CYBERSIKKERHET FOR
SMÅ VIRKSOMHETER

NorSIS

GRUNNLEGGENDE CYBERSIKKERHET

Cyberkriminelle går etter virksomheter i alle størrelser.

Kunnskap om grunnleggende cybersikkerhet, vil hjelpe deg med å beskytte virksomheten din og redusere risikoen for et cyberangrep.

BESKYTT FILENE OG ENHETENE DINE

Oppdater programvare

Dette inkluderer apper, nettlesere, og operativ-systemer. Velg automatisk oppdatering der det er mulig.

nettvett.no/oppdateringer/

Sikre filene dine

Sikkerhetskopier viktige filer til en ekstern harddisk eller i skyen. Pass også på å lagre papirdokumentene dine trygt, for eksempel i et låsbart dokumentskap.

nettvett.no/ti-tips-sikrere-pc-bruk/

Krev passord

Bruk sterke passord for alle datamaskiner, nett-brett og smarttelefoner – ikke bruk samme passord på ulike enheter.

nettvett.no/passord/

Krypter enheter

Krypter enheter og andre medier som inneholder personlig informasjon. Dette inkluderer datamaskiner, nettbrett, smart-telefoner, eksterne lagringsenheter, og skyløsninger.

Bruk totrinnsbekreftelse

Krev totrinnsbekreftelse for å få tilgang til områder i nettverket ditt med sensi-tiv informasjon. Det betyr at du i tillegg til brukernavn og passord også har en midlertidig kode eller annen verifisering på telefonen din.

nettvett.no/2-trinns-bekreftelse/

NorSIS

BESKYTT DITT TRÅDLØSE NETTVERK

Sikre ruteren din

Bytt standardnavn og -passord for administratorbrukeren, slå av fjernadministrasjon, og logg ut etter at ruteren har blitt konfigurert.

Bruk WPA2-kryptering eller bedre

Pass på at ruteren din tilbyr WPA2- eller WPA3-kryptering, og pass på at det er slått på. Kryptering beskytter informasjon sendt over nettverket ditt, så den ikke kan leses av andre.

nettvett.no/tradlost-nettverk/

SMART SIKKERHET

Krev sterke passord

Et sterkt passord er på minimum 12 tegn og er en blanding av tall, spesialtegn, store- og små bokstaver.

nettvett.no/passord/

Bruk aldri samme passord flere steder, og ikke del dem over telefon, SMS, eller e-post.

nettvett.no/sikker-palogging/

Begrens antall mislykkede innloggings-forsøk for å unngå angrep i form av passordgjetting.

Lær opp ansatte

Etabler en sikkerhetskultur gjennom regelmessig sikkerhetsopplæring av ansatte. Informer ansatte om risiko og nye sårbarheter. Gjør opplæringen obligatorisk.

nettvett.no/digital-sikkerhetskultur/

Ha en plan

Ha en plan for lagring av data, drift av virksomheten, og varsling av kunder om du opplever sikkerhetsbrudd.