

**Gjør det
i dag!**

SLIK HOLDER DU DEG UNDER RADAREN:

Kunsten å gjøre seg usynlig på nettet

Nettkriminelle blir stadig mer utspekulerte og sikter seg inn på både pc og mobil. Her får du tolv tips om hvordan du kan skjule dine spor og surfe i fred.



Journalist
Henning Rasmussen

Også for sikkerhetsekspertene og journalister som jobber med dette til daglig, kan det være en utfordring å ikke la seg lure av de stadig mer utspekulerte svindelforsøkene på nettet.

Det kan være ondsinnede informasjonsskapsler som etterlates av obskure nettsider og følger ferden din på nettet. Hackere kan forsøke å ta seg inn på pc-en ved å angripe din personlige IP-adresse, som maskinen villig avslører når du besøker nettsider eller klikker på koblinger i ondsinnet e-post. ID-tyver rapper bilder og informasjon på Facebook og oppretter nye profiler i ditt navn, slik at de kan utnytte vennene dine.

Truslene står nærmest i kø

I tillegg til alle farene som lurar på nettet, er du også utsatt for en rekke

trusler i din umiddelbare nærhet: Kriminelle kan forsøke å skaffe seg tilgang til det trådløse hjemmenettverket, slik at de kan ta seg inn på dine personlige enheter og få tilgang til både penger og informasjon. Du kan også oppleve at det trådløse gratisnettet på flyplassen ikke var så sikkert som du kanskje trodde. Er du riktig uheldig, kan du også risikere at svindlere forsøker å ta seg inn på maskinen via den trådløse Bluetooth-tilkoblingen når du tror at du befinner deg et trygt sted, for eksempel på en kafé eller i et møterom.

Mobilen kan være utsatt

En ting er alle truslene som konstant utsetter deg og Windows-maskinen for fare, men de fleste har også en annen enhet som kan være sårbar.

På samme måte som en datamaskin kan nemlig smarttelefonen være utsatt for farlige nettsider, virus og angrep via enhetens IP-adresse. I tillegg

kommer potensielle anrop fra svindlere, og det kan ramme selv om du har hemmelig telefonnummer. Telefonsvindlere ringer nemlig ofte tilfældige numre.

Denne formen for svindel øker dessuten raskt, og takket være kunstig intelligens og stor oppfinnsomhet har folkene bak blitt mye flinkere til å fremstå som troverdige.

Under radaren

Vi kan selvfølgelig ikke garantere at du *aldri* mer kommer til å bli utsatt for svindelforsøk etter å ha lest denne artikkelen, men vi gir deg tolv smarte metoder som kan gjøre livet og jobben til hackeren så vanskelig som overhodet mulig.

Målet er å gjøre deg selv, pc-en og mobilen tilnærmet usynlig – både på nettet og i den virkelige verden – slik at du ikke blir noe lett offer. Her viser vi trinn for trinn hvordan du kan forsure hackerens hverdag.



Slik skjuler du deg effektivt på nettet

Vil du unngå å bli enda et tall i statistikken over ofre for datakriminalitet? Da bør du gjøre deg vanskeligst mulig å finne når hackere og andre kriminelle er på jakt etter nye mål.

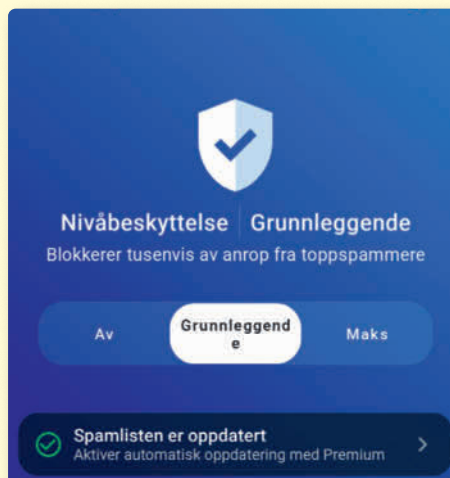
- | | | |
|---------------------------------------|--|--|
| ✓ Beskyttelse mot telefonsvindel | ✓ Sjekk om du kan spores på nettet | ✓ Bruk aldri gratis Wi-Fi |
| ✓ Hold deg skjult på en lånt pc | ✓ Slett ukjente apper fra mobilen | ✓ Sensitiv informasjon på Facebook |
| ✓ Gjør deg usynlig med gratis VPN | ✓ Tofaktorausautentisering overalt | ✓ En egen e-postkonto til det mindre viktige |
| ✓ Skjul navnet på det trådløse nettet | ✓ Slå av Wi-Fi og Bluetooth på mobilen | ✓ Bruk kryptering til å beskytte filer |

Beskyttelse mot telefon-svindel

Mange blir oppringt av falske Microsoft-ansatte, tvilsomme strømleverandører og selgere av fiktive produkter. Det kan du sikre deg mot.

Å bli oppringt av svindlere er irriterende og kan i verste fall være farlig. Den som ringer kan prøve å få deg til å takke ja til å abonnere på et eller annet, gjerne på gebrokkent engelsk – eller å installere et "hjelpesprogram" på pc-en. De kan også presentere seg på godt norsk og hevde at de ringer fra banken.

De fleste nyere smarttelefoner er utstyrt med funksjoner som oppdager og blokkerer mistenkelige nummer. Du kan også laste ned appen Truecaller til Android eller iOS og bli beskyttet mot svindelanropene.



Truecaller-appen finnes for både Android og iOS og sjekker inngående anrop mot en liste over svindelnumre, slik at du varsles i tide.



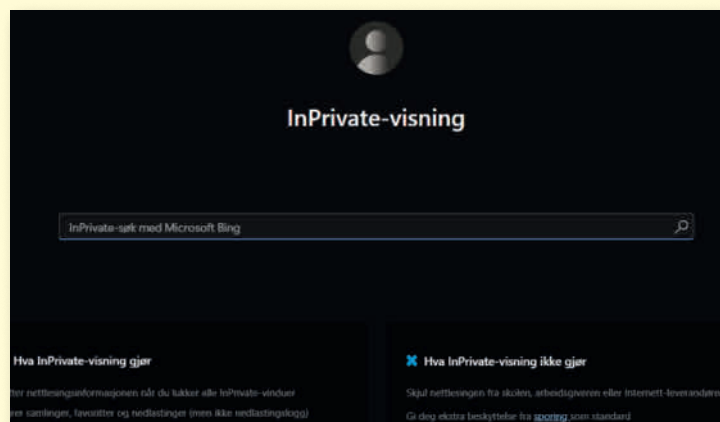
Derfor er det viktig

• Svindelanrop

Noen ringer og utgir seg for å være for eksempel fra banken, og vil ha deg til å overføre penger eller oppgi kontoinformasjon.

• Dyre samtaler

Du blir bedt om å trykke på en tast – og blir uten å vite det koblet til et betalingsnummer som koster mange kroner per minutt.



Når du bruker InPrivate-funksjonen i Edge eller Inkognito i Chrome, lagres ikke data om hvilke nettsider du har åpnet.



Derfor er det viktig

• Andre kan se loggen

Hvis du deler pc med andre, kan de se hvilke nettsider du har besøkt – som nettbanken, helserelaterte sider eller annet du vil ha for deg selv.

• Annonnene følger deg

Når du ikke bruker Inkognito, kan nettsider lagre informasjon på maskinen og vise annonser for varer eller tjenester du har søkt etter.

Hold deg skjult på en lånt pc

Hvis du bruker en pc på biblioteket eller et annet offentlig sted, bør du passe på at ikke maskinen lagrer sensitiv informasjon.

Når du åpner en ny fane i Inkognito-modus i Chrome, lagrer ikke nettleseren historikk, søk eller en oversikt over nettsider du har åpnet på maskinen. Det er smart hvis andre bruker samme pc og du vil verne om privatlivets fred. I Chrome kalles funksjonen "Inkognito", i Firefox heter den "Privat nettslesing" og i Edge er navnet "InPrivate".

Vær klar over at funksjonen bare skjuler spor lokalt på maskinen. Nettleverandøren og nettsidene du besøker, ser fortsatt hva du gjør. Det er altså ikke en fullstendig beskyttelse.



Gjør deg usynlig med gratis VPN

VPN står for Virtuelt Privat Nettverk og er et verktøy som beskytter deg når du er på internett fra pc eller mobiltelefon.

I praksis fungerer verktøyet ved at du installerer et lite program som er utviklet av en VPN-leverandør.

Leverandøren har en rekke servere i forskjellige land, og når du oppretter forbindelse til en av dem, blir alle dine data sendt via en slags sik-

ker tunnel. Resultatet er at ingen kan se hvilke nettsider du besøker, hva du skriver eller hvor i verden du befinner deg, ettersom også IP-adressen din er skjult. Det er særdeles nyttig hvis du benytter deg av trådløst nett på kafeer, hoteller eller er utenlands. En VPN-tjeneste – for eksempel gratisversjonen av Proton VPN som du finner på nettsiden vår – beskytter også mot hackere.



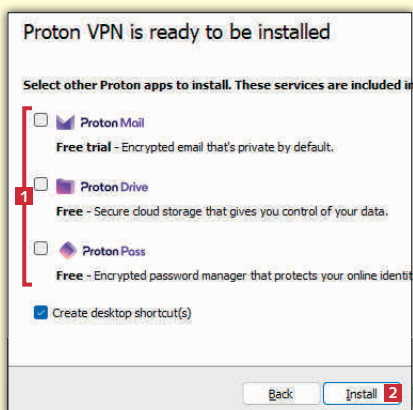
Derfor er det viktig

• Andre kan se hva du gjør

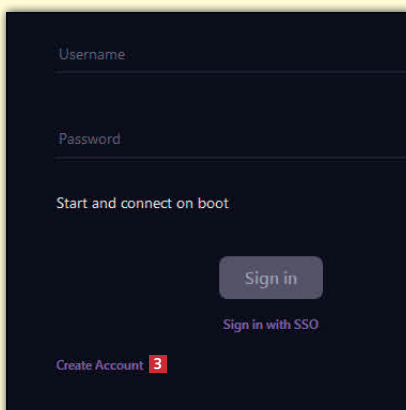
På offentlige nettverk kan uvedkommende se hva du gjør – for eksempel når du bruker nettbank eller leser e-post.

• Du blir sporet

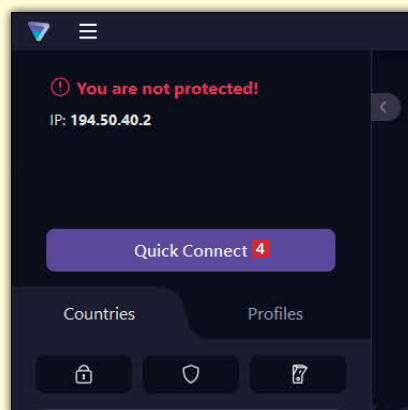
Nettsider og firmaer kan følge med på hva du ser på nettet og lagre informasjon om deg.



1 Last ned Proton VPN fra nettsiden vår, og start installering. Underveis fjerner du hakene ved de foreslåtte programmene **1** og klikker på **Install** **2**.



2 Den første gangen programmet starter, må du logge på med en gratis konto. Den oppretter du ved å klikke på **Create Account** **3**. Logg på den nye kontoen.



3 I programmet klikker du på **Quick Connect** **4**. Da kobler maskinen seg til den første tilgjengelige VPN-serveren, og dermed er pc-en beskyttet.



Derfor er det viktig

• Uønskede gjester

Hvis nettverket er synlig, kan folk i nærheten prøve å gjette passordet og få tilgang.

• Enkel tilgang for hackere

Når nettverket er synlig, er det også lettere for hackere å finne deg og forsøke å skaffe seg tilgang. Klarer de det, kan de se filene dine, stjele passord og forstyrre andre enheter.

Skjul navnet på det trådløse nettet

Det trådløse hjemmenettverket har et navn som vises når andre søker etter tilgjengelige Wi-Fi-nettverk i nærheten. Navnet kalles SSID, og skjuler du det, blir nettverket usynlig for uvedkommende.

Når nettverket er usynlig, blir det også vanskelig for fremmede å skaffe seg tilgang. Du kan selvfølgelig fortsatt bruke nettverket selv, men

forutsetningen er at du kjenner både nettverksnavn og passord og oppgir dette manuelt den første gangen du vil koble til en pc eller telefon. Du skjuler SSID på nettverket ved å logge inn på ruterens nettsiden. Der skal du se etter innstillingene for trådløst nettverk og fjerne haken ved "Vis nettverksnavn" eller lignende. Les mer i ruterveiledningen.

Sjekk om du kan spores på nettet

På hjemmesiden Cover Your Tracks kan du se hvor mye datamaskinen avslører om deg når du er på nettet. Uten at du er klar over det, kan nemlig nettsider avlese informasjon om maskinens skjermstørrelse, operativsystem og programmer du bruker. Dette kalles "fingeravtrykk" og kan brukes til å følge deg rundt på nettet, selv uten at du oppgir navnet ditt på nettsidene.

Siden tester nettleseren og forteller hvor lett du er å gjenkjenne, samtidig som du får vite hvor godt beskyttet du er og hvordan du kan bli mer anonym på nettet. Når testen er fullført, får du vite hvor "unik" nettleseren din er. Jo mer unik, desto lettere er det for hjemmesider å gjenkjenne deg og følge deg rundt på nettet. Hvis du er lett å gjenkjenne, kan du endre nettleserinnstillingene.



Derfor er det viktig

• Svekket personvern

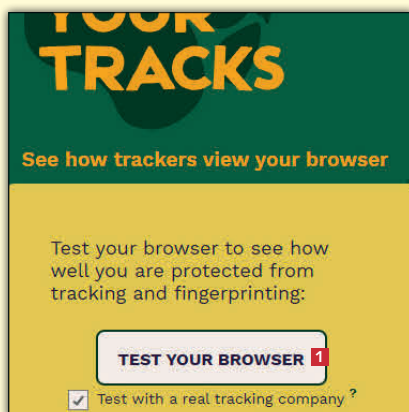
Nettsider kan følge ting du ser, klikker på og interesserer deg for – uten at du vet det.

• Målrettede annonser

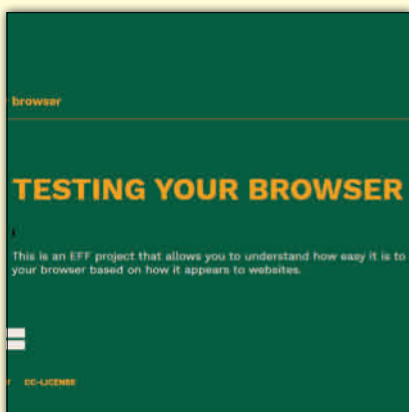
Adferden din brukes til å påvirke deg med tilpassede annonser.

• Data kan misbrukes

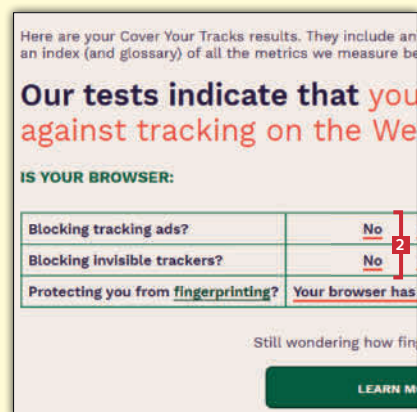
Informasjon om deg kan bli solgt eller lekket. I verste fall kan den brukes til svindel.



1 Åpne først nettleseren og gå deretter til nettsiden coveryourtracks.eff.org – der du klikker på **TEST YOUR BROWSER** **1**.



2 Nå begynner hjemmesiden å sjekke hvor utsatt maskinen er for å bli sporet på nettet. Hele prosessen tar 10–20 sekunder.



3 Hvis det står **No** **2** i de to feltene, er du IKKE beskyttet mot sporing. På komputer.no/2516 finner du en veiledning om hvordan du sikrer nettleseren mot sporing.



Derfor er det viktig

• ID-tyveri

Har du kommet i skade for å gi for mange tillatelser, kan ukjente apper stjele informasjon fra kontaktlisten, meldinger eller bilder og sende dem videre.

• Høy telefonregning

Skjulte apper kan forsyne seg av tilgjengelig datakvote, tappe batteriet og sende dyre tekstmeldinger uten at du vet det.

Slett ukjente apper fra mobilen

Det er særdeles fornuftig å sjekke hvilke apper du har på mobilen fra tid til annen. Du tror kanskje at du kjenner til alle appene, men noen apper kan faktisk ha blitt installert uten at du la merke til det, eller kanskje de fulgte med noe annet du har lastet ned. Er det en bestemt app du ikke gjenkjenner i oversikten over apper på mobilen, bør du undersøke

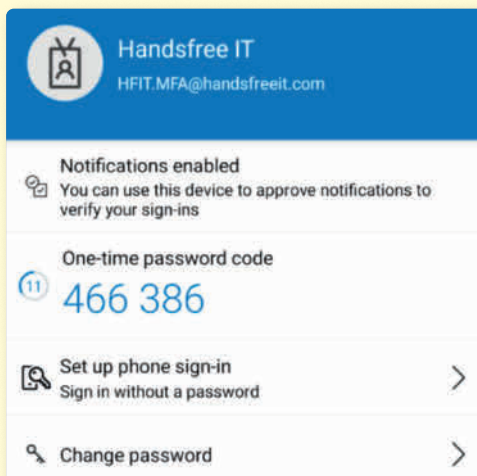
den nærmere eller ganske enkelt slette den. Noen apper kan ha tillatelse til å se kontaktene dine, hvor du befinner deg, kamera eller mikrofon, uten at du nødvendigvis har godkjent dette med vilje. Det betyr at eventuelle lyssky apper kan vite mer om deg enn de bør.

Derfor bør du sjekke listen over apper og fjerne dem du ikke bruker.

Tofaktor- autentisering overalt

Det har blitt for usikkert å kun bruke ett passord. Derfor bør du aktivere ekstra beskyttelse med sikre engangskoder der det er mulig.

Tofaktorausentisering er en ekstra sikkerhet som kan aktiveres til de fleste tjenester på nettet. I tillegg til passordet du selv har valgt, får du da en engangskode som enten sendes som sms til mobilen eller leveres i en engangskode-app. Det betyr at selv om noen skulle få tilgang til passordet ditt, så kan de ikke logge på uten engangskoden. Tofaktorausentisering aktiveres vanligvis i innstillingene for den aktuelle tjenesten. Det tar få minutter å sette det opp og gjør det veldig mye vanskeligere for uvedkommende å få tilgang.



Med en app som Microsofts gratis Authenticator kan du få langt sikrere engangskoder.



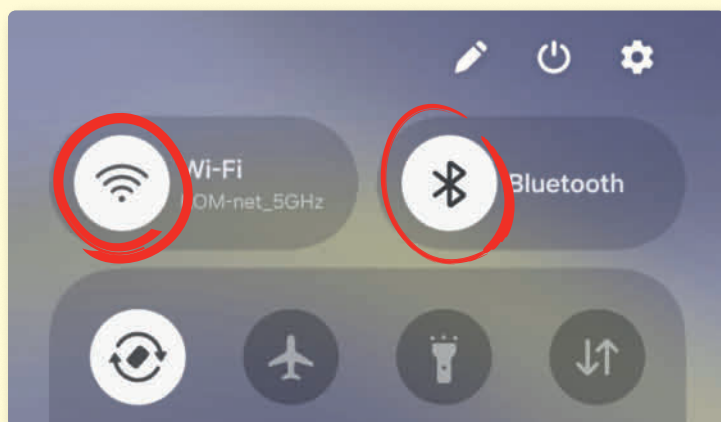
Derfor er det viktig

• Kontoer kan hackes

Hvis uvedkommende får tak i passordet ditt til en tjeneste på nettet, kan de også få tilgang til for eksempel e-post, kalender eller Facebook.

• Misbruk av informasjon

Får en hacker tilgang til kontoene dine, kan vedkommende lese meldinger, sende e-post i ditt navn eller stjele personlig informasjon.



På de fleste telefoner slår du av Bluetooth og Wi-Fi ved å dra to fingrer nedover fra toppen av skjermen og trykke på ikonene.



Derfor er det viktig

• Du kan spores

Når Wi-Fi og Bluetooth er slått på, kan mobilen sende signaler som gjør det mulig for andre å se hvor du er.

• Hackere kan få tilgang

Åpne signaler, som dem som sendes av Bluetooth og Wi-Fi, kan utnyttes av uvedkommende til å få tilgang til enheten eller data.

Slå av Wi-Fi og Bluetooth på mobilen

Trådløse teknologier som Wi-Fi, NFC og Bluetooth er nesten uunnværlige, men kan også gjøre deg sårbar for angrep når du er på farten.

Når du ikke bruker Wi-Fi eller Bluetooth på mobilen, er det smart å slå av begge deler – særlig når du er på reise. Når de trådløse teknologiene er aktive, vil mobilen hele tiden søke etter nettverk og enheter – og det kan gjøre deg sårbar. Fremmede kan prøve å opprette kontakt med mobilen eller følge dine bevegelser via de trådløse signalene, og det skjer uten at du oppdager det. Slår du av Wi-Fi og Bluetooth når du ikke bruker dem, sparer du strøm samtidig som du gjør det vanskelig for uvedkommende å spionere.

Bruk aldri gratis Wi-Fi

Det er forlokkende som en oase i ørkenen når man ser at det er gratis trådløst nett på kafeen eller flyplassen, men det kan være en sikkerhetsrisiko.

Gratis Wi-Fi på restauranter, hoteller eller flyplasser kan være fristende når du vil sjekke e-post eller lese nyheter, men slike nettverk er ikke nødvendigvis sikre. Kobler du deg på et åpent nettverk, er det fare for at andre på det samme nettverket følger med på hva du gjør – for eksempel hvilke passord du skriver, e-post eller annen privat informasjon. Noen ganger lager dyktige svindlere også falske tilgangspunkter som virker legitime, slik at du blir lurt til å koble deg direkte på hackerens nettverk. Derfor bør du unngå åpne nettverk.



Lite er like forlokkende som ordet "gratis", men noen ganger er prisen at personlig informasjon kan komme på avveie.



Derfor er det viktig

• Personvern

Svindlere som er koblet på samme nettverk som deg, kan få tilgang til dine personlige passord, e-post og andre følsomme data.

• Falske tilgangspunkter

En rutinert hacker kan sette opp et trådløst nett som virker ekte, og på den måten få tilgang til mobilen eller maskinen din.



På denne Facebook-kontoen er både personlig informasjon som innlegg og bilder skjult for andre enn venner.



Derfor er det viktig

• Identitetstyveri

Svindlere kan misbruke informasjon, innlegg og bilder til å opprette falske profiler eller utnytte ditt gode navn og rykte til å lure andre.

• Innbrudd eller svindel

Hvis du for eksempel deler et Facebook-innlegg om at du er på hytta, kan det fortelle en potensiell tyv at boligen din står tom.

Sensitiv informasjon på Facebook

Facebook gjør det lett å følge med på andres liv, men pass på at du kun deler bilder og informasjon med folk du kjenner, slik at det ikke misbrukes.

Er du på Facebook, bør du i det minste sørge for å skjule personlig informasjon og bilder for folk du ikke kjenner. Selv om det kan virke uskyldig, kan informasjon om hvor du bor, om samboeren og om sydenferien lett misbrukes av kriminelle. Slik informasjon kan i verste fall utnyttes til svindel eller identitetstyveri. Det kan også inspirere en innbruddstyv, hvis han eller hun vet at du ikke er hjemme. I Facebook-innstillingene kan du velge at bare venner kan få tilgang til å se det du deler, slik at ikke fremmede får tilgang til følsom informasjon.



Derfor er det viktig

• Du drukner i søppelpost

Hvis du kun bruker én e-post-adresse til alt, fylles innboksen raskt opp med nyhetsbrev og uønskede meldinger, slik at viktig e-post kan bli borte i mengden.

• Større risiko for svindel

Hvis e-postadressen din lekkes på nettet, kan den havne i feil hender og misbrukes til svindel eller forsøk på identitetstyveri.

En egen e-postkonto til det mindre viktige

Det er smart å supplere den private e-postadressen med en du har opprettet for det som er mindre viktig. Da kan du bruke den private kontoen til nettbank, e-boks, fastlege og kontakt med familie og venner. Den andre adressen, for eksempel på gmail.com, kan du bruke til nyhetsbrev, konkurranser, nettbutikker og steder der du må oppgi en e-post-

adresse for å komme videre. Det beskytter mot mengder av reklame og uønsket e-post som ellers raskt ville fylt opp innboksen. Samtidig reduserer du risikoen for svindel ved at du unngår å spre den primære e-post-adressen overalt på nettet. Skulle den "offentlige" kontoen en dag oversvømmes av søppel, kan du alltid slette den og opprette en ny.

Last ned Guardian Of Data fra komputer.no/2516



Bruk kryptering til å beskytte filer

På maskinens harddisk ligger normalt alle filer helt ubeskyttet, slik at en tyv eller andre uvedkommende kan lese dokumentene og se bildene dine. Hvis du derimot krypterer filene, blir de låst med en digital nøkkel, slik at det bare er du som kan åpne dem og se innholdet. Det er særlig viktig når det gjelder følsom informasjon i brev, kontoinformasjon eller private bilder. Bruker du kryptering,

er alle data fullstendig uleselige for alle andre enn deg og dem du har gitt tilgang. Har du en pc med Windows 11 Pro, inneholder den allerede et krypteringsprogram i form av funksjonen BitLocker.

Alle andre kan sikre filene med gratisprogrammet Guardian Of Data, som du kan laste ned fra nettsiden vår. Krypteringen i programmet beskytter all personlig informasjon.



Derfor er det viktig

• Datalekkasje

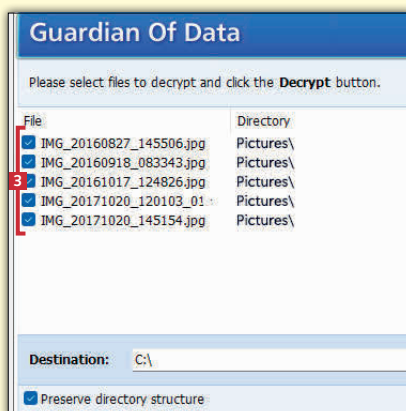
Hvis noen får tilgang til maskinen, kan de se dokumenter, bilder og annen informasjon.

• Identitetstyveri

Personlige data som personnummer og betalingsinformasjon kan misbrukes av folk som utgir seg for å være deg.



1 Last ned og installer programmet fra nettsiden vår. Når du starter det, klikker du på **Encrypt** **1** for å kryptere filer. Velg **Decrypt** **2** for å låse dem opp.



2 Når du har valgt **Decrypt**, får du mulighet til å velge hvilke filer **3** som skal låses opp. Dermed slipper du å dekode alt bare for å hente ut én fil.



På nettsiden vår kan du laste ned en komplett veiledning til programmet Guardian Of Data. I den kan du lese alt du trenger å vite om hvordan du bruker programmet til å sikre filene dine.