

Passord

Deltakerne lærer hvordan de kan beskytte informasjonen sin på nettet ved å bruke og opprettholde sterke passord. Deltakerne lærer om prinsippene for utforming av sterke passord og potensielle problemer ved deling av passord. De lærer også hvordan de kan sikre passordene sine, og hvordan de kan hindre uautorisert tilgang til kontoene sine.

Materiell

Lære om passord – utdelingsark

Grunnleggende om passord

Del 1

Fortell elevene dine

Ofte tenker vi ikke over passordene vi bruker til nettsteder, apper og tjenester. Men hvor gode passordene dine er, avgjør hvor sikker informasjonen din er.

Klasseaktivitet

Engasjer deltakerne i en diskusjon ved hjelp av følgende spørsmål. Minn deltakerne på at det er viktig ikke å dele de reelle passordene sine i denne og andre øvelser.

Spør elevene dine

Hvor mange passord har du?

Har du forskjellige passord for alle kontoene dine til e-post og sosiale medier?

Er de veldig forskjellige, eller er de en variant av ett enkelt passord?

Hvis du har mer enn ett passord, hvordan husker du hvilket som tilhører hvilken konto?

Spør elevene dine

Hvor ofte har du glemt et viktig passord?

Hva har du gjort når du har glemt passordet ditt?

Hvordan gjør du passordene dine enklere å huske?

Er det et passord du bruker hver dag?

Hva ville skje hvis noen fant ut hva passordet ditt var uten at du visste om det?

Ville det avhenge av hvem det var?

Hva slags informasjon kan noen få om deg hvis vedkommende bruker passordet ditt til å komme inn på kontoen din?

Del 2

Klasseaktivitet

Organiser deltakerne i par.

Fortell elevene dine

Sammen med partneren din diskuterer du hva som kan skje hvis noen som ønsker å skape problemer, fikk vite passordet til en plattform på sosiale medier du bruker ofte.

Klasseaktivitet

Gi deltakerne 5 minutter til å diskutere. Og be gruppen om å dele.

Fortell elevene dine

Diskuter med partneren din hva som ville skje hvis en hacker fikk vite passordet til nettbankkontoen til din forelder/foresatt.

Klasseaktivitet

Gi deltakerne 5 minutter til å diskutere. Deretter ber du gruppene om å dele hva de har diskutert.

Del 3

Fortell elevene dine

Du lurer kanskje på hvordan en hacker kan finne ut et privat passord. Det finnes flere måter, og én måte er å lure noen til å dele passordet sitt. En hacker kan gjøre det ved å sende en e-post som ser ut som den virkelig kommer fra en plattform eller et nettsted personen har en konto på. E-posten kan be personen om å klikke på en lenke og logge inn med brukernavn og passord, og når vedkommende logger inn, blir denne informasjonen tilgjengelig for hackeren.

Noen ganger prøver hackere å gjette passord ved å bruke vanlige uttrykk som «passord123», «test» eller for- eller etternavn.

Hackere kan også få vite et privat passord gjennom det som kalles et hackerangrep. Et hackerangrep oppstår når en hacker prøver å logge inn på kontoen din ved å prøve forskjellige passord gjentatte ganger. Selv om en hacker kan gjennomføre et hackerangrep personlig, gjennomføres det ofte ved å kjøre et dataprogram som raskt og automatisk prøver enhver mulig kombinasjon av passord det kan tenke seg. Det vil si en liste over sannsynlige passord eller et sett av passord som består av kombinasjoner av forskjellige bokstaver og tall, helt til det finner riktig passord.

Selvfølgelig er enkelte hackerangrep mer avanserte. Hvis passordet ditt er på en liste over sannsynlige passord, som «fido123» eller «passord», kan noen

programmer gjette det raskere ved å prøve disse alternativene før mindre sannsynlige eller tilfeldige muligheter. Angrepet kan også være mer finjustert hvis hackeren kjenner til informasjon om deg. Hvis hackeren for eksempel vet at kjæledyret ditt heter Toby, kan hackeren prøve «Toby» med forskjellige varianter av tall på slutten (f.eks. «Toby629» eller «Toby3020»).

Lage sterke passord

Del 1

Spør elevene dine

Hvem vet hva det vil si å ha et «sterkt» eller «sterkere» passord? Hvorfor er dette en god idé?

Fortell elevene dine

Et sterkt passord bidrar til å beskytte informasjonen din. Selv om et sterkt passord ikke garanterer at kontoen din ikke blir hacket, gjør et svakt passord det mye enklere for noen å få tilgang til informasjonen din.

Passordøvelse

Spør elevene dine

Har dere noen eksempler på svake passord?

1. Her er noen eksempler: Passord, 12345, Hallo!, en fødselsdato, et kallenavn.

Hvorfor tror du disse er svake?

1. De kan enkelt bli gjettet av en annen og/eller en datamaskin som kjører et kraftig angrep.

Hvordan kan du gjøre et passord sterkere?

1. Ved å legge til tall, små og store bokstaver, symboler, gjøre passordet lengre og unngå vanlige uttrykk og ord på egen hånd.

Klasseaktivitet

Etter at deltakerne har kommet med sine synspunkter, skriver du disse instruksjonene på tavlen:

Inkluder minst ett tall.

Inkluder minst ett symbol.

Inkluder minst én stor og én liten bokstav.

Passord bør bestå av minst sju tegn.

Passord bør være enkle å huske (med mindre du bruker en passordadministrator).

En passordadministrator er et nettsted eller en app som hjelper brukerne med å lagre og organisere passordene sine.

Passord bør ikke bestå av et enkelt vanlig ord eller personlig informasjon (fødselsdato, foreldres navn osv.).

Et passord bør ikke brukes på flere nettsteder.

Fortell elevene dine

Det er to tilnærminger til å opprette sterke passord. Den første er å følge en «passordoppskrift» som denne på tavlen. Med en slik oppskrift oppmuntres du til å inkludere elementer som er vanskeligere å gjette, i et passord bestående av tekst/tall, og det gjør selve passordet vanskeligere å gjette. Ulempen ved denne tilnærmingen er at den gjør det vanskeligere å huske passordene.

Sterke passord

Fortell elevene dine

En annen tilnærming til å opprette sterke passord er å bruke lange passord. Fordi passordstyrken er forbundet med hvor langt passordet er, blir passord mye vanskeligere å gjette for mennesker og hackerangrep hvis du bruker en streng på fire eller flere ord uten sammenheng. Denne metoden har i tillegg den fordel at den gir passord som er enklere å huske enn oppskriftsmetoden.

Til slutt kan man bruke en kombinasjon av disse to metodene ved å finne på en streng av fire eller flere ord uten sammenheng, og i tillegg inkluderer symboler og tall.

Målet med disse forskjellige metodene er det samme: å utvikle passord som er unike og vanskelige for andre å gjette.

Fortell elevene dine

Organiser deltakerne i par.

I par prøver dere å opprette et sterkt passord ved hjelp av instruksjonene som ble skrevet på tavlen tidligere. Husk at et passord som er vanskelig for en datamaskin å gjette tilfeldig, fremdeles kan være enkelt å gjette for et menneske eller en

datamaskin med en liste over vanlige lange passord. Arket med passordet ditt blir ikke samlet inn på slutten av aktiviteten. Deltakerne bør ikke bruke dette passordet på en av kontoene sine, siden personene i gruppen vil kjenne til det.

Gi deltakerne 5 minutter til å gjøre dette. Deretter går du rundt i rommet og spør deltakerne hva de synes de beste eksemplene på sterke passord er. Spør deltakerne om de kan huske passordene de har generert, uten å se direkte på dem.

Selv om noen nettsteder krever at passordene dine overholder noen av (eller alle) disse retningslinjene, har andre ingen slike begrensninger. Du kan også opprette passord med en rekke av tilfeldige vanlige ord.

Klasseaktivitet

Be deltakerne opprette nye passord som består av rekker av ord, fortsatt i de samme parene. Fortell dem at det bør være minst fire ord i passordet for at det skal være både sterkt og enkelt å huske. Gi deltakerne 5 minutter til å gjøre dette. Deretter går du rundt i rommet og spør deltakerne hvilke eksempler de har på passord. Minn deltakerne på igjen at arket ikke kommer til å bli samlet inn når aktiviteten er over, og at passordet ikke bør brukes til noen av kontoene deres.

Fortell elevene dine

Noen nettsteder bruker et system som kalles flerfaktorgodkjenning (eller tofaktorgodkjenning) til å verifisere identiteten din. Disse nettstedene bruker ofte tekstmeldinger, en app eller en e-post til å sende en engangskode som må angis sammen med passordet.

Denne metoden kan gjøre kontoene dine mye tryggere ved å legge til et ekstra sikkerhetslag som er mye vanskeligere å bryte. En person må for eksempel ha passordet ditt og tilgang til appen, enheten eller e-postadressen som er forbundet med kontoen, for å kunne logge inn på kontoen din.

Beskytte passord

Del én

Fortell elevene dine

Selv om du oppretter passord som er vanskelige for en datamaskin eller person å gjette, finnes det andre måter et passord kan være svakt på.

Spør elevene dine

Hvilke andre måter kan passord være svake på?

1. Noen eksempler inkluderer: å bruke ett passord for flere kontoer, å bruke et passord som inneholder personlig informasjon, å bruke det samme passordet i mange år, å glemme passordet sitt.

Hvor ofte mener du at du bør bytte passord?

Fortell elevene dine

Selv gode passord kan bli stjålet eller være utsatt, men det er ting du kan gjøre for å beskytte deg selv. Hvis det er databrudd på et nettsted hvor du har en konto, må du sørge for å bytte passord på det nettstedet i tillegg til på andre nettsteder hvor du bruker lignende passord.

Det kan være vanskelig å huske mange lange og kompliserte passord.

Spør elevene dine

Synes du det er en god idé å skrive ned passordene dine på et ark eller i et dokument på datamaskinen din? Hvorfor eller hvorfor ikke?

Klasseaktivitet

Nevn mulighetene for at noen finner arket eller legger merke til dokumentet på datamaskinen din. Forklar at en tilnærming er å bruke en passordadministrator, en app som hjelper brukerne med å lagre og organisere passordene sine.

Del to

Fortell elevene dine

Hver dag bruker vi mange forskjellige kontoer på forskjellige nettsteder. Det kan bli komplisert å logge inn og ut av hvert eneste nettsted hver gang.

Spør elevene dine

Har du noen gang brukt funksjonen «Lagre passord» i nettleseren for å lagre et passord på et nettsted? Hvorfor eller hvorfor ikke?

Forstår du hvordan nettstedet husker hvem du er?

1. Be om forklaringer. Forklar deretter at nettsteder kan huske at du har logget inn, ved å lagre en informasjonskapsel. Informasjonskapsler er bittesmå filer som lagres på datamaskinen din for å gjøre det lettere for et nettsted å vite hvem du og datamaskinen din er ved fremtidige besøk, uten at du trenger å logge inn på nytt. Men informasjonskapsler kan også brukes til å spore deg når du går fra nettsted til nettsted. Det er én måte annonser kan målrette mot deg på.

Er det greit å lagre et passord hvis det er på din egen datamaskin?

Spør elevene dine

Har datamaskinen din et innloggingspassord?

Hva hvis du deler datamaskinen med andre?

1. I dette tilfellet kan andre som bruker datamaskinen din, potensielt finne ut hva passordet ditt er, selv om passordet i passordfeltet kanskje er skjult av svarte prikker eller stjerner. Bare fordi du ikke kan se hva passordet er på skjermen, betyr det ikke at det ikke er lagret et annet sted.

Spør elevene dine

Er det noen gang greit å dele et passord? Når? Hvorfor?

1. Noen eksempler kan være at foreldre ønsker tilgang til passord eller at de har en delt familiekonto på for eksempel Netflix.

Deler du passord med noen? I tilfelle: med hvem og hvorfor?

Hvis du er god venn med noen, ville det fungert som en motivasjonsfaktor for å dele passord hvis vedkommende sa «hvis du bryr deg om meg»? Hvorfor eller hvorfor ikke?

Fortell elevene dine

Du kan velge å dele passordet ditt med noen du bryr deg om, men å bry seg om dem betyr ikke nødvendigvis at vedkommende fortjener full tilgang til nettkontoene

dine.

Tenk nøye gjennom forholdet til denne personen før du deler, inkludert hvordan forholdet kan endres over tid. Det er for eksempel stor forskjell på å dele passord med en forelder/foresatt enn å dele med bestevennen din.

Spør elevene dine

Hva kan skje med deg hvis du deler et passord?

1. Noen kan hacke seg inn på bankkontoene dine, gi seg ut for å være deg på nettet eller få vite noen av hemmelighetene dine.

Hvis du har delt et passord til en konto, ville du brukt den kontoen annerledes?

Spør elevene dine

Er det ting du ikke ville sett på Netflix eller ikke ville skrevet i en e-post hvis noen andre kunne se hva du gjorde?

Klasseaktivitet

Deltakerne bør tenke gjennom sin egen oppførsel når de bruker en delt konto. De bør tenke på at nettaktiviteten deres er synlig for andre brukere på kontoen.

Spør elevene dine

Profilen din på sosiale medier er en virtuell presentasjon av deg. Er det da greit å la andre bruke kontoen din?

Klasseaktivitet

Diskuter muligheten for at en annen gir seg ut for å være deg og sender meldinger til vennene dine.

Spør elevene dine

Tillater du at noen av enhetene du bruker, lagrer passordene dine? Hvorfor eller hvorfor ikke? Betyr det at det er trygt å lagre passordene dine på din personlige telefon eller datamaskin? Hva skjer om du lar en venn låne telefonen eller datamaskinen?

Deler du noen enheter med andre, som familie eller venner? Deler du en konto på enheten, eller har hver person sin egen?

Bruker du noen gang en offentlig enhet, f.eks. på biblioteket, skolen eller et annet

sted? Gjør du det samme på den enheten som du ville gjort på din private enhet?

Del tre

Klasseaktivitet

Organiser deltakerne i par.

Fortell elevene dine

I parene diskuterer dere om dere noen gang har logget inn på en datamaskin på skolen, på biblioteket eller et annet offentlig sted og har sett at en annen person fremdeles var logget inn på sin e-postkonto eller sosiale medier. Be dem om å vurdere om de ville gå inn på kontoen eller gjøre noe annet.

Klasseaktivitet

Gi deltakerne 5 minutter til å diskutere, og be dem deretter om å dele hva de har kommet frem til. Engasjer gruppen i en diskusjon om slik uautorisert bruk.

Uautorisert kontotilgang

Del én

Klasseaktivitet

Merk: En del av innholdet i denne aktiviteten har blitt dekket i «Aktivitet nr. 1: Grunnleggende om passord.» Du må selv vurdere om du vil gå gjennom dette materialet på nytt eller hoppe over det.

Fortell elevene dine

Det er mulig for andre å få tilgang til kontoen din, selv uten at de allerede kjenner til eller lykkes med en tilfeldig gjetning på passordet ditt. Hvis en person kjenner til nok personlig informasjon om deg, kan vedkommende gjette passordet ditt eller overbevise noen i en bedrift om å overgi informasjonen din. Siden vedkommende ikke bruker teknologi til å bryte seg inn på kontoene dine, kalles denne typen angrep sosial hacking.

Spør elevene dine

Rekk opp hånden hvis du har glemt passordet ditt til et nettsted noen gang.

Hva skjer når du klikker på «Jeg har glemt passordet mitt?»

1. Nettstedet ber vanligvis om svar på sikkerhetsspørsmål eller prøver å kontakte deg på e-post eller telefon.

Hvilke sikkerhetsspørsmål kan nettstedet stille?

1. Forklar hvorfor dette er spørsmål som venner eller bekjente kan svare på eller gjette. Ting som navnet på kjæledyret, hvor de ble født, morens pikenavn, navnet på favorittlæreren, navnet på bestevennen, favorittidrettslaget.

Hvem andre kan kjenne til denne typen informasjon om deg?

Hvordan kontakter et nettsted deg når du har glemt et passord?

Hvem andre kan ha tilgang til kontaktene dine?

Spør elevene dine

Hvordan kan en fremmed få vite den personlige informasjonen som er forbundet med svarene dine på sikkerhetsspørsmål?

1. Innlegg på sosiale medier, nettsøk på offentlig informasjon, gjette flere ganger, kontakte vennene dine osv.

Har du noen eksempler på innlegg på sosiale medier med personlig informasjon?

1. For eksempel et Instagram-innlegg av katten din med navnet dens i bildeteksten, et bilde med et sted tagget eller offentlige bursdagsinnlegg.

Hvordan kan du bruke Google til å finne ut mer om en person og hacke passordet til vedkommende?

1. Hvis en søkemotor viser deg klassebildet til en person fra niende klasse i en skoleavis på nettet, kan du få vite navnet på læreren til vedkommende i niende klasse.

Del to

Fortell elevene dine

Det kan være veldig utrygt å publisere informasjon som inneholder svarene på sikkerhetsspørsmålene dine. Sørg for å velge sikkerhetsspørsmål som har svar bare du kjenner til. Du kan også lage svar på sikkerhetsspørsmål, så lenge du lagrer dem i en passordadministrator eller de er enkle å huske.

Nettsteder kan kontakte brukerne med et telefonnummer eller en e-postadresse som er forbundet med brukerens konto. Hvis en bruker glemmer passord, oppgir nettsteder ofte et midlertidig passord eller en hyperlenke som brukeren kan bruke til å tilbakestille passordet sitt med.

Spør elevene dine

Finnes det en trygg måte å sikre at personen som ber om det nye passordet, er brukeren?

Hva om du deler e-postadressen som er tilknyttet kontoen?

1. Det er som regel trygt å tilbakestille passord via en lenke, men hvis du deler en konto eller et passord med noen andre, utsetter det deg for risiko.

Fortell elevene dine

Sosial hacking kan skje ved at folk kontakter deg direkte og prøver å lure deg til å gi fra deg informasjonen din. Noen ganger kan folk sende deg en e-post og utgi seg for

å være en annen (f.eks. en venn, et familiemedlem eller noen fra banken) og be deg om å dele viktig informasjon med dem (f.eks. fødselsdato) for å verifisere identiteten din. Dette kan også være mer subtilt, som at noen hacker en venns konto på sosiale medier og sender deg (og potensielt også mange andre) en melding og spør etter fødselsdato og hvor du vokste opp. Hvis du mottar meldinger som virker rare, fra en venn, bør du først kontakte vennen din (utenfor den sosiale medieplattformen) for å finne ut om vedkommende faktisk sender innholdet.

Angrep som bruker en e-postadresse eller et nettsted som ser ekte ut, kalles phishing og kan føre til identitetstyveri. En identitetstyv kan for eksempel åpne kredittkort i ditt navn og bruke dem, noe som kan gjøre det vanskelig for deg å få kredittkort når du blir eldre.

Gjennom phishing kan tyven gi seg ut for å være deg og få tilgang til mer informasjon, slik at vedkommende kan snoke rundt i e-postene dine, sende meldinger til vennene dine og utgi seg for å være deg eller stjele pengene dine. I denne prosessen kan tyven også blokkere din tilgang til kontoen din ved å opprette et nytt passord som du ikke kjenner til.

Oppgave

Utdelingsark

Oppgave

Be deltakerne om å svare på de følgende spørsmålene og legge til svarene sine i form av tekst eller visualiseringer på utdelingsarket Lære om passord.

1. Hvilke tre ting lærte du i denne økten som du vil bruke neste gang du oppretter et passord?
2. Kan du komme på ett tilfelle hvor du synes det er OK å dele passordet ditt med noen andre?
3. Hvilke tre strategier kan du bruke for å dele passordet ditt på en trygg måte med noen andre?
4. Kan du komme på tre eksempler på hva som kan gå galt hvis et passord kommer på avveie?