

Oktober 2026

9 Råd om cybersikkerhed til SMV'er

Cybersikkerhed er alvorligt. Men rådene må gerne være til at huske.
Brug dem som tjekliste internt eller sammen med IT-leverandøren.

1. Få overblik over virksomhedens IT

Kig godt efter - måske er der udstyr tændt, som du har glemt.

Sådan kan I gøre

- Lav en liste over enheder, systemer, tjenester og leverandører.
- Markér de systemer og data, som driften ikke kan undvære.
- Angiv ansvarlige og kontaktpersoner ved fejl eller angreb.
- Opdatér oversigten, når IT-miljøet ændres.

2. Hold systemer og enheder opdateret

“Påmind mig i morgen” er praktisk, men ikke en langsigtet sikkerhedsstrategi.

Sådan kan I gøre

- Slå automatiske opdateringer til, og kontrollér, at de installeres.
- Aftal ansvar for løsninger, der kræver manuel opdatering.
- Afklar opgavefordelingen med IT-leverandøren.
- Udskift løsninger, der ikke længere sikkerhedsopdateres.

3. Brug sikre loginløsninger

Password123 er nemt at huske. Det gælder desværre også for andre.

Sådan kan I gøre

- Brug unikke adgangskoder på mindst 15 tegn.
- Brug en passwordmanager til sikker opbevaring.
- Aktivér to-faktor-login, især på vigtige konti.
- Få hjælp til opsætningen fra IT-leverandøren ved behov.

4. Sørg for backup af vigtige data

En backup er først rigtig betryggende, når I ved, at den kan bruges.

Sådan kan I gøre

- Udpeg de data, virksomheden ikke kan undvære.
- Tag løbende backup, og hold mindst én kopi adskilt.
- Aftal ansvar og hyppighed for backup og gendannelse.
- Test jævnligt, at data faktisk kan genskabes.

5. Få styr på adgangsrettighederne

Alle behøver ikke en hovednøgle, heller ikke til de digitale døre.

Sådan kan I gøre

- Gennemgå adgange årligt og ved rolleændringer.
- Luk straks konti ved fratrædelse eller leverandørskifte.
- Begræns administratorrettigheder til få personer.
- Brug særskilte administratorkonti til særlige opgaver.

6. Brug relevante IT-sikkerhedsværktøjer

Sikkerhedsværktøjer virker bedst, når de er slået til og nogen reagerer.

Sådan kan I gøre

- Brug opdateret antivirus eller antimalware og firewall.
- Aktivér phishing- og spamfiltre i mailsystemet.
- Bevar anbefalede indstillinger og automatiske opdateringer.
- Aftal, hvem der reagerer på advarsler.

7. Arbejd sikkert uden for arbejdspladsen

Gratis wi-fi kan være fristende. Det kan fremmede forbindelser også.

Sådan kan I gøre

- Brug kun betroede netværk eller telefonens internetdeling.
- Brug virksomhedens VPN, når den er tilgængelig.
- Opdatér udstyret, og lås skærmen, når det forlades.
- Skærm fortrolige oplysninger mod uvedkommende.

8. Forbered medarbejderne på digital svindel

Et mistænkeligt link bliver ikke mere troværdigt af, at det haster meget.

Sådan kan I gøre

- Træn i at genkende mistænkelige mails, sms'er og opkald.
- Vær kritisk over for links, bilag og betalingsanmodninger.
- Kontrollér ændrede betalingsoplysninger via en anden kanal.
- Gør det trygt at melde tvivl, fejl og hændelser hurtigt.

9. Lav en enkel beredskabsplan

Når skærmen bliver sort, er det rart, at planen ikke kun ligger på skærmen.

Sådan kan I gøre

- Udpeg en ansvarlig for koordinering ved cyberhændelser.
- Saml kontaktoplysninger til IT, ledelse, bank og forsikring.
- Beskriv de første handlinger og beslutningskompetencer.
- Planlæg nøddrift, opbevar planen offline, og øv den.

En enkel måde at komme i gang på

Udpeg en ansvarlig, gennemgå rådene med IT-leverandøren, og tag de vigtigste mangler først. Cybersikkerhed behøver ikke blive ordnet på én dag, men den bliver heller ikke bedre af at vente til “på mandag”.

Cybersikkerhed bliver dermed en overskuelig del af den almindelige drift.