

Gør det allerede i dag!

SÅDAN GÅR DU UNDER RADAREN:

Skjul dig fuldstændig for de it-kriminelle

Truslerne mod din pc og telefon skyller ind fra nettet i disse år. Her får du 12 effektive tips til, hvordan du kan snige dig under de kriminelles radar på nettet.



Journalist
Henning Rasmussen

Selv for it-eksperter og computerblads-skribenter kan det være svært at gennemskue alle de sofistikerede svindelforsøg, der breder sig som en steppebrand i disse år.

Ondsindede cookies, der er efterladt af obskure hjemmesider, kan forfølge din færden rundt på nettet. Hackere forsøger at komme ind på din pc ved at angribe din personlige IP-adresse, som din pc velvilligt afslører, når du besøger hjemmesider eller klikker på links i ondsindede mails. Identitets-tyve stjæler dine billeder og oplysninger på Facebook, og opretter nye profiler i dit navn, så de kan udnytte dine venners godtroenhed.

Truslerne står i kø ved din pc

Udover alle de farer, der lurar på nettet, er du også udsat for en lang række

risici i din umiddelbare nærhed: Kriminelle kan forsøge at få adgang til hjemmets trådløse netværk, så de kan komme ind på dine personlige enheder og stjæle dine penge og informationer, eller du kan opleve, at det gratis Wi-Fi i lufthavnen slet ikke er så sikkert, som du måske forventede. Er du uheldig, kan du endda også risikere, at svindlere vil forsøge at bryde ind på din computer via dens trådløse Bluetooth-forbindelse, når du tror, at du sidder i et sikkert rum på fx en café eller til et møde.

Din telefon kan være farlig

En ting er alle de trusler, som konstant udsætter din pc og dig for farer, men derudover har de fleste af os også endnu en indgang, som svindlerne kan udnytte. Ligesom på din pc kan også din telefon være udsat for farlige hjemmesider, virus og angreb via telefonens IP-adresse. Derudover kommer potentielle telefonopkald fra svindle-

re, hvor du kan være i fare, selv hvis dit telefonnummer ikke er offentligt tilgængeligt, fordi svindlerne ofte ringer til tilfældige numre.

Denne type svindelopkald er i kraftig vækst, og svindlerne er takket være kunstig intelligens og stor opfindsomhed blevet meget bedre til at få svindlen til at virke ægte.

Gå under de kriminelles radar

Vi kan ikke udstede garantier for, at du *aldrig* mere bliver udsat for farligt svindel, hvis du læser denne artikel, men du får i hvert fald 12 gode vejledninger til, hvordan du gør arbejdet så besværligt som muligt for hackeren og hans kriminelle venner.

Det handler nemlig om, at du skal prøve at gøre dig selv, din pc og telefon så usynlig som muligt – på nettet og i virkeligheden – så du bliver et besværligt offer. I denne artikel viser vi, hvordan du på 12 trin kan besværliggøre hackerens arbejde.



Sådan skjuler du dig effektivt på nettet

Vil du undgå at blive endnu et offer i statistikken over it-kriminalitet? Så skal du være så svær som muligt at finde, når hackere og andre kriminelle leder efter nye stakler, de kan bedrage.

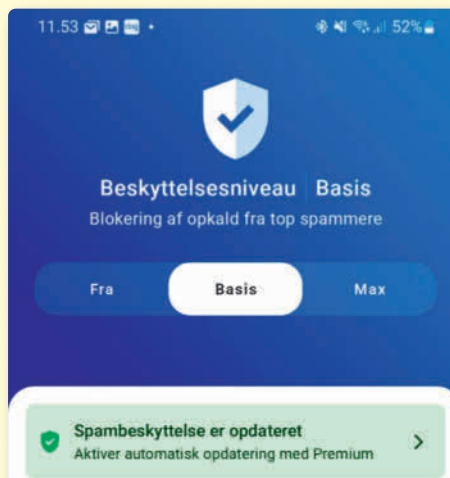
- | | | |
|--|---|---|
| ✓ Beskyt dig mod opkald fra svindlere | ✓ Tjek selv, om du kan spores på nettet | ✓ Brug aldrig de gratis hotspots |
| ✓ Skjul dig selv på fremmede computere | ✓ Smid ukendte apps ud af din telefon | ✓ Skjul dine oplysninger på Facebook |
| ✓ Bliv helt usynlig med en gratis VPN | ✓ Brug altid dobbelte koder til alt | ✓ Opret en mailkonto til det mindre vigtige |
| ✓ Fjern navnet på dit trådløse netværk | ✓ Sluk Wi-Fi og Bluetooth på telefonen | ✓ Beskyt dine filer med kryptering |

Beskyt dig mod opkald fra svindlere

Mange danskere modtager opkald fra falske Microsoft-ansatte, tvivlsomme elskelskaber og sælgere af fiktive produkter. Det kan du sikre dig imod.

Spam-opkald er irriterende og kan i værste fald være farlige. Du kan genkende dem på, at personen ofte på gebrokkent engelsk forsøger at få dig til at sige ja til at abonnere på noget – eller at installere et "hjælpeprogram" på din pc. De kan også på udmærket dansk præsentere sig som medarbejdere fra din bank.

De fleste smartphones har i dag indbyggede funktioner, der kan opdage og blokere mistænkelige numre. Du kan også hente app'en Truecaller på din Android-telefon eller iPhone og blive beskyttet mod svindelopkaldene.



Truecaller-app'en, som du kan hente til Android og iOS tjekker dine indgående opkald mod en lang liste over svindelnumre, så du advares i tide, hvis kriminelle ringer dig op.



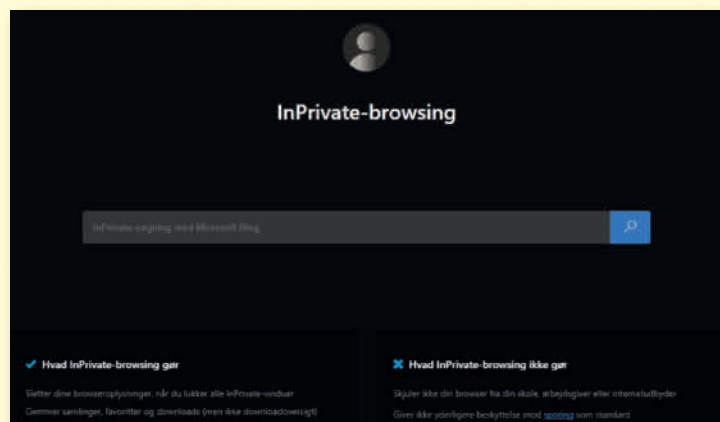
Derfor er det vigtigt

• Svindelopkald

En person ringer og udgiver sig for at være fx fra banken, og prøver få dig til at overføre en sum penge eller at lokke kontooplysninger ud af dig.

• Dyre opkald

Du bliver bedt om at trykke på en tast – og bliver helt uden at vide det koblet til et betalingsnummer, der koster mange penge i minuttet.



Når du bruger InPrivate-funktionen i Edge eller Inkognito i Chrome, gemmes der ikke data om dine internetbesøg på computeren.



Derfor er det vigtigt

• Andre kan se historik

Hvis du deler pc med andre, kan de se de hjemmesider du har besøgt – fx netbank, helbredsopslag eller gaver, du har kigget på.

• Reklamer følger dig

Når du ikke bruger Inkognito, kan hjemmesider gemme oplysninger på din pc og vise dig reklamer for det, du har søgt efter.

Skjul dig selv på fremmede computere

Hvis du bruger en pc på biblioteket eller et andet offentligt sted, bør du sørge for, at computeren ikke gemmer oplysninger om din færd.

Når du åbner en ny fane i Inkognito-tilstand i Chrome, gemmer browseren ikke din historik, søgninger eller en oversigt over de hjemmesider, du har besøgt på pc'en. Det er smart, hvis andre bruger samme computer, og du vil holde tingene privat. I Chrome hedder funktionen 'Inkognitotilstand', i Firefox hedder den 'Privat browsing' og i Edge er navnet 'InPrivate'. Funktionen skjuler dog kun dine spor på selve computeren. Din internetudbyder og de hjemmesider, du besøger, kan stadig se, hvad du laver. Det er altså ikke en fuld beskyttelse.



Bliv helt usynlig med en gratis VPN

VPN står for Virtuelt Privat Netværk, og det er et værktøj, der kan beskytte dig, når du bruger internettet fra din pc eller telefon.

I praksis virker en VPN ved, at du installerer et lille program, som er lavet af en VPN-udbyder. Udbyderen har en række servere installeret i forskellige lande, og når du opretter forbindelse til en af dem med programmet, bliver alle dine data sendt

gennem en slags sikker tunnel. Det betyder, at ingen kan se, hvilke hjemmesider du besøger, hvad du skriver, eller hvor i verden du er, da også din IP-adresse er skjult. Det er især nyttigt, hvis du bruger trådløst internet på caféer, hoteller eller i udlandet. En VPN-tjeneste – som fx det gratis Proton VPN, du kan hente på vores hjemmeside – beskytter dig også mod hackere.



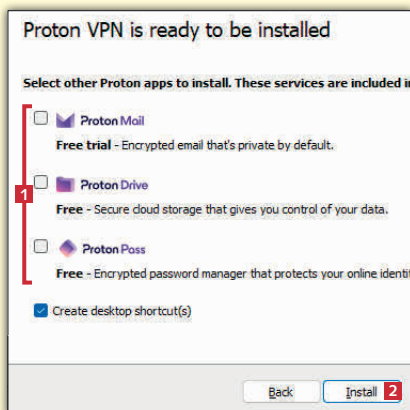
Derfor er det vigtigt

• Andre kan kigge med

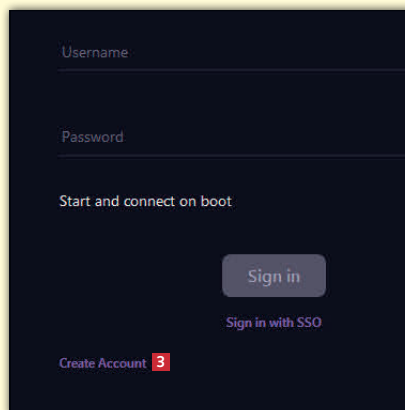
På offentlige netværk kan uvedkommende se, hvad du laver – fx når du bruger din netbank eller læser e-mails.

• Du bliver sporet

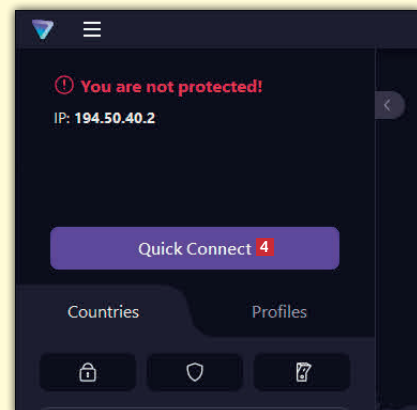
Hjemmesider og firmaer kan følge med i, hvad du ser på nettet, og gemme oplysninger om dig.



1 Hent Proton VPN fra vores hjemmeside og start installationen. Undervejs skal du fjerne fluebenene ud for de foreslåede programmer **1**, og klikke på **Install** **2**.



2 Når programmet starter første gang, skal du logge på med en gratis konto. Den opretter du ved at klikke på **Create Account** **3**. Log herefter på med din nye konto.



3 Inde i programmet skal du blot klikke på **Quick Connect** **4**. Så kobler din computer på den først tilgængelige VPN-server, og din pc er beskyttet mod hackere.



Derfor er det vigtigt

• Uønskede gæster

Hvis dit netværk er synligt, kan folk i nærheden forsøge at gætte din adgangskode og få adgang.

• Nem adgang for hackere

Når netværket er synligt, kan hackere lettere finde det og forsøge at bryde ind. Hvis det lykkes, kan de snuse i dine filer, aflure dine adgangskoder og forstyrre dine enheder.

Fjern navnet på dit trådløse netværk

Dit trådløse netværk har et navn, som dukker op, når du eller naboen søger efter tilgængelige Wi-Fi-netværk i nærheden. Navnet kaldes SSID, og hvis du skjuler det, bliver dit netværk usynligt for andre.

Når netværket på den måde er usynligt, bliver det sværere for fremmede at forsøge at bryde ind på dit Wi-Fi. Du kan stadig selv bruge net-

værket, men du skal på forhånd kende navn og kodeord, og taste det ind manuelt første gang, du vil forbinde din pc eller telefon til netværket. Du skjuler SSID på dit netværk ved at logge ind på din router fra browseren. Her skal du finde indstillingerne for trådløst net og fjerne fluebenet ved "Vis netværksnavn" eller lignende. Læs mere i routerens manual.

Tjek om du kan spores på nettet

På hjemmesiden Cover Your Tracks kan du se, hvor meget din computer afslører om dig, når du går på nettet. Uden du ved det, kan hjemmesider nemlig aflæse oplysninger om pc'ens skærmstørrelse, dit styresystem og hvilke programmer, du bruger. Det kaldes "fingeraftryk", og kan bruges til at følge dig rundt på nettet, selv om du ikke direkte bruger dit navn på hjemmesiderne.

Siden tester din browser og fortæller, hvor let du er at genkende, og du får at vide, hvor godt du er beskyttet, og hvordan du kan blive mere anonym på nettet. Når testen er færdig, får du at vide, hvor "unik" din browser er. Jo mere unik, desto nemmere kan hjemmesider genkende dig og følge dig rundt på nettet. Hvis du er let at genkende, kan du ændre browserindstillingerne.



Derfor er det vigtigt

• Mindre privatliv

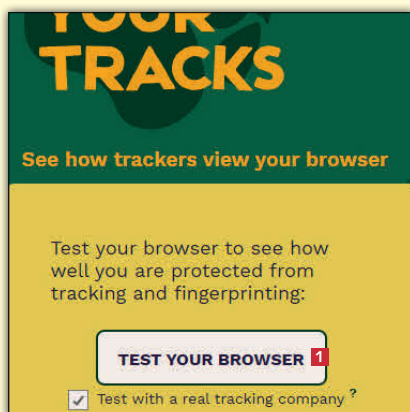
Hjemmesider kan følge de ting du ser, klikker på og interesserer dig for – uden du ved det.

• Målrettede reklamer

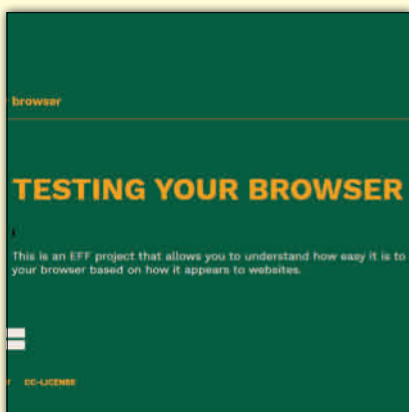
Dine vaner bruges til at påvirke dig med personlige reklamer.

• Data kan misbruges

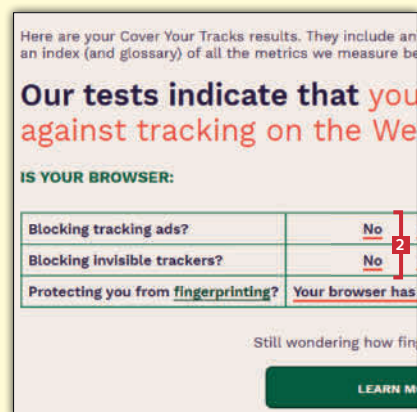
Oplysninger om dig kan blive solgt eller lækket, og i værste fald bruges til svindel.



1 Åbn først din browser og besøg så hjemmesiden coveryourtracks.eff.org – her klikker du på knappen **TEST YOUR BROWSER** **1**.



2 Hjemmesiden går nu i gang med at tjekke, hvor modtagelig din computer er for at blive sporet på nettet. Det tager 10-20 sekunder.



3 Hvis der står **No** **2** i de to felter, er du IKKE beskyttet mod sporing. På komputer.dk/2516 finder du en guide, der viser hvordan du sikrer din browser mod sporing.



Derfor er det vigtigt

• Tyveri af dine oplysninger

Er du kommet til at acceptere for mange tilladelser, kan ukendte apps snuse i dine kontakter, beskeder eller billeder og sende dem videre.

• Dyrt telefonforbrug

Skulte apps kan bruge af din tilgængelige datamængde, suge på dit batteri og sende dyre sms'er uden din viden.

Smid ukendte apps ud af din telefon

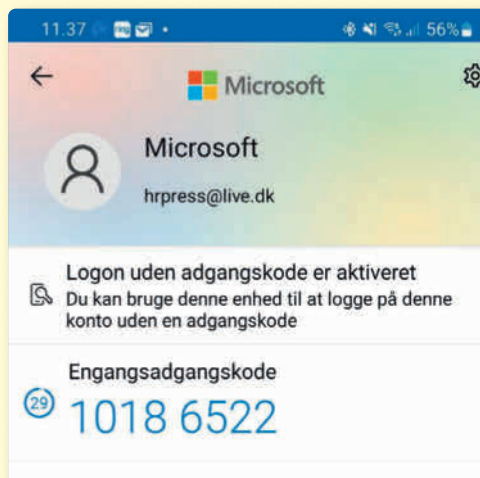
Det er en rigtig god idé, at du jævnligt tjekker, hvilke apps du har liggende på din telefon. Du tror måske, at du kender dine apps, men nogle apps kan faktisk være blevet installeret uden at du lagde mærke til det, eller måske fulgte de med noget andet, du hentede. Hvis du ikke kender en specifik app i oversigten over apps på din telefon, bør du kaste

et kritisk blik på den eller helt slette den. Nogle apps kan have tilladelse til at tilgå dine kontakter, din placering, kamera eller mikrofon, uden at du nødvendigvis har sagt ja til det med vilje. Det betyder, at eventuelle lyssky apps måske ved mere om dig, end du ønsker. Derfor bør du indimellem gennemgå listen over apps og fjerne dem, du ikke bruger.

Brug altid dobbelte koder til alt

Det er blevet for usikkert at sikre sig med én kode alene. Sørg derfor for også at tænde for ekstra beskyttelse med sikre engangskoder.

Tofaktorgodkendelse er en ekstra sikkerhed, du kan aktivere til de fleste tjenester på nettet. Ud over dit eget valgte kodeord skal du bruge en engangskode, som enten sendes per sms til din telefon eller leveres i en engangskode-app. Det betyder, at selv hvis nogen gætter dit kodeord, kan de ikke logge ind uden den ekstra engangskode. Du slår normalt tofaktorgodkendelse til i indstillingerne for den tjeneste, du bruger. Det tager kun få minutter at indstille, men gør det meget, meget sværere for kriminelle at få adgang til dine ting på nettet.



Med en app som Microsofts gratis Authenticator kan du få leveret mere sikre engangskoder.



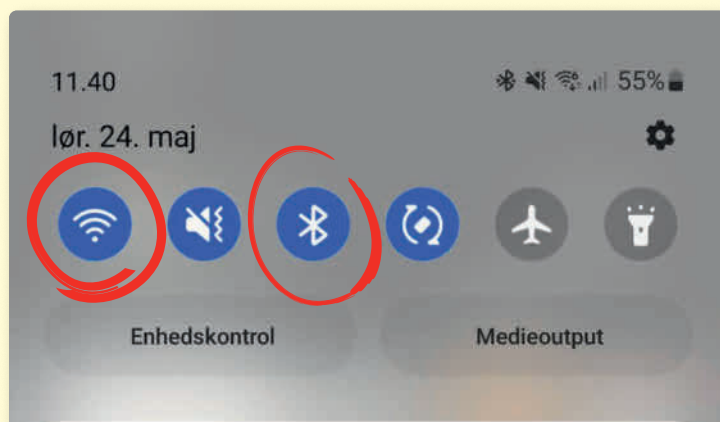
Derfor er det vigtigt

• Dine konti kan hackes

Hvis uvedkommende gætter eller stjæler dit kodeord til en tjeneste på nettet, kan de få adgang til fx din e-mail, kalender eller Facebook.

• Misbrug af oplysninger

Får en hacker adgang til dine konti, kan han læse dine beskeder, sende mails i dit navn eller stjæle dine personlige oplysninger.



På de fleste telefoner slukker du nemt for Bluetooth og Wi-Fi ved at trække to fingre ned fra toppen af skærmen. Tryk så på deres ikoner.

Sluk Wi-Fi og Bluetooth på telefonen

Trådløse teknologier som Wi-Fi, NFC og Bluetooth er næsten uundværlige, men de kan samtidig gøre dig sårbar overfor angreb, når du er på farten.

Når du ikke bruger Wi-Fi eller Bluetooth på din telefon, er det en god idé at slå funktionerne fra – især når du er ude i verden. Hvis de trådløse teknologier er tændte, vil din telefon konstant lede efter netværk og enheder, og det kan gøre dig sårbar. Fremmede kan forsøge at oprette forbindelse til din telefon eller følge dine bevægelser via de trådløse signaler, og det sker, uden at du opdager det. Ved at slukke for Wi-Fi og Bluetooth, når du ikke bruger det, sparer du både på batteriet og gør det sværere for uvedkommende at snuse med.



Derfor er det vigtigt

• Du kan blive sporet

Når Wi-Fi og Bluetooth er tændt, kan din telefon sende signaler, som gør det muligt for andre at følge med i din færden.

• Hackere kan få adgang

Åbne signaler, som dem der udsendes af Bluetooth og Wi-Fi, kan blive udnyttet af svindlere til at få adgang til din telefon eller dine data.

Brug aldrig de gratis hotspots

Det kan virke som en oase i en gold ørken, når du ser et gratis trådløst netværk på cafeen eller i lufthavnen, men netværket kan true din sikkerhed.

Gratis Wi-Fi på restauranter, hoteller eller i lufthavne kan være fristende, når du vil hente mails eller læse nyheder, men det er ikke altid sikkert. Hvis du kobler dig på et åbent netværk, kan andre personer på samme netværk måske følge med i, hvad du laver – fx se dine adgangskoder, e-mails eller andre private oplysninger. Nogle gange laver dygtige svindlere endda falske hotspots, der ligner det rigtige netværk, så du i virkeligheden kobler pc'en direkte på de kriminelles netværk. Derfor bør du undgå de åbne netværk, hvis det er muligt.



Intet kan lokke som ordet "gratis", men i nogle tilfælde betaler du med risikoen for at miste personlige oplysninger.



Derfor er det vigtigt

• Afluring af oplysninger

Svindlere, der er koblet på samme netværk som dig, kan aflure dine personlige adgangskoder, e-mails og andre private data.

• Pas på falske hotspots

En rutineret hacker kan oprette et trådløst netværk, der ligner det rigtige, og på den måde få adgang til din telefon eller computer.



På denne Facebook-konto er såvel personlige oplysninger som opslag og billeder skjult for ikke-venner, så ingen uvedkommende kan se dem.



Derfor er det vigtigt

• Identitetstyveri

Svindlere kan misbruge dine oplysninger, dine opslag og dine billeder til at oprette falske profiler eller snyde andre i dit navn.

• Indbrud eller svindel

Hvis du fx deler et opslag på Facebook om din nuværende ferie i sommerhuset, kan det give tyve en idé om, at dit hjem står tomt.

Skjul dine oplysninger på Facebook

Facebook gør det nemt at følge med i vennernes liv, men sørg for, at du kun deler billeder og oplysninger med dem du kender, så de ikke kan misbruges.

Hvis du bruger det sociale netværk Facebook, er det en god idé at skjule dine personlige oplysninger og billeder for folk, du ikke kender. Selv om det måske virker uskyldigt, kan oplysninger om din bopæl, din ægtefælle og din ferie sydpå nemlig nemt misbruges af kriminelle. Oplysningerne kan i værste fald udnyttes til svindel eller identitetstyveri, og det kan også inspirere en indbrudstyv, hvis han ved, at du ikke er hjemme. Du kan i Facebooks indstillinger vælge, at kun dine venner må se det, du deler, så fremmede ikke får adgang til dit privatliv.



Derfor er det vigtigt

• Du drukner i spam

Bruger du blot én mailadresse til alt, bliver indbakken hurtigt fyldt med nyhedsbreve og uønskede beskeder, så vigtige mails kan blive overset.

• Større risiko for svindel

Hvis din mailadresse spredes på nettet, kan den ende i de forkerte hænder og misbruges til fup eller forsøg på identitetstyveri.

Opret en mailkonto til det mindre vigtige

Det er smart at supplere din private mailadresse med en, du har oprettet til lejligheden. Din private konto kan du bruge til personlige ting som netbank, e-boks, læge og kontakt med familie og venner. Den anden adresse, som du fx nemt opretter på gmail.com, bruger du til nyhedsbreve, konkurrencer, netbutikker og steder, hvor du bare skal oplyse en mail-

adresse for at komme videre. Det beskytter dig mod en masse reklamer og uønskede mails, som ellers hurtigt vil fylde din indbakke op. Samtidig mindsker du risikoen for svindel, fordi du ikke spredt din rigtige mailadresse overalt på nettet. Skulle din "offentlige" mail en dag flyde over med spam, kan du bare slette den og oprette en ny.

Hent Guardian Of Data på komputer.dk/2516



Beskyt dine filer med kryptering

På din pc's harddisk ligger alle dine filer normalt helt ubeskyttede hen, så en tyv eller andre uvedkommende fx kan læse dine dokumenter eller se dine billeder. Men hvis du krypterer filerne, bliver de låst med en digital nøgle, så kun du selv kan åbne og se indholdet. Det gælder i særdeleshed følsomme informationer som breve, kontooplysninger eller dine private billeder, der med krypte-

ring bliver fuldstændig ulæselige for dem, du ikke har givet adgang. Hvis din pc er udstyret med Windows 11 Pro, rummer den allerede et krypteringsprogram i form af funktionen BitLocker. Men for alle os andre kan filerne sikres med det gratis program Guardian Of Data, som du kan hente på vores hjemmeside. Krypteringen beskytter så dine minder og alle personlige oplysninger.



Derfor er det vigtigt

• Læk af dine oplysninger

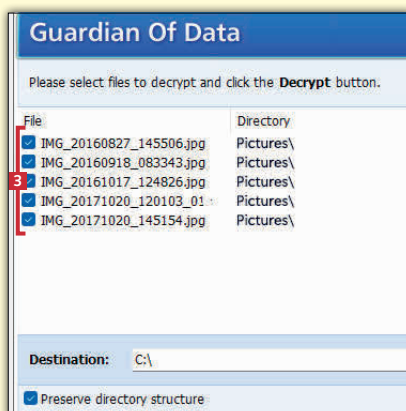
Hvis nogen får adgang til din pc, kan de se dine dokumenter, billeder og andre oplysninger.

• Identitetstyveri

Dine helt personlige data som CPR-nummer og bankoplysninger kan misbruges af svindlere, der udgiver sig for at være dig.



1 Hent programmet fra vores hjemmeside og installér det. Når du starter det, skal du klikke på **Encrypt 1** for at kryptere filer. Vælg **Decrypt 2** for at låse filerne op.



2 Når du har valgt **Decrypt**, får du mulighed for at vælge, hvilke filer **3** der skal låses op for. Dermed behøver du ikke dekryptere alt for blot at hente én fil.



På vores hjemmeside kan du hente en komplet guide til programmet Guardian Of Data. Her kan du læse alt om, hvordan du sikrer dine filer med programmet.