ET SIKKERHEDSTJEK
PÅ 15 MINUTTER



Er jeres hjemmeside sikret mod angreb?

Seks hurtige tjek, som hjælper jer med at se, om jeres hjemmeside er sårbar over for kriminelle, og hvad I kan gøre ved det.

magnetic

Anna Hessenbruch · november 2026

HVORFOR DENNE TJEKLISTE

Jeres hjemmeside kan fortælle fremmede mere, end I tror.

Efter de seneste sårbarheder i PHP blev jeg nysgerrig på, hvor mange organisationer der kan have svagheder på deres hjemmeside uden at vide det. Så jeg kiggede på 40 af Danmarks største indsamlende organisationer og brugte kun det, som enhver besøgendes browser allerede kan se.

40
af landets største NGO'er er gennemgået

77 %
viser åbent, hvilket system deres hjemmeside kører på

45 %
har et maildomæne, som svindlere kan sende falske mails fra

De fleste rettelser går hurtigt, og I kan selv køre alle tjekkene.

PHP-fejlen ramte en bestemt Windows-opsætning og gik derfor stort set uden om NGO'erne. Hverdagens risici ligger tættere på, fx forældet software, maildomæner, som andre kan sende fra, og sider, der viser, hvilket system de kører på. Styrelsen for Samfundssikkerhed vurderer truslen fra cyberkriminalitet mod Danmark som meget høj.

Gå de seks tjek igennem, eller spring til side 6, og lad en AI gøre det for jer.

Kilder: Styrelsen for Samfundssikkerhed, Cybertruslen mod Danmark 2025. PwC, Cybercrime Survey 2025. magnetics gennemgang af offentligt synlige indstillinger for hjemmeside og mail hos 40 af Danmarks største indsamlende organisationer, oktober 2026.

TJEKKENE

Seks tjek til jeres egen side

Hvert tjek tager omkring et minut. Til hvert tjek står der, hvad det ser på, og hvorfor det er vigtigt, efterfulgt af et gratis værktøj.

01

Bruger jeres side altid en sikker forbindelse?

Tjekket viser, om jeres side altid åbner med https:// og en hængelås. Det betyder, at oplysninger mellem de besøgende og jeres side er krypteret.

Uden kryptering kan alt, hvad en giver eller et medlem skriver, fx navn, mail eller kortoplysninger, blive læst eller ændret undervejs, for eksempel på et offentligt wifi.

GRATIS TJEK

ssllabs.com/ssltest

Indtast jeres adresse, og vent et minut eller to. Karakteren A eller A+ er god. B eller lavere er værd at tage op.

SPØRG DEM, DER DRIVER SIDEN

Bliver alle sider tvunget over på https, og er HSTS slået til?

02

Viser jeres side, hvad den er bygget med?

Mange hjemmesider viser navn og version på den software, de kører på, fx WordPress 6.4, i deres kode.

Når der bliver fundet en svaghed i en bestemt version, bruger kriminelle automatiske værktøjer til at finde sider, der kører den. Viser I jeres version, kan jeres side havne på den liste.

GRATIS TJEK

builtwith.com

Indtast jeres adresse, og kig under »CMS« og »Web Server«. Står der et versionsnummer ved softwarens navn, kan alle se det.

SPØRG DEM, DER DRIVER SIDEN

Viser vores sider navn eller version på vores software, og kan det skjules?

03 Er jeres software opdateret?

De fleste NGO-hjemmesider kører på et CMS, fx WordPress eller Drupal, med tilføjelser som plugins og temaer. Alle dele skal opdateres løbende.

Opdateringer lukker ofte sikkerhedshuller, som allerede er offentligt kendte. Forældet software er en almindelig vej ind på en hjemmeside.

GRATIS TJEK

sitecheck.sucuri.net

Indtast jeres adresse, og se efter advarsler om forældet software, plugins eller kendte sårbarheder. Scanningen ser kun det offentlige, så et rent resultat er et godt tegn snarere end en garanti.

SPØRG DEM, DER DRIVER SIDEN

Bliver vores kernesoftware, plugins og temaer opdateret jævnligt, og hvem holder øje med det?

04 Kan andre sende mails i jeres navn?

Tjekket ser på tre indstillinger, SPF, DKIM og DMARC, som fortæller mailudbydere, hvilke mails der reelt kommer fra jeres domæne.

Mangler de, kan kriminelle sende mails, der ser ud til at komme fra jer, fx med en opfordring til at give penge til en falsk konto. I PwC's Cybercrime Survey 2025 peger 62 % af de ramte virksomheder på phishing.

GRATIS TJEK

mxtoolbox.com/dmarc.aspx

Indtast jeres domæne, altså det, der står efter @ i jeres mailadresse. Se efter en DMARC-post med p=quarantine eller p=reject. Står der p=none, eller findes der ingen post, kan falske mails stadig nå frem.

SPØRG DEM, DER DRIVER SIDEN

Har vi SPF, DKIM og DMARC på plads, og står DMARC til »quarantine« eller »reject«?

05 Bruger jeres side browserens sikkerhedsindstillinger?

Hjemmesider kan sende instruktioner, såkaldte sikkerheds-headers, som fortæller de besøgendes browser, hvordan den skal opføre sig sikkert på jeres side.

Slipper der skadelig kode ind på en side, fx via et kompromitteret plugin eller en reklame, kan indstillingerne stoppe koden eller begrænse, hvad den kan, fx at kopiere oplysninger fra en formular.

GRATIS TJEK

developer.mozilla.org/en-US/observatory

Indtast jeres adresse, og se karakteren. A eller B er godt. C eller lavere betyder, at nogle beskyttelser mangler, og resultatet viser hvilke.

SPØRG DEM, DER DRIVER SIDEN

Bruger vi en Content-Security-Policy og de øvrige almindelige sikkerheds-headers?

06 Hvem holder det hele opdateret?

Tjekket handler om mennesker frem for teknik: om nogen har ansvaret for, at hjemmeside og mail forbliver sikre over tid.

Indstillinger ændrer sig, når siden bliver opdateret, leverandører skifter, eller nye tjenester kommer til. Hver rettelse holder, så længe nogen har ansvaret for den.

GRATIS TJEK

internet.nl

Siden er på engelsk. Kør både hjemmesidetesten og mailtesten, og gem resultaterne. Gentag hvert kvartal. Falder scoren, har noget ændret sig, og det bør undersøges.

SPØRG DEM, DER DRIVER SIDEN

Hvem har ansvaret for sikkerheden på vores hjemmeside og mail, og hvordan ved vi, at opdateringerne bliver lavet?

TIL BETALTE ERHVERVSKONTI

Lad en AI tjekke jeres side

Denne fremgangsmåde er til organisationer med en betalt erhvervskonto, fx Claude Team eller Enterprise eller ChatGPT Business eller Enterprise. Med de konti kan AI'en som regel browse for jer, og som udgangspunkt bliver jeres samtaler holdt uden for træningen af modellerne.

1. **Slå browsing til**
   Brug Claude med Chrome-udvidelsen eller ChatGPT med agent-funktionen. Jeres administrator skal måske slå det til.

2. **Sig, at det er jeres egen side**
   Skriv organisationens navn og din rolle, og log gerne ind med din arbejdsmail.

3. **Vær klar til at vise, at siden er jeres**
   Hvis AI'en spørger, så åbn administrationen af hjemmesiden eller domæneindstillingerne, eller tilføj den korte verifikationskode, den foreslår.

PROMPT TIL AT KOPIERE

Jeg står for hjemmesiden hos [organisationens navn] og har ansvaret for dens sikkerhed. Gennemgå vores egen side, [jeresorganisation.dk], og vores maildomæne ud fra offentligt tilgængelige oplysninger. Tjek, om siden kræver en sikker forbindelse, afslører sin software eller version, kører forældet software og sender de almindelige sikkerheds-headers, og om vores domæne kan bruges til at sende falske mails (SPF, DKIM og DMARC). Se derefter efter andre offentligt synlige risici. Forklar det hele på almindeligt dansk, så medarbejdere uden teknisk baggrund kan forstå det, og undgå fagudtryk. Skriv for hvert problem, hvor alvorligt det er, hvad der kan ske, og hvad vi skal spørge dem, der driver siden, om. Hvis du ikke kan se noget direkte, så sig det, og nævn et gratis værktøj, der kan vise det.

TIL ENHVER AI, OGSÅ DE GRATIS

Gratis tjek og en forklaring på almindeligt dansk

Denne fremgangsmåde virker med ethvert AI-værktøj, også de gratis udgaver af Claude og ChatGPT. Værktøjerne finder fakta, og AI'en forklarer dem.

1 **Kør to gratis tjek**

internet.nl (kør både hjemmesidetesten og mailtesten) og sitecheck.sucuri.net. Skriv jeres egen adresse eller jeres domæne ind.

2 **Kopiér resultaterne**

Kopiér teksten fra hver resultatside. Skærmbilleder virker også.

3 **Sæt dem ind i AI'en sammen med prompten**

Indsæt resultaterne under prompten, og send.

PROMPT TIL AT KOPIERE

Jeg står for vores organisations hjemmeside. Nedenfor er resultaterne fra gratis sikkerhedstjek af vores eget domæne, [jeresorganisation.dk]. Forklar hvert fund på almindeligt dansk, så medarbejdere uden teknisk baggrund kan forstå det, og undgå fagudtryk. Sig, hvor alvorligt hvert fund er, hvad der kan ske, og hvad jeg skal spørge dem, der driver siden, om. Påpeg også andre risici, som resultaterne peger på. Ligger noget uden for resultaterne, så sig det i stedet for at gætte.

HVIS ANDRE DRIVER JERES SIDE

Spørg dem, der driver siden

De fleste organisationer får andre til at drive deres hjemmeside, og det fungerer fint, når det er tydeligt, hvem der har ansvaret for sikkerheden. Send dem disse spørgsmål, og gå efter konkrete svar.

- [ ] Bliver alle sider tvunget over på https, og er HSTS slået til?
- [ ] Bliver vores kernesoftware, plugins og temaer opdateret jævnligt, og hvem holder øje med det?
- [ ] Viser vores sider navn eller version på vores software, og kan det skjules?
- [ ] Bruger vi en Content-Security-Policy og de øvrige almindelige sikkerheds-headers?
- [ ] Har vi SPF, DKIM og DMARC på plads, og står DMARC til »quarantine« eller »reject«?
- [ ] Hvem ringer vi til, og hvor hurtigt reagerer I, hvis siden bliver hacket eller går ned?

Vil I have hjælp til noget af det?

Jeg hjælper NGO'er og medlemsorganisationer med at få det væsentlige på plads på almindeligt dansk. Jeg kan køre tjekkene sammen med jer eller tage hele opgaven.

magneticconsulting.dk · anna@magneticconsulting.dk