Appendiks 4. Personlig cybersikkerhed for bestyrelsesmedlemmer – 20 konkrete råd

#	Forebygge	
1	Kend og overhold virksomhedens it-sikkerhedspolitik	› IT-sikkerhedspolitikken kan f.eks. indeholde om, hvilke fildelingstjenester du kan bruge m.v.
2	Skab overblik over data og systemadgange	› Hvordan opbevares dine og virksomhedens data? › Hvad er risikoen, hvis de mistes?
4	Brug en dedikeret e-mailkonti til virksomhedskommunikation	› Hvis du bruger din egen, så benyt en anerkendt udbyder med spamfiltre og to-faktor login.
5	Arbejd ikke som lokal administrator på din computer	› Hvis kun én bruger har administratorrollen på din private pc, bør du oprette en ny administrator-bruger, og ændre din nuværende til standardbruger.
5	Brug stærke adgangskoder og genbrug ikke	› Brug mindst 12 tegn og kun ét sted. Brug gerne en veletableret og gennemprøvet passwordmanager. Hør evt. om virksomheden har en løsning.
6	Benyt to-faktorautentificering	› Slå altid 2-faktor-autentificering til. Se vejledning på www.sikkerdigtial.dk.
7	Kontroller om du har været med i et læk af adgangskoder	› Tjek dette på f.eks. https://haveibeenpwned.com/ og https://haveibeenpwned.com/Passwords
8	Tænk over hvad du deler på sociale medier	› Minimér privat information og tænk over om det, du deler, kan misbruges.
9	Brug ikke fremmede USB-enheder eller opladere	› Brug kun dine egne USB-sticks og opladere - ellers anvend et kabel eller en 'USB Charge-Only Adapter'.
#	**Beskytte**	
10	Benyt et privacy-filter til din computer og tablet	› Gør det sværere for folk at se, hvad du har på din skærm, og du kan arbejde sikkert i offentligheden.
11	Lås altid dine enheder	› Indstil dine enheder til automatisk skærmlås.
12	Krypter dit indhold	› Du bør også gøre fjernsletning af data muligt.

#	Beskytte	
13	Benyt sikkerhedsprodukter med antivirus og firewall	› Din computer skal være sikret mod cyberangreb, f.eks. med en firewall og antivirus. Der findes også firewall og antivirus til telefoner og tablets. Læs mere: https://sikkerdigital.dk/borger/gode-raad/beskyt-dine-enheder-mod-virus/
14	Opdater dit operativsystem og programmer regelmæssigt	› Opdater dine enheder efter, du har fået notifikation om, at de er tilgængelige. › Slet programmer, du ikke bruger. › Læs mere: https://sikkerdigital.dk/borger/gode-raad/opdater-dine-programmer/
15	Beskyt dig med VPN på usikre netværk	› Hvis du ikke bruger VPN, skal du sikre, at følsom kommunikation er beskyttet med kryptering.
#	**Opdage**	
16	Sund skepsis og opmærksomhed	› Vær opmærksom på mistænkelige henvendelser.
17	Vær opmærksom på atypiske hændelser på din computer eller mobiltelefon	› Ignorer ikke hvis f.eks. programmer åbner og lukker tilfældigt, din mus bevæger sig af sig selv mv. Reager straks. afbryd forbindelsen til internettet og kontakt en it-ekspert. Sluk ikke computeren.
18	Underret virksomhedens it-afdeling hurtigst muligt	› Gem klokkeslæt og beskriv fejlen, så godt som du kan, f.eks. gennem billeder af skærmen.
#	**Håndtere**	
19	Hav en plan klar til når uheldet er ude	› Hav altid en plan klar for, hvem du skal kontakte, f.eks. en aftale med virksomhedens it-afdeling.
#	**Genoprette**	
20	Tag sikkerhedskopier – både online og offline	› Husk sikkerhedskopier (backup) af dine data, f.eks. gennem en cloud-tjeneste eller eksternt harddisk.

BESTYRELSESFORENINGEN
Center for Cyberkompetencer

KROMANN REUMERT

CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND
FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation