IT's tjekliste og guide til træning af medarbejderne

eloomi

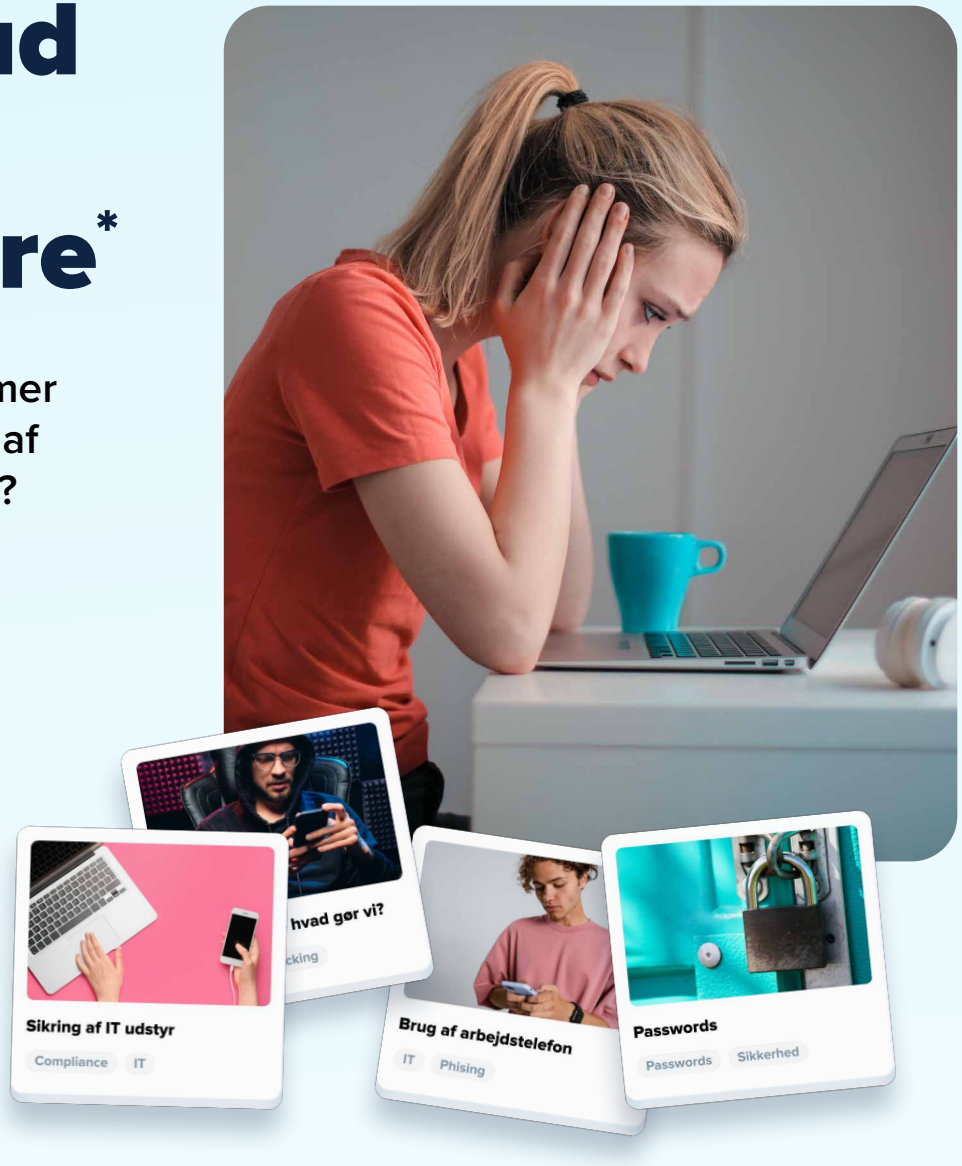
Gør medarbejderne til en del af jeres cyberdefence

Over 50% af alle brud på IT-sikkerheden skyldes medarbejdere*

Vi bruger mange kræfter på at beskytte vores systemer mod cyber-kriminelle. Men hvad hjælper det hvis en af dine medarbejdere kommer til at lukke hackeren ind?

Flere undersøgelser viser, at størstedelen af alle brud på IT-sikkerheden skyldes manglende viden eller uforsigtighed hos medarbejderne. 70%* vil klikke på linket i en spear phishing-mail (hvor offeret er nøje udvalgt). 30%* vil klikke på en almindelig phishing mail, hvis de ikke har modtaget undervisning i at spotte det.

Medarbejdernes handlinger udgør generelt en stor risiko for IT-sikkerheden. Dine kolleger burde være en del af jeres cyberdefence – men kan reelt være det stik modsatte.



* Kilde: Center for IT-sikkerhed

Nemt, pædagogisk, underholdende og automatisk

Uddan medarbejderne i cyberdefence

- Er medarbejderne klædt på til at modstå den stadig mere udspekulerede cyberkriminalitet?
- Er der styr på hvem, som har modtaget hvilken træning?
- Bliver nye medarbejdere uddannet? Eller bliver det glemt?
- Der er hele tiden nye trusler at være forberedt på. Er I det?

✓ Træning og test af medarbejderne er vigtigt for at undgå hackerangreb, data-lækage eller anden cyber-kriminalitet.

✓ eloomi er den nemme og fleksible e-learning platform, dine medarbejdere kan bruge, når de har tid.

✓ Det er nemt, pædagogisk, underholdende og baseret på video, så medarbejderne hurtigt og løbende bliver opgraderet og tjekket – og du kan altid følge med i, hvor langt de er kommet.

✓ Din opgave som ansvarlig for IT-sikkerhed bliver derfor meget nemmere.

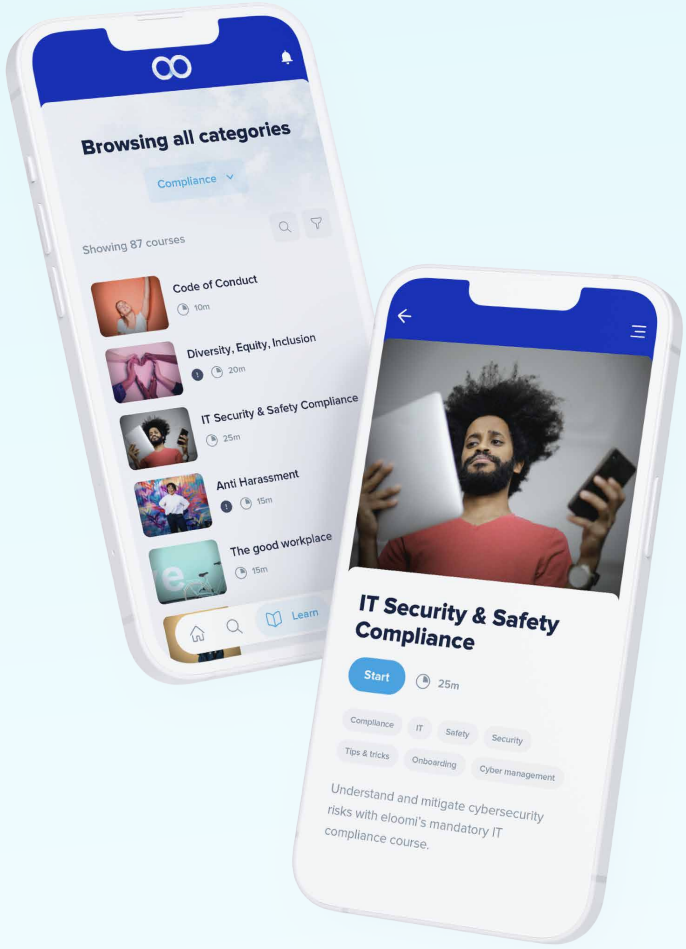
Den IT-ansvarliges cyber-sikkerheds tjekliste
(og lektionsplanlægger)

Vi har gjort det nemt og praktisk. Brug listen over eloomi IT-sikkerheds e-learning titler som din tjekliste.

☒ **Sæt kryds,** hvis du mener, dine medarbejdere har helt styr på det.

☐ **Lad boksen stå tom,** hvis du ikke kan sige, at du er 100% sikker på det.

Alle de tomme bokse viser både hullerne i jeres IT-sikkerhed OG jeres anbefalede lektionsplan i eloomi.



Er IT-sikkerheden gennemhullet?

Gennemgå din tjekliste og se resultatet

Vi kan arbejde overalt – helt sikkert. Tror vi.

1

Dårlige passwords

2

Overholder ikke GDPR! Eller regler for sensitiv information

3

Genkender ikke phishing og scams

4

Ikke styr på generel IT-sikkerhed

5

Glemmer den fysiske sikkerhed

6

Kan ikke identificere malware og hacking-forsøg

7

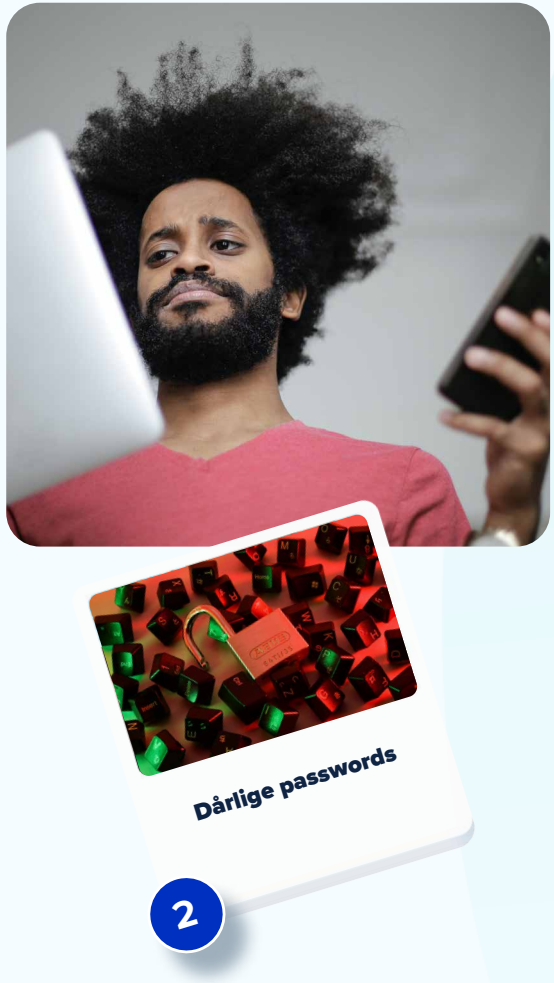
Resultat af testen

✓

1 Vi kan arbejde overalt – helt sikkert. Tror vi.

Vi arbejder overalt. På forskellige enheder og wifi-forbindelser. Er du helt tryg ved dine medarbejderes adfærd? Sæt kryds, hvor du føler dig helt sikker og ved at dine kolleger ved, hvad de må og ikke må.

- [ ] **Gratis wifi.** Det er nemt for hackere at monitorere, hvad andre mennesker laver, mens de er tilsluttet samme gratis wifi.
- [ ] **Hjemme wifi.** Sørg altid for, at dit wifi hjemme er sikkert og krypteret.
- [ ] **Juice Jacking.** Oplad altid dine enheder med din egen oplader og dit eget kabel ellers kan du ikke garantere it-sikkerheden.
- [ ] **Hjemme wifi (ferie-version).** Lær at bruge wifi sikkert under ferier, eller hvis du arbejder i udlandet.
- [ ] **Fysiske medier.** Det er nemmere at stjæle fysiske data end hacke databaser og gætte passwords.
- [ ] **Flytbare medier.** Der er en risiko forbundet med at bruge flytbare medier. Vær sikker på at kryptere dine dokumenter for det tilfælde, at din USB-nøgle bliver væk eller stjålet.
- [ ] **Deling på sociale medier.** Vær forsigtig med, hvad du deler på sociale medier.
- [ ] **Ukendte netværk.** Hackere kan sætte et wifi access point op, og hvis du forbinder til det, kan meget af din kommunikation blive monitoreret eller manipuleret.
- [ ] **Værdigenstande i bilen.** Hvis du er betroet klassificeret information på elektroniske medier og print, er det ikke sikkert at efterlade dem i bil.
- [ ] **VPN - arbejde hjemmefra.** En VPN-forbindelse skaber en virtuel tunnel mellem PC'en eller andre enheder og virksomhedens server.
- [ ] **Håndtering af arbejdsmail.** Arbejdsmailen bør kun anvendes til arbejdsrelaterede formål - og ikke kun på grund af work-life balance...
- [ ] **Hjemmearbejde - insider trussel.** Refererer normalt til ansatte, der lækker data, men data kan også lækkes via venner.
- [ ] **Hjemmearbejde - uovervåget PC.** Hvis du efterlader din PC ulåst eller uovervåget, kan det skabe alvorlige problemer, hvis nogen har adgang til den.



2 Dårlige passwords

Er dine medarbejdere 100 meter mestre i passwords? Listen herunder afslører, hvor der er huller, som bør dækkes ind af undervisning.

- [ ] **Håndtering af passwords.** Mange forskellige passwords er noget af en udfordring, men at skrive dem ned eller gemme dem ved PC'en er præcis, hvad hackeren håber på...
- [ ] **Multifaktor godkendelse.** Hackere er gået efter passwords, siden internettet så dagens lys, og de er forbavsende dygtige til at stjæle dem og endda gætte dem.
- [ ] **Pass-fraser.** Glem komplekse passwords. Opfind i stedet dit helt eget password af flere ord. Det er nemmere at huske og i øvrigt mere sikkert.
- [ ] **Password manager.** Vi vil altid have brug for passwords, men det kan være svært at huske dem.
- [ ] **Passwords.** Det bedste password består af små og store bogstaver, symboler og tal.
- [ ] **Samme password.** Det er noget af en opgave at holde styr på mange passwords, men her får du grundene til, at du aldrig skal bruge samme password til flere konti.
- [ ] **Password sharing.** Nogle ting deler man bare ikke.

3 Overholder ikke GDPR! Eller regler for sensitiv information

Kender dine medarbejdere reglerne for omgang med personfølsomme oplysninger? Eller risikerer de at behandle data letsindigt og kompromittere både sig selv og jeres virksomhed? Det er bedre at forebygge end at helbrede. Skal der tankes lidt viden op om emnerne herunder?

- [ ] **Autofill.** Nogle gange lækkes fortroligt materiale, fordi e-mail afsenderen har travlt eller er distraheret og får sat den forkerte modtager på.
- [ ] **Clean desk.** Vores skriveborde er ikke sikre steder at opbevare fortroligt materiale.
- [ ] **Firma kreditkort.** Undgå at cyberkriminelle bruger jeres organisations kreditkort til deres shoppingture.
- [ ] **Datalæk.** En datalæk er en bevidst eller ubevidst frigivelse af privat/fortroligt materiale til et miljø, man ikke stoler på.
- [ ] **Dobbelttjek før du stoler på noget.** Man skal altid overveje muligheden for, at en e-mail konto er blevet hacket, og at meddelelser og forespørgsler fra kolleger eller forretningspartnere kan være falske.
- [ ] **Dumpster diving.** En hel masse værdifuld information kan findes, hvis man gennemgår affaldet fra papirkurvene i jeres virksomhed.
- [ ] **GDPR - personlig information.** Hvis en kunde beder jer glemme alt om dem, er I nødt til at efterkomme det.
- [ ] **Håndtering af fortroligt materiale.** Din personlige e-mail og dit online datalager er normalt ikke så sikker som din arbejdsmail.
- [ ] **Sikker opbevaring af data.** Kan jeres kunder betro jer deres information? Beskytter I den lige som jeres egen?
- [ ] **Netværksprinter.** Den største risiko, når du anvender netværksprinter, er at vælge den forkerte.
- [ ] **Online oprettelse af PDF'er.** Vælg ikke magelighed frem for sikkerhed.
- [ ] **Print.** Når du printer, så husk af skaffe dig af med printene igen på en sikker måde.
- [ ] **Deling af information.** Vær ekstra forsigtig med, hvem du deler fortroligt materiale med. Vær sikker på, at modtageren har den fornødne autoritet til at modtage materialet.
- [ ] **Social engineering.** Del ikke fortroligt materiale med uautoriserede personer. Heller ikke dine bedste venner.
- [ ] **Unødvendige data.** Læs de privatlivsregler, det er vigtigt for dig at kende i dit daglige arbejde. Hvis du fejler, kan det medføre, at din arbejdsplads får en bøde.

4 Genkender ikke phishing og scams

Cyberkriminelle har “tasken” fuld af værktøjer, som er designet til at ramme svage punkter og lokke “svage sjæle”. Kan dine medarbejdere spotte en phishing e-mail, eller åbner de døren til jeres systemer og data på vid gab? Her er en vigtig tjekliste over viden til at stække hackerne.
Sæt kryds, hvor I har styr på det:

- [ ] **CEO scam.** Dobbelttjekker I altid usædvanlige forespørgsler fra chefen omkring finansielle transaktioner.
- [ ] **Tjekke kontonumre:** Svindlere kan nemt sende en falsk faktura ind i jeres bogholderi. Dobbelttjekker I altid nye kontonumre?
- [ ] **Korrekte links**. Kig nøje på links i e-mails, før du klikker på dem for at sikre, at de leder dig det rigtige sted hen.
- [ ] **Dobbelttjek før du stoler på noget.** Vær opmærksom på, at der altid kan være nogen, der “lytter med” på dine mail-konversationer.
- [ ] **Extortion e-mails.** Cyber-kriminelle benytter sig af og til at vores svage punkter til pengeafpresning eller til at skaffe sig mere information.
- [ ] **Ondartede vedhæftninger.** Al mail er ikke nødvendigvis god mail. Åbn aldrig vedhæftninger eller links fra ukendte afsendere.
- [ ] **Risici ved online handel.** Den største risiko ved at shoppe online er ikke bare at kunne miste sine penge...
- [ ] **Phishing der opfordrer til handling nu:** Hvis en e-mail fortæller, at det er nødvendigt at udføre en handling her og nu, er det et af de mest almindelige tegn på, at det er en phishing e-mail.
- [ ] **Phishing – med påtrængende nødvendighed.** Hvis en e-mail indeholder en form for nødvendighed, er det et af de mest almindelige tegn på, at det er en phishing e-mail.
- [ ] **Romantiske scams - social engineering.** Hold øje med advarselstegnene i nye digitale forhold. At spille på menneskers ensomhed er en meget udbredt taktik blandt scam’ere.
- [ ] **Spear Phishing.** At kende nogens interesser og hobbies er værdifuldt og hjælper hackere til at lave spear phishing e-mails, som er specielt designet til den pågældende person.

- [ ] **Spear Phishing II.** Vær forsigtig med, hvad du deler på sociale medier. Cyberkriminelle kan bruge interesser eller hobbies til at lave målrettede phishing e-mails, som ser helt almindelige ud.
- [ ] **Vishing.** Når en person ringer til dig og bruger en falsk grund eller et krav til at afgive følsomme oplysninger - som for eksempel dit CPR-nummer eller kreditkort information - kaldes det vishing.

5 Ikke styr på generel IT-sikkerhed

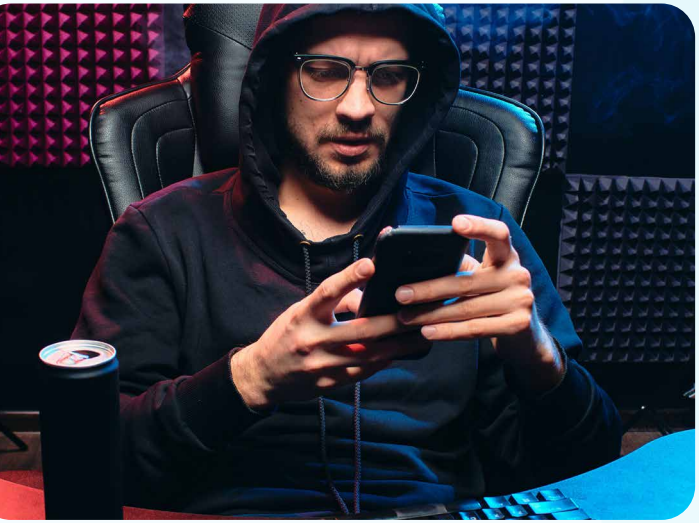
Har dine medarbejdere en adfærd, som gør det svært for hackerne at snige sig ind? Er de opmærksomme på alle farerne - og de nye, der løbende opstår? Det er spørgsmålet, og du kan bruge tjekpunkterne her til at finde hullerne, som skal lukkes med IT-sikkerheds e-learning.

- [ ] **Kædemails.** Det er højest usandsynligt, at en kædemail indeholder relevant information. Hvis du sender den videre, spilder du bare nogens tid.
- [ ] **HTTPS-forbindelser.** En web-adresse, der starter med HTTPS er kryperet og meget sikrere end en adresse, der starter med HTTP.
- [ ] **Misinformation - tjek kilden.** Alt, der glitrer, er ikke guld, lige som alt på internettet ikke er sandt. Vær forsigtig med, hvad du tror på og åbner online.
- [ ] **Lås mobiltelefonen.** Dokumenter, memos, e-mails og kontakter kan blive stjålet, hvis du efterlader din telefon ulåst.
- [ ] **Popups.** Ved du, hvordan du lukker en pop-up ned på den rigtige måde?
- [ ] **Sikkerheds-opmærksomheds træning.** Når vi kender farerne omkring os, kan vi tage vores forholdsregler og navigere rundt mere sikkert.
- [ ] **Sikkerhedskultur.** At grundlægge og opretholde en god sikkerhedskultur på arbejdspladsen er noget, som alle virksomheder burde stræbe efter.
- [ ] **Installation af software.** Gør arbejdet nemmere for jeres IT-teknikere ved ikke at installere software på arbejds-PC'en uden tilladelse.
- [ ] **Tænk før du poster noget.** Tænk dig om en ekstra gang, inden du poster eller kommenterer noget på sociale medier. Hvordan vil det påvirke dig og din arbejdsplads?
- [ ] **Overvej en ekstra gang.** Interne e-mails kan være sjove – men vi må ikke glemme e-mail etiketten.
- [ ] **Uovervåget PC.** At efterlade din PC ulåst og uovervåget kan forårsage alvorlige problemer, hvis en anden har adgang til den.

- [ ] **Opdater din software.** Hvis du opdaterer din software, hver gang du får en notifikation, kan du spare mange problemer og meget tid i det lange løb.
- [ ] **Zoom bombing.** Med nye teknologier følger nye store risici.

6 Glemmer den fysiske sikkerhed

Kunne en uvedkommende snige sig ind til en firmafest på jeres arbejdsplads og skaffe sig adgang til fortroligt materiale? Har I en politik for adgang? Den fysiske side af IT-sikkerhed er vigtig. Tjek faldgruberne her.
Er der noget, som I skal have fortalt medarbejderne mere om?



- [ ] **Luk den rigtige ind (Halloween special).** Skab sikkerhed for, at det alene er ansatte, der har adgang til arbejdspladsen - både i arbejdstiden og udenfor.
- [ ] **Privacy skærme.** At benytte en privacy skærm er en meget billig måde at øge sikkerheden væsentligt på, når der arbejdes uden for kontoret.
- [ ] **Skulder-surfing.** Cyber-kriminelle nøjes ikke med at hacke eller gætte dit password. Nogle gange ser de dig simpelt hen skrive det.
- [ ] **Stakeout.** Vær altid opmærksom på omgivelserne.
- [ ] **Tailgating.** Hackere bruger venlige fremmede til at skaffe sig adgang til lukkede områder.
- [ ] **Tailgating II.** Alle arbejdspladser burde have en restriktiv politik og nedskrevne procedurer for at undgå, at uvedkommende får adgang til lukkede områder.

7 Kan ikke identificere malware og hacking-forsøg

Spyware, malware, ransomware. De fleste har hørt om dem – men hvordan identificerer I hackerens foretrukne døråbnere, og hvad gør I efterfølgende? Hvis du mener, dine medarbejdere er helt skarpe på her, kan du tage det helt roligt. I modsat fald var det måske en idé med lidt træning?

- [ ] **Risiko ved konferencer.** Vær opmærksomme på eksterne harddiske og ladestationer.
- [ ] **Keylogger.** Tjek portene i din PC jævnligt for ukendte enheder.
- [ ] **Microsoft risiko.** Slå ikke editing til på et Office dokument, hvis du ikke er helt sikker på at ville gøre det.
- [ ] **Mobiltelefon aflytning.** Pas på! Malware kan blive installeret på din telefon og åbne kameraet og slå mikrofonen til og lytte med på dine konversationer.
- [ ] **Personlige USB-drev.** Din hjemme-PC er ikke så godt beskyttet som din arbejds-PC.
- [ ] **Ransomware.** Er virus eller malware, som krypterer data på din PC eller på hele dit netværk.
- [ ] **Ransomware angreb.** At acceptere software opdateringer eller downloads fra en hjemmeside er “risky business”.
- [ ] **Virusspredning.** Hvis du installerer ikke godkendt software på din PC, kan hele kontornetværket blive inficeret.
- [ ] **Spyware.** Hvordan kommer spyware ind i din PC. Her er én måde...
- [ ] **Spyware i vedhæftninger.** Når det kommer til at sprede virus, spyware eller anden malware, er ingen metode mere populær blandt hackere end vedhæftninger.
- [ ] **Tab af USB-nøgle.** Hvad gør du, hvis du finder en usb-nøgle. Uanset hvad, så lad være med at sætte den ind i din PC.

Resultat

0	78
Har vi helt styr på	Potentielle huller i IT-sikkerheden

Det er en lang tjekliste! Var der mange huller?

Det er nemlig utrolig meget, dine kolleger skal vide, hvis I skal være mere sikre.

- ✓ Det er heldigvis nemt og underholdende at rette op på med eloomi – og nu har du endda allerede din lektionsplan.
- ✓ Det vil vi gerne vise dig – book en demo her!

eloomi er fleksibel e-learning, som dine medarbejdere vil elske!

Og gør det nemt for dig!

Nye og kommende medarbejdere stiller højere og højere krav til arbejdspladsens evne til at kommunikere digitalt og fleksibelt. Træning er bestemt ingen undtagelse! Derfor skal du vælge læringsplatform med omhu.

eloomi er den prisvindende og innovative e-learning platform, som er skabt til at honorere disse krav. Den sætter helt nye standarder for arbejdet med kompetenceudvikling, motivation og målstyring.

✓ **Globalt dansksproget læringsindhold**
- udviklet i samarbejde med førende eksperter inden for IT-sikkerhed.

✓ **Fleksibilitet**
Giv dine kolleger mulighed for at tage lektionerne, hvor og hvornår det passer dem.

✓ **Rapportering og automatisering:**
Hold øje med, om alle har gennemført den nødvendige træning og sørg for, at alle automatisk får tildelt relevante kurser.

Skærp dit værn mod cyber-angreb - start nu!

- ✓ Med eloomi eliminerer I uvidenhed om IT-sikkerhed, og risikoen for succesfulde cyber-angreb.
- ✓ I øger bevidstheden om alvoren af IT-sikkerhed hos alle ansatte, og skaber en stærk og konsistent IT-sikkerhedskultur.

Book demo →

Start allerede i dag