POLITIET

Den lille brosjyren om datasikkerhet

1.0/Desember 2021

Tips 1: Bruk sterke passord

Passord er nøkkelen til ditt digitale liv. Sørg for at ingen andre kan få tilgang til det!

Enkle passord er enkle å gjette. Unngå å bruke ord som er knyttet til privatlivet ditt, som for eksempel navnet på kjæledyret, fotballaget eller barnet ditt. E-posten din bør alltid ha et eget passord. Og viktigst av alt: Ikke del passordene dine med noen!

Et sterkt passord kan du lage ved å kombinere tre tilfeldige ord med tall, symboler og store bokstaver. For eksempel: 15fiskeRspist(middaG1!. OBS: Ikke bruk dette passordet – finn heller på ditt eget.

Tips 2: Bruk totrinnsbekreftelse

Med totrinnsbekreftelse unngår du at andre utgir seg for å være deg på nett.

Kriminelle kan stjele passord. Kontoer som er satt opp med totrinnsbekreftelse, krever at du må oppgi en ekstra "faktor" for å logge inn. Dette vil være noe bare du har tilgang til, for eksempel en kode på SMS eller fra en app på enheten din. Selv om en kriminell vet passordet ditt, kommer altså vedkommende seg ikke inn på kontoen din.

Aktivér alltid totrinnsbekreftelse når det er mulig.
Gå til https://nettvett.no/2-trinns-bekreftelse/ for veiledning i hvordan du setter opp totrinnsbekreftelse for vanlige nettbaserte tjenester.

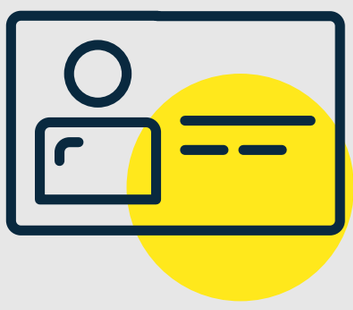
Tips 3: Tenk deg om før du klikker på vedlegg eller deler lenker

Hvis du klikker på ukjente vedlegg eller lenker, kan kriminelle få tilgang til enhetene dine.

E-poster eller SMS du mottar kan inneholde vedlegg eller lenker du blir bedt om å klikke på. Hvis du gjør det, går du forbi alle sikkerhetstiltakene dine. Hvis meldingen var fra kriminelle, kan de få tilgang til eller infisere datautstyret ditt.

Dobbeltsjekk før du klikker på et vedlegg eller en lenke med mindre du selv kan verifisere hvor den kom fra. Ring avsenderen for å få bekreftet at den er ekte. Hvis du er i tvil, ikke klikk!

Tips 4: Vær skeptisk når noen spør om din personlige informasjon



Kriminelle finner på alle mulige slags historier for å forsøke å lure deg til å gi fra deg penger eller personlig informasjon.

Enten det skjer ansikt til ansikt, over telefonen eller på internett, foregår mye kriminalitet ved at kriminelle utgir seg for å være noen de ikke er. De kan late som de er fra politiet, skatteetaten, banken din eller noen andre du stoler på for å forsøke å stjele dataene eller pengene dine.

Aldri gi fra deg informasjon til noen som kontakter deg uten at du forventer det. Ta deg tid til å sjekke med pålitelige kilder at de faktisk er hvem de utgir seg for å være. Vær skeptisk til pengeoverføringer som haster.

Tips 5: Bruk antivirus

Antivirusprogrammer er din digitale vaksine. Husk å installere det på alle enhetene dine, og vær sikker på at programmet er oppdatert.

Virus og skadelige programvarer kan angripe alle typer enheter, datamaskiner, mobiltelefoner, nettbrett m.m. Har du først fått virus, kan det låse deg ute fra enhetene dine og stjele informasjonen din. Ja, til og med overvåke deg i ditt eget hjem. Antivirus beskytter deg mot dette.

De fleste datasystemer har innebygget antivirus. Sørg for at du benytter deg av dette. Vurder også om du bør installere ekstra antivirusprogrammer på alle enhetene dine. Programvaren overvåker alt som kommer inn på enhetene dine og advarer deg hvis noe prøver å angripe systemet ditt.

Tips 6: Oppdater alltid programvare

Sårbarheter er som hull i datamaskinens system. Oppdateringer lapper igjen hullene.

Programvare er aldri perfekt. Ofte har de sårbarheter eller hull som kriminelle kan bruke for å få tilgang til dine systemer. Når en sårbarhet blir funnet, lager og utgir program-vareprodusenten en oppdatering som fikser problemet.

Oppdater alltid programvaren din med en gang du får beskjed om det, slik at systemene dine er trygge og sikre til enhver tid.

Tips 7: Ta sikkerhetskopi av dataene dine

Ta kopier av det som er viktig for deg. Oppbevar kopiene på en sikker måte.

Filene dine, kontaktene dine og bildene dine er kanskje noe av det viktigste du har på datautstyret ditt. Hvis datautstyret går i stykker eller blir infisert, sikrer kopiene at du ikke mister de viktige dataene dine.

Sikkerhetskopiér de viktigste filene dine regelmessig. Lagre disse på et eksternt lagringsmedium som for eksempel en ekstern harddisk, USB-disk eller skytjeneste. Sørg også for at kopiene holdes adskilt fra originalene.

Tips 8: Vær forsiktig når du kobler til offentlige nettverk

Offentlige eller gratis Wi-Fi er ikke sikre. Noen kan overvåke det du gjør!

Hvis et Wi-Fi nettverk er offentlig, slik som i en butikk, på en restaurant, et hotell eller en flyplass, må du passe på at nettsidene du besøker er krypterte. Hvis du ser «https» eller en hengelås i adresselinjen, er siden kryptert og trygg å bruke.

Tenkt deg godt om før du bruker offentlig Wi-Fi til noe du ikke vil at en fremmed skal se. Skru av Wi-Fi på enhetene dine når du ikke bruker det.

Tips 9: Vær bevisst på hva du deler på sosiale medier

Hvis du ikke er forsiktig på sosiale medier, kan det hende du deler personlig informasjon med feil folk.

Sosiale medier er en god måte å holde kontakt med familie og venner på. Hvis du imidlertid ikke har sjekket personverninnstillingene dine, kan det hende du deler mer personlig informasjon enn du tror. Vær oppmerksom på at når noe først ligger ute på internett, så vil det være der til evig tid.

Ha kontroll på hvem som kan se hva du deler på internett, sjekk personvern-innstillingene dine og sett dem på høy/sterk beskyttelse. Ikke del privat informasjon på sosiale medier, som for eksempel adressen eller skolen din. Sørg for at hele familien følger de samme rådene

Tips 10: Rapportér datakriminalitet

Politiet kan ikke stoppe kriminalitet vi ikke har kunnskap om at foregår. Rapportér derfor inn datakriminalitet og bedrageriforsøk til politiet.

Selv om du ikke har tapt penger eller data, bør du rapportere forsøk på bedrageri eller datakriminalitet du blir utsatt for. Informasjonen bidrar i politiets etterforskning, hindrer de kriminelle og reduserer skadevirkningene av kriminaliteten. Rapporteringen bidrar også til analyser av trender og informasjonskampanjer for å beskytte befolkningen og virksomhetene.

Rapportér online på Datakriminalitet og bedrageri – **Politiet.no eller ring oss på 02800.**
På nettsiden finner du mer informasjon fra politiet og samarbeidende etater. samt informasjon om hvordan du kan anmelde datakriminalitet.
Økokrim sitt responssenter er åpent på dagtid **8-16. Telefon 23 29 11 00**

Utarbeidet av Oslo politidistrikt og Nasjonalt cyberkrimsenter (NC3)

Information in English on the Website.