Seniornett – får seniorene på nett!

Trusler og sikkerhet

Seniornett Frogn 7/12-2023

Sikre mobilen, nettbrettet og PC,en

- Ikke fall for fristelsen til å droppe pin kode på mobilen fordi det er tungvint. Ta heller i bruk tilleggsfunksjoner som fingeravtrykksleser eller ansiktsgjenkjenning.
- Bruk alltid pin kode på SIM kortet.
- Pass på at du har etablert automatisk sikkerhetskopiering.
- Pass på at du har aktivert automatisk oppdatering. Da får du også de siste sikkerhetsoppdateringer.

Lagre i skyen

Mobilen er med overalt og vi tar mye mer bilder enn før. Det er fort gjort at en mobil blir mistet eller ødelagt. Det er derfor viktig å ta i bruk skytjenester som Onedrive, Googledrive eller iCloud for lagring av bilder og dokumenter.

Da vil bildene være tilgjengelig selv om du mister mobilen eller om du ønsker å vise bildene på en PC etc. Bytter du mobil vil bildene fra den gamle mobilen blir tilgjengelig også for den nye.

Hva om du mister mobilen eller om det blir stjålet.

- Dersom mobilen er påslått og fortsatt har kontakt med nett kan du spore mobilen. Du vil da kunne se hvor mobilen er i et kart.
- Du kan få mobilen til å spille av en lyd i 5 min eller beskytte mobilen ved at den blir avlogget. Du kan også tømme mobilen for alt innhold. Mobilen blir tilbakestilt til fabrikkinnstillinger og dine data blir da ikke tilgjengelige via mobilen.

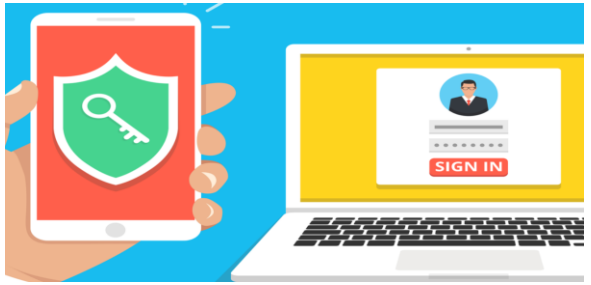
- For android-telefon gjør du dette ved å gå inn på https://www.google.com/android/find
- For iPhone logger du deg inn på iCloud og går du inn på https://www.icloud.com/find

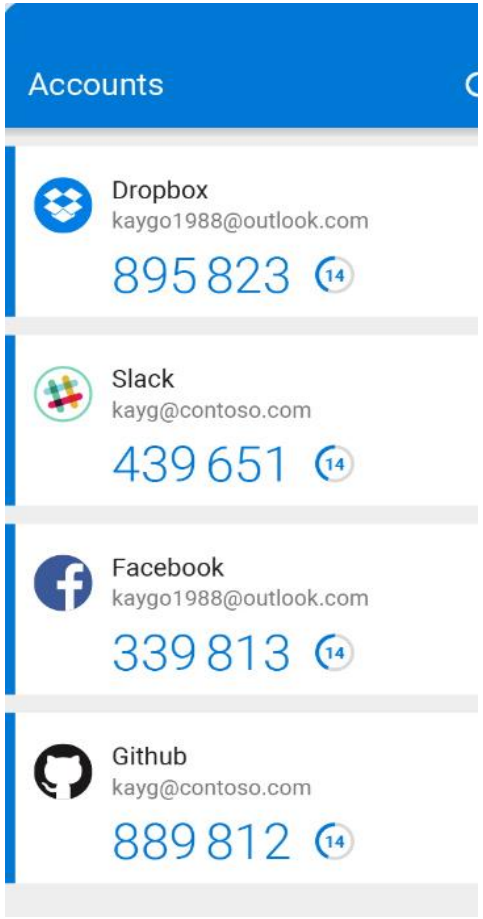
Dine passord

Passord er i mange tilfeller det eneste som hindrer uvedkommende fra å få tilgang til dine bilder og filer som er lagret på nett. Det er derfor viktig å:

- Unngå å bruke opplagte passord som vinter, sommer etc. samt ord som er knyttet til deg som person
- Bruk et passord som du kan huske. Det er mye bedre med et langt passord som er enkelt å huske fremfor et kryptisk passord som du må skrive ned. Bruk gjerne en setning. (mitt hus er blått&rødt)
- Ikke bruk det samme passordet overalt.
- Det finnes «passordgeneratorer» som kan holde orden på passordene.

2 trinns verifisering





Vi benytter 2 trinns verifisering når vi logge oss inn i nettbanken og i offentlige tjenester ved hjelp av Bankid.

Med 2 trinns verifisering må vi i tillegg til å vite passordet ha en kode som genereres med f. eks en kodegenerator.

Det kan etableres 2 faktor autentisering på mange tjenester som epost, lagring i skyen, facebook mm.

Epost trusler og sikkerhet

Spam/søppelpost er betegnelsen på uønsket masseutsendt reklame eller unyttig informasjon. Utgjør i dag et stort problem for brukerne og tilbydere da så mye som 90-95% av all e-post er uønsket søppelpost.

Vær alltid skeptisk. Sjekk ekstra når du mottar SMS eller e-post som ber om handling fra deg.

Oppdater programvare både operativsystemet og apper/e-posten din jevnlig.

Alt som er for godt til å være sant er **alltid** det.

Epost trusler og sikkerhet

Phishing er den mest brukte formen for svindel og har som mål å «fiske ut» personlig informasjon fra den som forsøkes svindlet. Phishing angrep kommer som regel via en epost, en SMS eller et telefonanrop.

Eposter og SMS,er inneholder gjerne et falskt vedlegg eller en lenke som fører til en nettside som tilsynelatende kan være en pålitelig bank eller nettbutikk.

Den falske nettsiden er satt opp til å fiske opp ditt brukernavn og passord og lure til seg dine tilganger til f. eks bank konti, gjerne kombinert med bruk av telefonsamtale som ser ut til å komme fra din bank.

Phishing via epost- eksempler

C	cloud	Lagringskrise: Skyplassen din er oppbrukt, men vi har 50 GB gratis! Lagringsplassen din er full! Cher clie
P	preferansebasen@nettsvar.no	[redacted] | Enheten din er infisert med (4) virus. DITT NORTON -ABBONNEMENT ER UTLØPT 05-11-202
A	Anti-Virus	⚠ Haster: Merknad om kontosuspensjon ⚠ - Forny lisensen din nå! ENDELIG ADVARSEL Etter utløpsd
A	Amdin_FEDEX	✅Leveringsmelding [redacted] _Bekreft pakken din 📦 -Denne meldingen ble sendt fra en pålitelig
F	FEDEX	Pakken din kunne ikke leveres.📦 Fed Ex Â® Levering mislyktes for Lynx! L
G	Gratulerer!	Din sjanse til å få en GRATIS iPhone 15 Pro I anledning Googles bursdag

Råd for å unngå å bli lurt av falske e-poster og SMSér:

- Vær kritisk. Sjekk avsenderen. Kommer den fra en pålitelige kilde? Vær spesielt forsiktig med e-poster fra ukjente.
- Sjekk URL-er: Klikk aldri på lenker i e-post/SMS hvis du ikke er helt sikker på at den er ekte.
- Vær obs på dårlig grammatikk og stavefeil, men det alene holder ikke…
- Del aldri personlig eller økonomisk informasjon via e-post eller SMS med mindre du er sikker på at mottaker er legitim. Det være seg passord, personnummer, bankkortnummer etc. Vanlig at det bes om oppdatert betalingsinformasjon. Vær obs på konkurranser/spørreundersøkelser

NB! Banken eller politiet vil aldri spørre deg om din BankID eller ditt passord

Råd for å unngå å bli lurt av falske e-poster og SMSér:

Sikre nettverk.

Ikke koble deg til åpne trådløse nettverk (nettverk uten pålogging) for å logge deg på eller utføre transaksjoner som krever passord og personopplysninger. Bruk heller nettet fra mobiloperatøren din.

Sikker netthandel.

Pass på at du handler på nettsider med solid rykte. Sjekk om siden har en liten gul hengelås i linjen til nettleseren eller nederst i høyre hjørne. Da har den sikkerhetssertifikat. Bruk *kredittkort* til netthandel.

Digipost – din digitale postkasse

- Send og motta post til virksomheter og personer.
- All forsendelse i Digipost er kryptert ende til ende.
- Garanti for at de som sender ikke er noen andre enn det de utgir seg for å være.
- All post er tilgjengelig overalt via nett
- Kan også benyttes til å sende og lagre viktige dokumenter.

GARANTERT FRI FOR SPAM