved slutten av denne laboratoriet vil studentene kunne:

- Identifiser hvilke typer informasjon som kan inkluderes i et digitalt fotavtrykk.
- Bestem hvilke deler av informasjon de ønsker og ikke vil ha i sitt digitale fotavtrykk.
- lære teknikker for å kontrollere deres digitale fotavtrykk.

GULT NIVÅ
NETTMOBLER OG HACKERE

Studentene ser på nytt konseptet med etisk databehandling med fokus på nettmobbing. De lærer så om de forskjellige typene hackere; i tillegg til uetiske/ulovlige hackere, er det også etiske/lovlige hackere som bruker dagene på å motarbeide de dårlige skuespillerne. Elevene utforsker noen måter dårlige skuespillere bruker phishing og sosial ingeniørkunst for å plante virus og ormer – to typer skadelig programvare som kan forårsake skade.

Klikk på hver tittel eller aktivitetsnavn for å se aktiviteten i Sphero Edu-appen

GUL 1 *Nettmobbing: Ikke vær en mobber*

Nettmobbing kan ha utrolig negative effekter på ikke bare offeret, men også personen som driver med nettmobbing og hele nettsamfunn.

Ved slutten av denne laboratoriet vil studentene kunne:

- forklare definisjonen av nettmobbing.
- diskutere effektene nettmobbing har på psykisk helse.
- utforske ulike måter du kan forhindre nettmobbing på.

GUL 2 *Typer hackere: Å hacke eller ikke hacke*

Det gode, det dårlige og alt i mellom. Nettsikkerhetsverdenen er fylt med alle typer hackere med et bredt spekter av motivasjoner.

Ved slutten av denne laboratoriet vil studentene kunne:

- forklare definisjonen av hacking.
- diskutere de juridiske og etiske konsekvensene av hacking.

GUL 3 *Phishing: Hvordan finner ulovlige hackere deg*

Phishing og sosial manipulering er vanlige teknikker som uetiske hackere bruker for å overbevise intetanende mennesker om å gi informasjonen sin fritt, og deretter bruke den til å få tilgang til passordene deres, bankkontoene, kredittkortinformasjonen og mer.

Ved slutten av denne laboratoriet vil studentene kunne:

- forklare definisjonen av phishing.
- diskutere farene ved phishing, svindel og sosial ingeniørkunst.
- diskuter ulike måter du kan beskytte deg selv mot å bli offer for phishing.

GUL 4 *Virus: modellering av spredningen av en datamaskininfeksjon*

Skadelig programvare, eller ondsinnet programvare utviklet for å skade og forstyrre teknologien vår, er dessverre et faktum i moderne liv. Men å lære hva det er og hvordan det fungerer, kan hjelpe oss alle med å holde datamaskinene våre og oss selv tryggere.

Ved slutten av denne laboratoriet vil studentene kunne:

- beskrive de tre hovedtypene av skadelig programvare.
- modeller hvordan skadelig programvare som et virus sprer seg med BOLT.
- beskrive trinnene enkeltpersoner og cybersikkerhetseksperter tar for å bekjempe skadelig programvare.

GUL 5 *The Morris Worm: Historisk skadelig programvare*

Akkurat som en fysisk orm, kan dataormer vri seg, spre seg og vokse over et nettverk, og infisere datamaskiner mens de går. Selv om de noen ganger er ufarlige, er mange ormer skadelig programvare som kan skade datamaskiner og skape muligheter for angrep.

Ved slutten av denne laboratoriet vil studentene kunne:

- sammenligne og kontrastere ormer og virus.
- modellere Morris Worm med et BOLT-program.
- beskriv hvilke typer skade ormer kan forårsake.

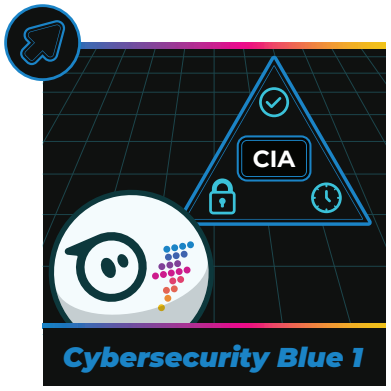
BLÅTT NIVÅ

CIA TRIAD OG ANgrep

Studentene lærer om CIA Triad-modellen, brukt av cybersikkerhetseksperter for å planlegge informasjonssikkerhet. De får da vite om andre trusler om dårlige skuespillere, inkludert DDoS-angrep, sniffing og skanning og person-i-midten-angrep. Innvevd i hver er strategier brukt av lovlige hackere for å motvirke trusselen og sikre informasjonstilgjengelighet, integritet og konfidensialitet.

Klikk på hver tittel eller aktivitetsnavn for å se aktiviteten i Sphero Edu-appen

BLÅ 1 *CIA Triad: Planlegging for sikkerhet*

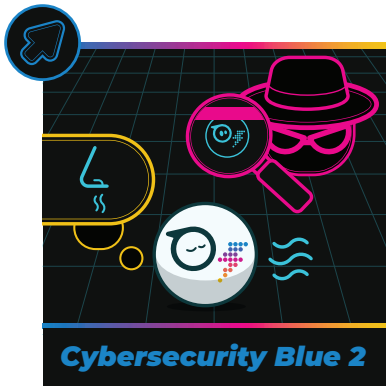


Når de planlegger informasjons- og nettverkssikkerhet, holder cybersikkerhetseksperter CIA-triaden – konfidensialitet, integritet og tilgjengelighet – i kjernen av beslutningsprosessen.

Ved slutten av denne laboratoriet vil studentene kunne:

- forklare betydningen av konfidensialitet, integritet og tilgjengelighet i CIA-triaden.
- beskrive rollen til hvert prinsipp i CIA-triaden for å beskytte informasjon og data.

BLÅ 2 *Hacker-snoking: Sniffing og skanning*



Før en hacker kan angripe deg, må de lære om sårbarhetene dine. Nettsikkerhetskriminelle bruker to rekognoseringsteknikker for å lære om sårbarhetene dine: snusing og skanning.

Ved slutten av denne laboratoriet vil studentene kunne:

- beskriv forskjellen mellom sniffing og skanning.
- forklare hvordan angripere bevæpner informasjon de samler inn om datasystemer.
- bruke IR-meldinger til å ta over motstanderlagets BOLT.

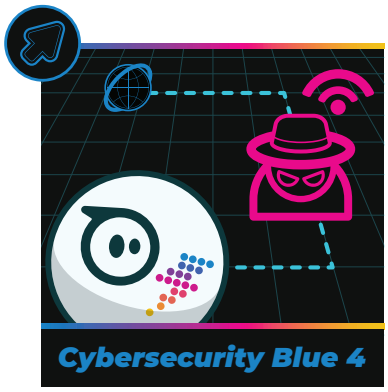
BLÅ 3 *Avvist: Denial of Service-angrep*

Denial of Service (DoS) og Distributed Denial of Service (DDoS)-angrep er noen av de mer vanlige og forstyrrende cyberangrepene. Relativt uerfarne nettkriminelle kan ta ned store nettsteder og gjøre informasjon og tjenester utilgjengelige.

Ved slutten av denne laboratoriet vil studentene kunne:

- beskrive Denial of Service (DoS) og Distributed Denial of Service (DDoS) angrep.
- programmer to BOLT-er for å representere angriperen og offeret i et DoS-angrep.
- endre programmet for å redusere BOLTens mottakelighet for et DDoS-angrep.

BLÅ 4 *Person-i-midt-angrep: Hvem er der?*



Et person-i-midten-angrep høres akkurat ut som det det er: en ulovlig hacker som avskjærer kommunikasjon mellom deg og internetttjenestene du bruker mens du er på en datamaskin.

Ved slutten av denne laboratoriet vil studentene kunne:

- beskrive et person-i-midten-angrep.
- modeller et person-i-midten-angrep med BOLT-roboter.
- forklare hvordan de kan holde seg trygge mens de bruker Internett-tilkoblede datamaskiner.

BLÅ 5 *Circles of Influence: Autentiser og autoriser*

For å skille mellom ulike typer brukere kan ulike typer brukerautorisasjoner benyttes. Når denne autorisasjonen kompromitteres, kan det få kaotiske konsekvenser.

Ved slutten av denne laboratoriet vil studentene kunne:

- definere autentisering og dens betydning for cybersikkerhet.
- diskutere de fire generelle måtene å autentisere en brukers identitet på (passord, biometrisk, elektronisk, smartkort).
- modell autorisasjonsnivåer med BOLT.
- beskrive noen av de viktigste sikkerhetsproblemene for brukerautentisering.

GRØNT NIVÅ
KRYPTOGRAFI OG DIN FREMTID

På siste nivå graver studentene dypere inn i cybersikkerhetsfagfolks verden og undersøker hvordan passord og informasjonskryptering kan holde vår digitale informasjon og liv trygge. I den siste laboratoriet, etter å ha utviklet en innledende forståelse av mange cybersikkerhetsemner, forhåndsviser studentene jobbmuligheter i en verden av cybersikkerhet.

Klikk på hver tittel eller aktivitetsnavn for å se aktiviteten i Sphero Edu-appen

GRØNN 1 *p@$$W0RD$!: Hva er bak et sterkt passord*

Hva er mektigst: et menneske eller en maskin? Vel, når det kommer til å knekke passord, er datamaskiner mye raskere enn oss.

Ved slutten av denne laboratoriet vil studentene kunne:

- bruk BOLT for å knekke en kombinasjonslås.
- beskrive to metoder ulovlige hackere bruker for å knekke passord.
- forklare hvordan du lager sterke og minneverdige passord.

GRØNN 2 *Introduksjon til kryptografi: Pigpen Cipher*

Har du noen gang sendt notater i en hemmelig kode? Vel, datamaskiner kommuniserer hele tiden i krypterte meldinger.

Ved slutten av denne laboratoriet vil studentene kunne:

- bruk BOLT og grisebingen for å sende hemmelige meldinger til klassekameratene dine.
- forklare hvordan ren tekst krypteres til chiffertekst og deretter dekrypteres tilbake til ren tekst.
- krypter og dekrypter meldinger med BOLT og pigpen-chifferet.

GRØNN 3 *Cæsarskiftet: Cæsar sier hva?!*

Med ordene til den gamle romerske lederen, Julius Caesar, "RljvnRbjfRlxwzdnanm." Vent, hva?!?! Det viser seg at Caesar ofte krypterte kommunikasjonen hans, og en av de mest kjente av alle chiffer, Caesar Shift, er oppkalt etter ham.

Ved slutten av denne laboratoriet vil studentene kunne:

- krypter og dekrypter meldinger med Caesar Shift.
- manipulere et JavaScript BOLT-program for å utforske kryptografi.
- identifisere egenskapene til sterke chiffer.

GRØNN 4 *Multipliser det! Modulo aritmetikk og chiffer*

Lær om multiplikasjonschifferet, et monoalfabetisk chiffer. I prosessen vil du bli komfortabel med modulær aritmetikk og begynne å forstå betydningen av den for moderne kryptografi.

Ved slutten av denne laboratoriet vil studentene kunne:

- krypter og dekrypter meldinger med et multiplikasjonschiffer.
- bruk modulo-operasjonen for å beregne resten.

GRØNN 5 *Karriereparade for cybersikkerhet*

Hendelsesvarere, kryptografer, penetrasjonstestere; En av disse kan være jobbtittelen din i fremtiden.

Ved slutten av denne laboratoriet vil studentene kunne:

- identifisere ulike cybersikkerhetskarrierer.
- forstå hvor og hvilke yrker som er etterspurt.
- forklare detaljer om en cybersikkerhetskarriere de selv velger.

TEKNOLOGITIPS

Sphero Edu-appen

Last ned The Sphero Edu-appen her .

Opprett klasser og tildel aktiviteter

Opprett en lærerkonto slik at du kan konfigurere og administrere klasser som pedagog. Du har noen alternativer for å administrere klassene dine:

- **Klassekoder (anbefalt)**

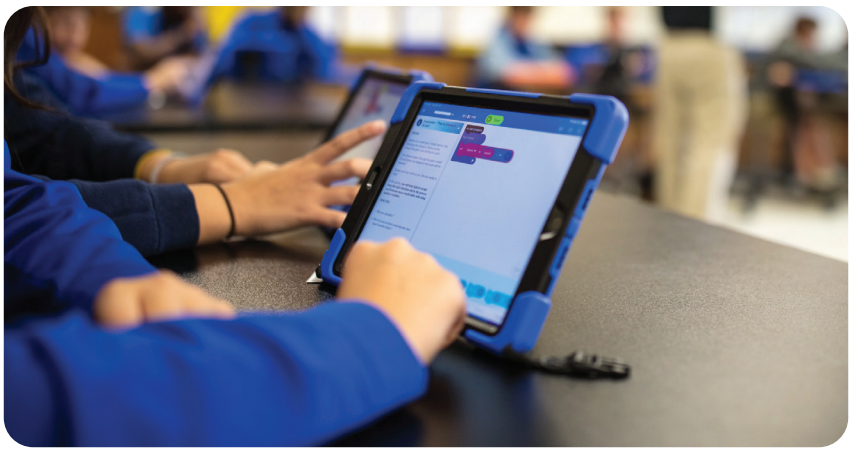
  Hvis du foretrekker at elevene skal jobbe med oppgaver uten brukernavn og passord, distribuer klassekoder. Bare skriv inn et klassenavn og klassekoden genereres automatisk. Gi elevene klassekoden for å få tilgang til oppgavene deres og fortsette å jobbe med programmene deres. I motsetning til standardklasser, lagres elevfremgang i klassen i stedet for en konto. Lære mer **her** .

- **Standard klasse**

  Opprett elevkontoer manuelt eller ved å laste opp en CSV. Disse studentkontoene inkluderer individuelle brukernavn og passord for hver student. I denne modellen kan du tilordne aktiviteter til studenter for gjennomføring, men kan ikke direkte tildele programmer. Alt elevarbeid lagres på deres personlige konto og ikke klassen selv.

- **Google eller smarte brukere**

  Du kan automatisk synkronisere klassene dine til Sphero Edu. Se mer informasjon **her** .



Lade roboter

Sphero BOLT-roboter lader via induktiv lading i den medfølgende holderen. For å lade, plasser roboten på ladeholderen med tung side ned. Du vil se et blått lys blinke på holderen for å indikere at den lader. BOLT vil trenge opptil 6 timer for full lading, men tiden vil variere avhengig av batteriets nåværende nivå, og du vil vite at det er ladet når det blå lyset slutter å blinke.

Feilsøking

- Sørg for at robotens fastvare er oppdatert. Hvis en fastvareoppdatering er nødvendig, starter den automatisk etter at den er koblet til en enhet.
- Lad roboter og enheter kvelden før du bruker dem i timen.
- Sørg for at Sphero Edu-appen er oppdatert.
- Start Sphero-roboten på nytt ved å holde knappen nede på laderen og fjerne roboten fra ladekrybben, og plasser den deretter tilbake på ladekrybben.

Brukerstøtte

Sphero styrker fremtidens skapere av morgendagen og setter dem opp for suksess.
Vi kunne ikke vært mer begeistret for fremtidens utdanning og rollen vi spiller. For mer informasjon om Sphero og for å bli involvert i fellesskapet vårt kan du finne lenker til flere ressurser nedenfor.

- **Sphero Blog -** Besøk vår **utdanningsblogg** for oppdateringer, tips og forslag.
- **Brukerstøtte -** Besøk vår **støtteside** for vanlige spørsmål og feilsøkingstips og triks.
- **Kontakt oss -** Kontakt oss for ytterligere støtte eller hjelp **her** .