

Vi holder hackerne ude – undervisning i informationssikkerhed

Undervisningsvejledning 15-25-årige

Indledning

Dette undervisningsmateriale er udviklet af /KL.7 for Digitaliseringsstyrelsen, KL og Danske Regioner i samarbejde med Medierådet for Børn og Unge og med hjælp fra UCC, Ældre Sagen, Styrelsen for It og Læring og Styrelsen for Undervisning og Kvalitet.

Undervisningsmaterialet er udviklet i forbindelse med en større kampagne om informationssikkerhed, som Digitaliseringsstyrelsen, KL og Danske Regioner lancerede i efteråret 2017.

Undervisningsmaterialet er udviklet med henblik på at gøre de konkrete råd fra kampagnen endnu mere håndgribelige og handlingsorienterede.

I denne vejledning vil vi gennemgå materialet overordnet og i dybden. Du vil også få anvisninger og tips og tricks til, hvordan du bruger det. Målgruppen for modulerne er borgere mellem **15 og 25 år**. De anbefalede antal deltagere på en kursusgang er **10**.

Du kan altid læse meget mere om hvert tema i undervisningsmaterialet på www.viholderhackerneude.dk

Hvordan bruger du materialet?

Materialet er inddelt i tema-moduler, en intro og en outro. Det betyder, at du frit kan sammensætte det oplæg, der passer til dine deltageres behov. Hvis du f.eks. allerede har undervist dem i at lave stærke kodeord, kan du tage fat i nogle af de andre temaer og sætte dem sammen, som du ønsker. Du skal blot tilpasse indholdsfortegnelsen i intro- og outro-delen (slide nr. 7 i ”Intro” og slide nr. 1 i ”Outro”).

Der er seks temaer: Falske beskeder, kodeord, e-handel, opdatering af programmer, sikkerhedskopiering og anvendelse af NemID. Modulet om NemID omhandler anvendelse af ny digital nøgleapp til lancering i maj og er derfor ikke udgivet. Der udarbejdes en beskrivelse af temaet ifm. udgivelse af undervisningsmodulet.

Der er tidsangivelser på hvert enkelt modul, så du har en idé om, hvor lang tid, det vil tage at komme igennem. Sæt evt. ekstra tid af til de moduler, der har mange øvelser, eller skær ned i antallet af øvelser.

Opbygning af materialet

Materialet er bygget op med en forholdsvis kort introduktion til problemstillingen og derefter en meget konkret øvelse. Dog har enkelte moduler ikke øvelser knyttet til sig.

Øvelserne fokuserer på én af følgende to ting: At deltagerne udfører en konkret handling, eller at deltagerne aktiverer den viden, de har fået via den informerende del af undervisningsmaterialet.

Den primære pointe med denne opbygning er at skrue ned for mængden af information om, hvad man bør gøre, for i stedet at guide deltagerne igennem de konkrete handlinger i undervisningssituationen.

I nogle af øvelserne er der screenshots, som kan være forældede, når du skal i gang med at bruge dem. De kan nemt udskiftes. Alternativt kan du vælge at vise det ”live” på din egen computer, mens du underviser. Det er faktisk til tider nemmere for deltagerne at følge med i.

Øvelserne er opdelt i tre typer:

1. Computerøvelse (her skal deltagerne bruge deres computer)
2. Mobiløvelse (her skal deltagerne bruge deres smartphone)
3. Fællesøvelse (foregår i plenum uden brug af digitale enheder)

Inden du går i gang:

- ✓ Har du selv gennemgå øvelserne? (Hvis ikke, er det en rigtig god idé, da det er meget nemmere at hjælpe deltagere, der går i stå, hvis man selv har prøvet det for nyligt).
- ✓ Er der lettilgængelige strømkilder til alle deltagere?
- ✓ Er der internetadgang til alle deltagere?

Forudsætninger:

- Deltagerne skal have egen computer med
- Deltagerne skal kunne bruge NemID
- Deltagerne skal have en Facebook-profil og kende deres kodeord (hvis de ikke har, så kan de godt kigge med hos sidemanden under denne øvelse)
- Deltagere, der bruger Mac, skal kunne huske deres Apple ID (da Mac-brugere skal kunne logge ind i App Store)

Kursets temaer

Undgå falske beskeder (Tid 1:00)

Ønsket adfærd

At få deltagerne til at lade være med at klikke på links i mails, der er fra (eller angiver at være fra) virksomheder, pengeinstitutter og offentlige myndigheder.

Overordnet om temaet

Der findes ikke længere skudsikre kendetegn på, at en besked er falsk. Det gør dette modul deltagerne opmærksomme på. Det centrale læringspunkt for deltagerne er altid at gå uden om links i beskeder fra virksomheder, pengeinstitutter og offentlige institutioner. I stedet opfordrer vi dem altid til at logge ind ved at gå direkte ind på f.eks. deres banks side.

Modulets øvelser

Modulet indeholder en fællesøvelse om at undgå den falske besked. Øvelse er ikke lavet til, at deltagerne efterfølgende skal kunne genkende en falsk besked. Den er lavet for at tydeliggøre, at det reelt er umuligt at skelne falske beskeder fra ægte. På den måde opdager deltagerne, at det er nødvendigt at tage visse forholdsregler omkring alle beskeder – uanset hvem afsenderen ser ud til at være.

Bliv klogere på dette tema

Forbrugerrådet Tænks app ”Mit Digitale Selvforsvar” indeholder både viden og alerts om falske beskeder, der er i omløb.

Hent appen her:

- App Store: <https://itunes.apple.com/us/app/mit-digitale-selvfor-svar/id1218846009?mt=8>
- Google Play: <https://play.google.com/store/apps/details?id=dk.taenk.mitdigitaleselvfor-svar>

Tjek 'om os'-siden før du handler (Tid 1:00)

Ønsket adfærd

At få deltagerne til at tjekke om en netbutik er reel.

Overordnet om temaet

Der findes mange fupbutikker på nettet, som udnytter brugernes tillid med

kopivarer og ugyldige handelsvilkår. Forbrugere bliver snydt og lovlige webshops mister omsætning. Imidlertid kan man relativt nemt tjekke en netbutik ved at læse ”om os”-siden, der som regel i en reel netbutik fortæller en troværdig historie.

Modulets øvelser

Øvelse 1 – Tjek altid ”Om os”-siden

Øvelsen præsenterer deltagerne for tre hjemmesider fra webbutikker. Her skal deltagerne gennemskue, hvilken af de tre hjemmesider, der er en fupbutik.

Øvelse 2 - Se efter e-mærket

Øvelsen præsenterer deltagerne for e-mærket og viser, hvor man skal finde e-mærkets certifikat.

Tag sikkerhedskopier (Tid 0:30)

Ønsket adfærd:

At deltagerne laver backup/tager en sikkerhedskopi én gang om ugen.

Overordnet om temaet:

At tage backup er et simpelt råd, men det er ikke altid nemt at følge. Særligt kan det være svært at forstå, hvorfor man som enkeltperson er interessant for hackere, og hvorfor hackere er interesserede i fx private ferie billeder. Det er heller ikke selve billederne, der er interessante, men derimod muligheden for at tjene penge ved at tage data som ’gidsel’ ved hjælp af ransomware, der gør private borgere og virksomheders data interessante. Har en hacker mulighed for at låse data, er der en indtægtsmulighed. Og den bliver udnyttet.

Der er en del afvejninger, man skal gøre for at opsætte ordentligt backup. Vi har vurderet, at det ikke kan håndteres på dette kursus.

Derfor er dette tema bygget op som en information om de forskellige løsninger (med fordele og ulemper), samt en beskrivelse af de to måder, man kan sikkerhedskopiere – men ingen øvelser.

Vi anbefaler, at du inden kurset undersøger, hvornår I har it-café næste gang, som du så kan henvise til.

Bliv klogere på dette tema:

Læs mere om forskellige muligheder for sikkerhedskopiering på kampagnens hjemmeside: <https://www.viholderhackerneude.dk/sikkerhedskopier>

Opdatér dine programmer (Tid 0:30)

Ønsket adfærd:

At få deltagerne til at sætte styresystemer (også på mobile enheder) til automatisk opdatering, så vidt det er muligt.

Overordnet om temaet

Der er mange, der tror, at det kun er vigtigt at opdatere programmer og styresystemer, hvis man vil have de nyeste funktioner og layout. Mange opdaterer endda med vilje ikke, fordi de frygter, at et nyt udseende eller nye funktioner vil gøre det mere besværligt at finde rundt i et program eller styresystem.

Faktum er imidlertid, at opdateringer ofte lukker meget vigtige sikkerhedshuller, og at det derfor er meget risikabelt ikke at opdatere styresystemer og programmer regelmæssigt.

Udover at ændre udseende og byde på nye funktioner kan opdateringer have de to ulemper, at 1) de kan gøre din enhed langsommere og 2) de kræver, at du accepterer en hel masse (nye) vilkår. Det er dog ulemperne værd at holde hackerne ude af sin computer og mobiltelefon, og derfor er begge ulemper adresseret i informationsdelen.

Modulets øvelser

Øvelse 1: Tjek om dit styresystem til computeren er opdateret

Øvelsen er en guide til at tjekke, om Windows eller macOS er opdateret. Hvis deltagerens Windows ikke er opdateret, vil det være nødvendigt at finde ud af, hvilken version af Windows, de har. Som regel kan de blot klikke på en knap og opdatere, men en gang imellem vil der være deltagere, der stadig har Windows 7, 8, 10 osv.

Hvis det er tilfældet, vil det som regel være forbundet med en større udgift at opdatere. Derfor er der ikke andet at gøre end at 1) anbefale dem at opdatere til et nyere styresystem og 2) hvis du kan, henvise dem til den lokale it-café for at få hjælp undervejs.

Øvelse 2: Tjek om din mobilts styresystem er opdateret

Øvelsen er simpelt bygget op uden en konkret screenshot-vejledning. Det skyldes, at især Android er meget vanskeligt at vise screenshots fra, da der er mange versioner i omløb. Tjek gerne nogle af nedenstående links igennem, inden du går i gang med øvelsen:

Bliv klogere på dette tema:

Sæt dine apps og programmer til at opdatere automatisk:

- iPhone /iPad /iPod Touch: <https://support.apple.com/da-dk/HT202180#iOS>
- Mac computer: <https://support.apple.com/da-dk/HT202180#computer>
- Android: <https://support.google.com/googleplay/answer/113412?hl=da>
- Windows PC: <https://support.microsoft.com/da-dk/help/15081/windows-turn-on-automatic-app-updates>
- Hvilken version browser bruger du? <http://www.whatbrowser.org/intl/da/>

Lav dine kodeord længere og slå to-trins-login til (Tid 1:45)

Ønsket adfærd

Deltagerne skal lave længere kodeord, slå to-trins-login til og undlade at genbruge kodeord.

Overordnet om temaet:

Dette tema er det sværeste af dem alle sammen. Der er også sat 1:45 af til det, og det er nødvendigt. Hvis du vil undervise i dette, skal du ikke undervise i andre af temaerne i samme omgang. Det er øvelserne, der er vanskelige, og du kan derfor let udelade nogle af øvelserne. Husk, at de to ”LastPass”-øvelser hører sammen – det fremgår af selve undervisningsmaterialet.

Kodeord er et komplekst tema, fordi der er mange ønskede handlinger, som indebærer andre nødvendige handlinger. Hvis vi f.eks. vil have deltagerne til at undlade at genbruge kodeord, skal vi også hjælpe dem med at gøre det nemt at administrere og huske hvilke kodeord, der hører til hvilke profiler – heraf øvelsen med password-manageren.

Øvelser

Øvelse 1. Hold styr på alle profilerne med en passwordmanager

Øvelsen er en guide til at oprette en profil på LastPass, implementere LastPass i browseren og indsætte et login ind i LastPass fra Facebook.

LastPass er, som det fremgår af undervisningsmaterialet, blot én ud af flere mulige password-managere. LastPass er en af de mest populære gratis managere. Denne øvelse skal ses som en mulighed for at forstå, hvad en passwordmanager kan, og hvordan den fungerer. LastPass er naturligvis fin at fortsætte med, hvis deltagerne aldrig kommer videre. Dette står som noter i undervisningsmaterialet.

Guiden er ikke så udførligt billeddokumenteret. Det skyldes, at det ser forskelligt ud fra browser til browser, og at guiden til de forskellige browsere er ret udførlig, når man går den igennem.

Den sidste del af processen, hvor man skal oprette et kodeord til passwordmanageren, er dog dokumenteret. Når deltagerne laver dette kodeord, skal det være sikkert, og de skal kunne huske det.

Den sidste del af øvelsen går ud på at prøve password-manageren af ved at lade den gemme deltagerens Facebook-login, så de kan prøve at logge ud og logge ind igen.

Øvelse 2. Hent LastPass til din mobil og kopiér ét kodeord

Denne øvelse kan udelades, men kan ikke stå alene uden øvelse nr. 1. Den går meget lavpraktisk ud på at lade deltagerne opleve, at en passwordmanager også er nem at anvende på en mobil enhed.

Øvelse 3. Er din profil blevet kompromitteret?

Denne øvelse er en guide til at tjekke, om deltagerens e-mail dukker op på lister over e-mails/profiler, der er blevet hacket. Denne oplysning hentes fra flere forskellige steder og du kan læse meget mere om det på hjemmesiden www.havei-beenpwned.com

Alt efter resultatet, kræver det forskellige handlinger:

Grøn betyder, at der er intet galt og ingen handling er påkrævet

Rød betyder, at profiler hos specifikke tjenester er blevet kompromitteret (f.eks. Dropbox). Det kræver, at man skal ændre sit kodeord på de relevante tjenester. Rød kan også indebære, at man optræder på en liste, som er blevet solgt på the dark web. Det kræver, at man ændrer sit kodeord på de vigtigste login, hvor den pågældende e-mail anvendes som brugernavn.

Giv deltagerne lidt tid til at ændre kodeord. Nogle deltagere har dog flere e-mail-adresser, så husk at sætte en max-tidsgrænse på f.eks. 10 min.

Husk: Deltagerens status vil ikke ændre sig på hjemmesiden, selvom de har udbedret problemet.

Øvelse 4 – Aktiver to-trins-login på Facebook

Øvelsen er en trin-for-trin-guide til at aktivere to-trins-login på Facebook. Denne øvelse er ikke så browserspecifik, men der er en risiko for, at Facebook har ændret enten udseende eller måde at slå to-trins-login til på.

Bliv klogere på dette tema

Tjek evt. dine egne profiler på <https://haveibeenpwned.com> eller <https://breachalarm.com>.

Guides til at slå to-trins-login til på forskellige tjenester:

- LastPass: <https://helpdesk.lastpass.com/da/multifactor-authentication-options/>
- Facebook: <https://www.facebook.com/help/148233965247823>
- Google-konto: <https://www.google.com/intl/da/landing/2step/>
- Apple-ID: <https://support.apple.com/da-dk/HT204915>
- Dropbox: https://www.dropbox.com/da_DK/help/security/enable-two-step-verification
- Microsoft: <https://support.microsoft.com/da-dk/help/4028586/microsoft-account-turning-two-step-verification-on-or-off-for-your-mic>
- Flere guides samlet ét sted: <https://www.turnon2fa.com/tutorials/>

Hold dit NemID for dig selv (Tid 0:40)

Ønsket adfærd:

At deltagerne ikke tager billeder af deres NemID, samt at deltagerne bliver i stand til at anvende NemID nøgleappen.

Overordnet om temaet:

Den første del er nem at formidle, fordi den ønskede adfærd er meget enkel. Det vigtigste er: Hvad skal man gøre, hvis man frygter, at ens NemID er blevet kompromitteret. Her er en sammenligning med spærring af Visa/Dankort god, da det er noget, de fleste kender.

Desuden er der tilføjet et slide med måder at spærre ens NemID nøglekort på.

OBS: Det kræver pas eller kørekort for at bestille et nyt nøglekort online.

Unge-målgruppen kan have svært ved at følge rådet, da mobilen er det eneste, de altid har på sig. Derfor giver det en naturlig overgang til anden del om nøgleappen.

Anden del, introduktionen til NemID nøgleappen, forudsætter at deltagerne har downloadet appen, at appen er aktiveret og at deltagerne har deres nøglekort/nøgleviser med.

Det vigtigste med øvelserne er, at deltagerne forstår, hvordan appen fungerer, herunder godkendelse og afvisning af anmodninger. Derudover skal det også gøres klart for deltagerne, at NemID nøgleappen er et supplement til nøglekortet, og de aldrig må smide deres nøglekort væk.

Øvelser:

1. Log på selvbetjeningen med nemid.nu med NemID nøgleapp

Øvelsen forudsætter, at deltagerne har downloadet appen, at appen er aktiveret og at deltagerne har deres nøglekort/nøgleviser med. I øvelsen skal deltagerne logge på selvbetjeningen på nemid.nu ved hjælp af nøgleappen og uden at bruge det fysiske nøglekort.

2. Afvis en anmodning i NemID nøgleappen

Denne øvelse forudsætter også, at man har appen aktiveret. I øvelsen skal deltagerne forsøge at logge på selvbetjeningen på nemid.nu og så afvise anmodningen i NemID nøgleappen. Formålet er at skabe en bevidsthed om, hvem der er afsender på anmodningen.

Bliv klogere på dette tema:

- Spørgsmål og svar om nøgleappen: www.nemid.nu/app

Bliv klogere på informationssikkerhed

Links til værktøjer

- Forbrugerrådet Tænks app ”Mit Digitale Selvforsvar”, der indeholder både viden og alerts om falske beskeder, der er i omløb.
 - App Store: <https://itunes.apple.com/us/app/mit-digitale-selvfor-svar/id1218846009?mt=8>
 - Google Play: <https://play.google.com/store/apps/details?id=dk.taenk.mitdigitaleselvfor-svar>

- DigiSafe er en app og hjemmeside, som indeholder læringsværktøjer om NemID, handel på internettet, sociale medier og E-boks til unge med særlige behov. Læs mere på <http://digisafe.dk>.
- <https://viholderhackerneude.dk/> indeholder mere baggrundsmateriale om de seks hackerråd og henviser til yderligere materiale.
- <https://www.borger.dk/internet-og-sikkerhed> indeholder en lang række artikler og spørgsmål/svar om internet og sikkerhed.

Vil du lære mere?

eKurser.nu er en portal, der samler små kurser om hverdags-it. Med kurserne kan du lære at udnytte services, som stilles til rådighed på internettet. De kurser, du finder på eKurser.nu, ligger emnemæssigt inden for de emner, som folkebibliotekerne traditionelt vejleder i på it-området. Det vil sige kurser i selvbetjeningsløsninger fra det offentlige, bibliotekernes egne netjenester, brug af computer, søgning på internettet samt de muligheder på internettet, som kan have almen interesse. Læs mere på www.ekurser.nu.

God fornøjelse!