

**Gör det
redan
idag!**

SÅ SMYGER DU UNDER RADARN

Håll dig dold för de kriminella

Hoten mot datorn och mobilen strömmar in från nätet i dessa dagar. Här är tolv effektiva tips för hur du kan smyga under nätbrottslingarnas radar.



Journalist
Henning Rasmussen

Det är svårt även för IT-expert och skribenter i datortidningar att alltid lyckas genomsåga de sofistikerade bedrägeriförsök som sprider sig som en löpeld nuförtiden.

Skadliga cookies som lämnas av obskyra webbplatser kan spåra dina aktiviteter på nätet. Hackare försöker ta sig in i datorn genom att attackera din IP-adress som din dator frivilligt avslöjar när du besöker webbplatser eller klickar på länkar i mejl med skadligt innehåll. Identitetstjuvar stjälar dina bilder och uppgifter på Facebook och skapar nya profiler i ditt namn så att de kan lura dina vänner.

Hoten mot datorn står i kö

Förutom alla faror som lurar på nätet utsätts du också för en rad risker i din omedelbara närhet: Kriminella kan

satsa på att få tillgång till ditt trådlösa nätverk för att komma åt dina enheter och via dem försöka stjäla dina pengar och uppgifter, eller så kan du upptäcka att gratis Wi-Fi på flygplatsen inte alls är så säkert som du kanske trodde. Om du har otur kan du till och med riskera att bedragare försöker bryta sig in i din dator via dens trådlösa Bluetooth-anslutning när du tror att du sitter i ett säkert rum på exempelvis ett konditori eller i ett mötesrum på ett kontor.

Din mobil i farozonen

Alla dessa hot som ständigt utsätter din dator och dig för fara är en sak, men dessutom har de flesta av oss ytterligare en ingång som kriminella gärna försöker utnyttja. Precis som din dator kan även din mobil utsättas för skadliga webbplatser, virus och attacker via mobilens IP-adress. Här kan du dessutom få telefonsamtal från bedragare där du kan råka illa ut trots

att ditt nummer kanske är hemligt eller på andra sätt inte är offentligt tillgängligt, eftersom bedragarna ofta ringer slumpmässiga nummer.

Denna typ av bedrägerisamtal ökar kraftigt, och på grund av artificiell intelligens och uppfinningsrikedom har de kriminella blivit mycket bättre på att få sina bedrägerier att kännas väldigt trovärdiga.

Smyg under de kriminellas radar

Vi kan inte garantera att du *aldrig* kommer att utsättas för bedrägerier igen om du läser den här artikeln, men du får tolv tips på hur du gör arbetet så svårt som möjligt för hackaren och hans kriminella vänner.

Det handlar om att göra dig själv, din dator och din mobil så osynliga som möjligt – både på nätet och ute i verkligheten – så att du blir ett så svårt offer som möjligt. I den här artikeln visar vi hur du kan göra hackerns jobb svårare i tolv steg.



Så döljer du dig effektivt på internet

Vill du undvika att bli ännu ett offer i statistiken över cyberbrott? Då gäller det att vara så svår att hitta som möjligt när hackare och andra brottslingar letar efter nya offer att lura.

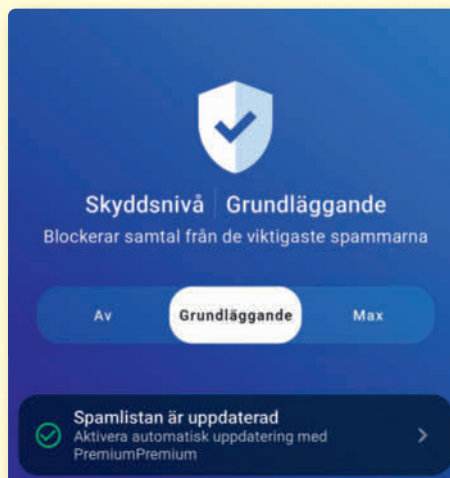
- ✓ Skydda dig mot bluffsamtal
- ✓ Testa om du kan spåras på nätet
- ✓ Använd aldrig gratis hotspots
- ✓ Dölj dig på främmande datorer
- ✓ Radera okända appar på mobilen
- ✓ Dölj din information på Facebook
- ✓ Bli helt osynlig med gratis VPN
- ✓ Använd alltid tvåstegsverifiering
- ✓ Skapa ett mejlkonto för det mindre viktiga
- ✓ Ta bort namnet på ditt trådlösa nätverk
- ✓ Stäng av Wi-Fi och Bluetooth
- ✓ Skydda dina filer med kryptering

Skydda dig mot bluffsamtal

Många blir uppringda av oseriösa elbolag, falska Microsoft-anställda, och försäljare av påhittade produkter. Det kan du skydda dig mot.

Spam-samtal är irriterande och kan i värsta fall vara farliga. Du kan känna igen dem på att personen ofta försöker få dig att gå med på att prenumerera på något på bruten engelska, eller att installera ett "verktyg" på din dator. De kan även presentera sig som medarbetare från din bank på perfekt svenska.

De flesta smarta mobiler har idag inbyggda funktioner som kan upptäcka och blockera misstänkta nummer. Du kan också hämta appen Truecaller till din Android-mobil eller iPhone för att skydda dig mot bluffsamtal.



Appen Truecaller, som finns för Android och iOS, kontrollerar inkommande samtal mot en lång lista med bluffnummer så att du blir varnad i tid om brottslingar ringer dig.



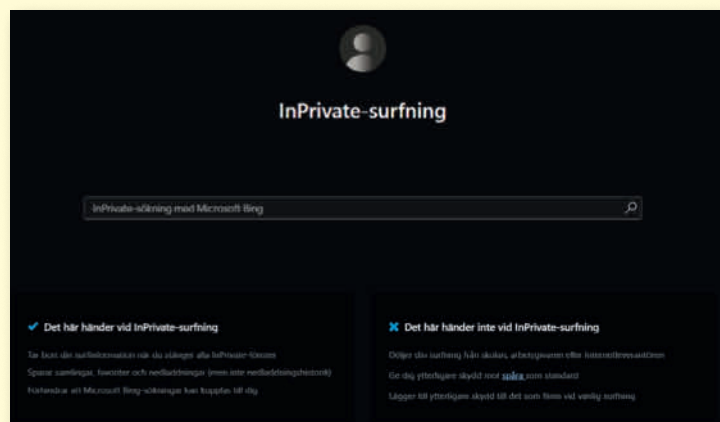
Därför är det viktigt

• Bluffsamtal

Någon ringer och utger sig för att till exempel vara från din bank och försöker få dig att föra över pengar eller lura av dig kontouppgifter.

• Dyra samtal

Du uppmanas att trycka på en knapp – och kopplas utan att veta om det till ett betalnummer som kostar mycket pengar per minut.



När du använder InPrivate-funktionen i Edge eller Inkognito i Chrome sparas inga data om dina internetbesök på datorn.



Därför är det viktigt

• Andra kan se historik

Delar du dator med andra kan de se vilka webbplatser du har besökt – till exempel nätbank, hälsoplattformar och gåvor du letat efter.

• Reklamen följer dig

Utan Inkognito eller liknande kan webbplatser lagra en massa information på datorn och visa annonser för det du har sökt efter.

Dölj dig på främmande datorer

Om du använder en offentlig dator i ett bibliotek eller på en annan allmän plats, se till att datorn inte lagrar information om vad du gör.

När du öppnar Chrome i inkognitoläge sparar webbläsaren *inte* din historik, sökningar eller en översikt över webbplatser du har besökt på datorn. Det är extra viktigt om andra använder samma dator och du vill hålla saker privata. I Chrome heter funktionen "Inkognito-läge", i Firefox heter den "Privat surfning" och i Edge heter den "InPrivate". Funktionen döljer dock bara dina spår på själva datorn. Din internetleverantör och de webbplatser du besöker kan fortfarande se vad du gör. Det är alltså inte ett fullständigt skydd.



Bli helt osynlig med gratis VPN

VPN står för Virtuellt Privat Nätverk och är ett verktyg som kan skydda dig när du använder internet från din dator eller mobil.

Enkelt uttryckt fungerar en VPN genom att du installerar ett program som är skapat av en VPN-leverantör. Leverantören har ett antal servrar installerade i olika länder, och när du använder programmet för att ansluta till en av dem skickas all din

data genom en slags säker tunnel. Det innebär att ingen kan se vilka webbplatser du besöker, vad du skriver eller var i världen du befinner dig, eftersom din IP-adress är dold. Det är användbart om du använder trådlöst internet på kaféer, hotell eller utomlands. En VPN-tjänst som den kostnadsfria Proton VPN, som finns på vår hemsida, kan också skydda dig mot hackare.



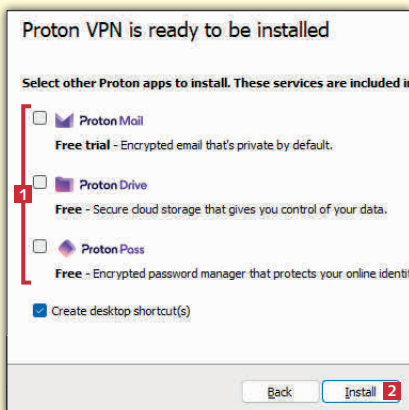
Därför är det viktigt

• Andra kan tjuvlyssna

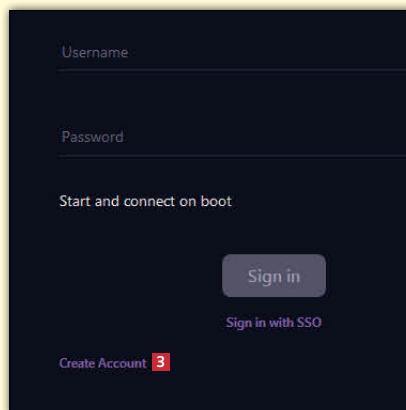
På offentliga nätverk kan andra spionera på vad du gör genom att trådlöst tjuvlyssna på din trafik över nätverket.

• Du blir spårad

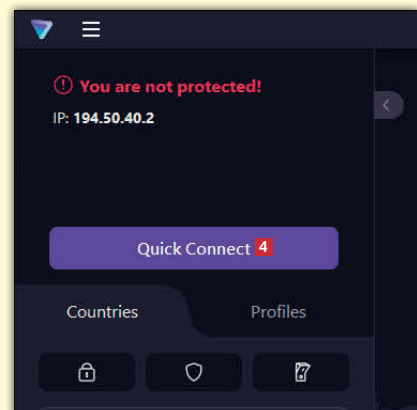
Webbplatser och företag kan spåra vad du tittar på online och spara information om dig.



1 Hämta Proton VPN från vår hemsida. Under installationen ska du avmarkera de föreslagna programmen **1** och sedan klicka på **Install 2**.



2 När programmet startar första gången måste du logga in med ett gratis konto. Det gör du genom att klicka på **Create Account 3**. Logga sedan in med ditt nya konto.



3 I programmet klickar du bara på **Quick Connect 4**. Då ansluter din dator till den första tillgängliga VPN-servern och din dator är skyddad mot hackare.



Därför är det viktigt

• Önskade gäster

Om trådlösa nätverket är synligt kan personer försöka gissa ditt lösenord för att sedan använda din internetuppkoppling.

• Enkelt tillgång för hackare

När nätverket är synligt blir det lätt för hackare att hitta det och försöka bryta sig. Om de lyckas kan de snoka i dina filer, stjäla lösenord och störa dina enheter.

Ta bort namnet på ditt trådlösa nätverk

Ditt trådlösa nätverk har ett namn som visas när du eller din granne söker efter tillgängliga Wi-Fi-nätverk i närheten. Namnet kallas SSID, och om du döljer det blir ditt nätverk osynligt för andra.

När nätverket är osynligt på detta sätt blir det svårare för främlingar att hitta och försöka bryta sig in. Du kan fortfarande använda det själv, men

du måste känna till både namnet och lösenordet i förväg och ange det manuellt första gången du vill ansluta någonting till nätverket. Du döljer SSID genom att logga in på din router från webbläsaren. Här hittar du inställningarna för trådlöst nätverk och markerar kryssrutan vid "Dölj nätverksnamn" eller liknande. Läs mer i routerns manual.

Testa om du kan spåras på nätet

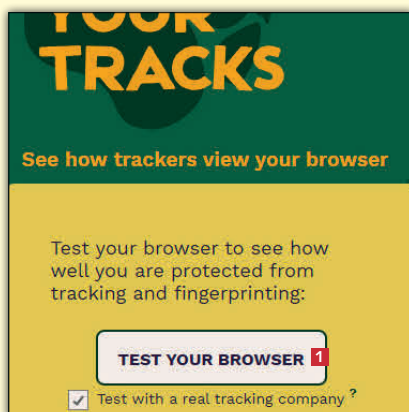
På webbplatsen Cover Your Tracks kan du testa hur mycket din dator avslöjar om dig när du är på nätet. Utan att du märker det kan webbplatser läsa information om datorns skärmstorlek, ditt operativsystem och vilka program du använder. Det här kallas "fingeravtryck" och kan användas för att följa dig på nätet, även om du inte direkt använder ditt namn på webbplatser. Cover Your

Tracks testar din webbläsare och berättar sedan hur lätt det är att känna igen dig, hur väl skyddad du är och hur du kan bli mer anonym på nätet. När testet är klart får du veta hur "unik" din webbläsare är. Ju mer unik, desto lättare är det för webbplatser att känna igen dig och följa dig på nätet. Om du är lätt att känna igen kan du ändra inställningarna för din webbläsare.

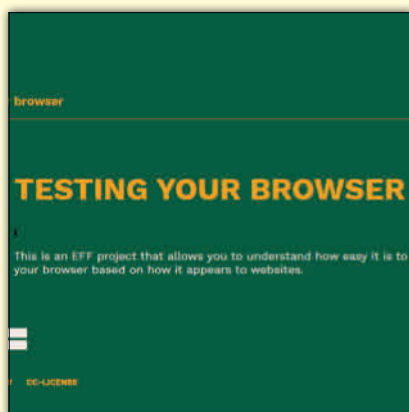


Därför är det viktigt

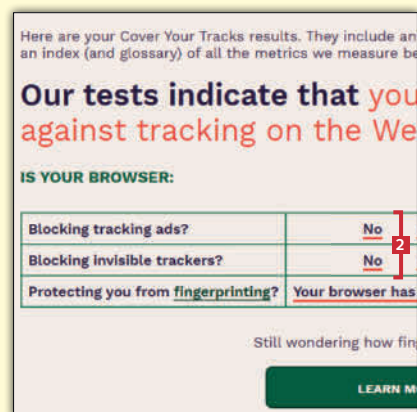
- **Sämlre personlig integritet**
Webbplatser kan följa det du ser, klickar på och bryr dig om – utan att du märker det.
- **Anpassad reklam**
Dina vanor används för att visa personligt anpassade annonser.
- **Data kan missbrukas**
Information om dig kan säljas eller läcka, och kan i värsta fall användas vid bedrägerier.



1 Öppna din webbläsare och surfa till hemsidan coveryourtracks.eff.org. Här klickar du på knappen **TEST YOUR BROWSER** **1**.



2 Webbplatsen börjar nu undersöka hur känslig din dator är för att spåras på nätet. Det brukar ta 10-20 sekunder.



3 Om det står **No** **2** i de två fälten är du INTE skyddad mot att spåras. På pctidningen.se/2516 hittar du en guide om hur du skyddar din webbläsare mot att spåras.



Därför är det viktigt

- **Stöld av din information**
Om du av misstag godkänner för många behörigheter kan okända appar snoka i dina kontakter, meddelanden och foton, och skicka dem vidare.
- **Dyr mobilräkning**
Dolda appar kan göra slut på din tillgängliga datamängd, sluka batteri och skicka dyra sms utan att du vet om det.

Radera okända appar på mobilen

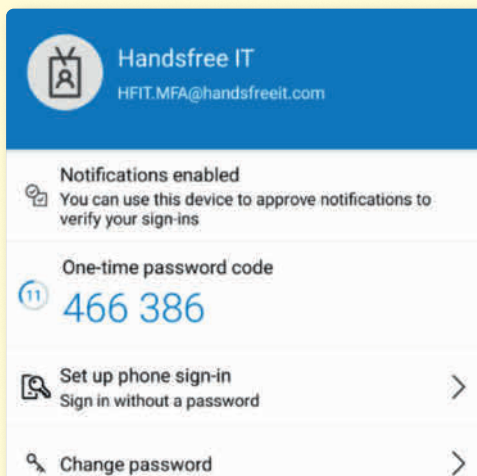
Det är en bra idé att regelbundet kontrollera vilka appar du har på din mobil. Du kanske tror att du känner till dina appar, men vissa appar kan ha installerats utan att du har märkt det, eller så kanske de följde med något annat som du har hämtat. Om du inte känner igen en viss app i listan över appar på din mobil bör du ta en kritisk titt på den eller helt

enkelt radera den. Vissa appar kan ha fått tillstånd att komma åt dina kontakter, din plats, kamera eller mikrofon utan att du nödvändigtvis har gett ditt samtycke till det. Det innebär att alla skumma appar kan veta mer om dig än du vill att de ska veta. Därför bör du ibland gå igenom din lista över appar och ta bort dem du inte använder.

Använd alltid tvåstegs-verifiering

Det har blivit alldeles för osäkert att skydda sig med enbart lösenord, så använd alltid tvåstegsverifikation där du har möjlighet att göra det.

Tvåstegsverifiering är en extra säkerhet som du kan aktivera för de flesta onlinetjänster. Förutom ditt eget valda lösenord behöver du en engångskod som antingen skickas till din mobil eller levereras via en autentiserings-app. Det innebär att även om någon gissar ditt lösenord kan de ändå inte logga in utan den extra engångskoden. Tvåstegsautentisering aktiveras i inställningarna för den tjänst du använder. Det tar ett par minuter att ställa in och gör det mycket, mycket svårare för brottslingar att komma åt dina saker online.



Med en app som Microsofts Authenticator kan du effektivt skydda dina konton.



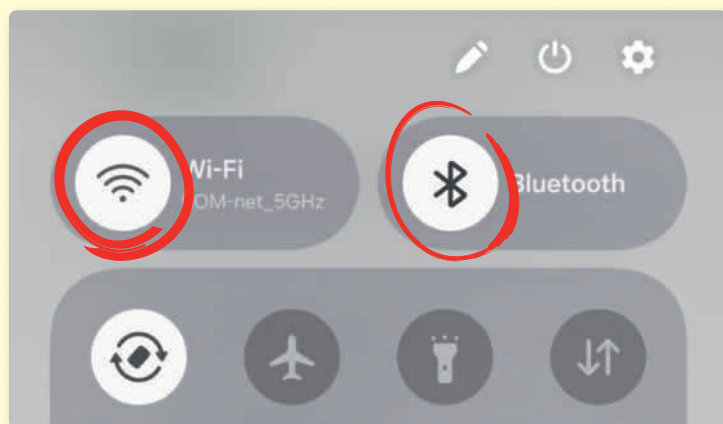
Därför är det viktigt

• Dina konton kan hackas

Om obehöriga personer gissar eller stjälar ditt lösenord till en onlinetjänst kan de få tillgång till din mejl, kalender och Facebook.

• Informationsmissbruk

Om en hackare får tillgång till dina konton kan de läsa dina meddelanden, skicka mejl i ditt namn och stjäla din personliga information.



På de flesta mobiler kan du stänga av Bluetooth och Wi-Fi genom att dra två fingrar nedåt från toppen av skärmen och trycka på dessa ikoner.

Stäng av Wi-Fi och Bluetooth

Trådlösa tekniker som Wi-Fi, NFC och Bluetooth är nästan oundgängliga, men de kan också göra dig sårbar för attacker när du är på resande fot.

När du inte använder Wi-Fi eller Bluetooth i mobilen är det en bra idé att stänga av dessa funktioner - särskilt när du är ute och reser. Om trådlös teknik är påslagen söker mobilen hela tiden efter trådlösa nätverk och andra enheter, vilket kan göra dig sårbar. Främlingar kan därmed hitta och försöka koppla upp sig mot din mobil, eller följa dina rörelser via dina trådlösa signaler utan att du märker det. Om du stänger av Wi-Fi och Bluetooth när du inte använder dem sparar du både batteri och gör det svårare för obehöriga att snoka.



Därför är det viktigt

• Du kan bli spårad

När Wi-Fi och Bluetooth är påslagna kan mobilen skicka signaler som gör det möjligt för obehöriga att följa hur du rör dig.

• Hackare kan ta sig in

Öppna signaler, likt de som skickas ut av Bluetooth och Wi-Fi, kan utnyttjas för att få tillgång till din mobil och informationen på den.

Använd aldrig gratis hotspots

Det kan kännas som en oas i en öken när du ser ett gratis trådlöst nätverk på kaféet eller flygplatsen, men det nätverket kan hota din säkerhet.

Gratis Wi-Fi på restauranger, hotell och flygplatser kan vara frestande när du vill komma ikapp med mejlen eller läsa nyheter, men det är inte alltid säkert. Om du ansluter till ett öppet nätverk kan andra personer på samma nätverk se vad du gör - som dina lösenord, mejl och annan privat information. Skickliga bedragare kan till och med falska hotspots som ser ut som det riktiga nätverket, så att du i själva verket kopplar upp dig direkt mot brottslingarnas egna nätverk. Därför bör du undvika öppna nätverk om det är möjligt.



Inget kan locka som ordet "gratis", men du kan riskera att du betalar med din privata information.



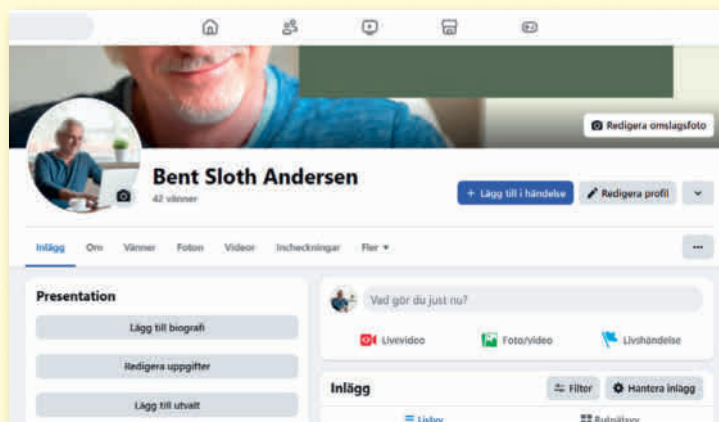
Därför är det viktigt

• Information på vift

Bedragare som är anslutna till samma nätverk som du kan snappa upp dina lösenord, mejl och annan privat information.

• Se upp gratis internet

En hackare kan skapa ett trådlöst nätverk som ser ut som ett publikt nätverk, och få tillgång till din mobil eller dator när du ansluter till det.



På det här Facebook-kontot är personlig information samt inlägg och foton dolda för icke-vänner så att ingen obehörig kan se dem.



Därför är det viktigt

• Identitetsstöld

Bedragare kan använda din personliga information, dina inlägg och dina foton för att skapa falska profiler eller lura andra i ditt namn.

• Inbrott

Om du till exempel delar ett inlägg på Facebook att du är på semester i ditt fritidshus kan det informera inbrottsjuvar att ditt hus står tomt.

Dölj din information på Facebook

Facebook att du kan hålla kontakten med släkt och vänner, men dela bara foton och information med personer du känner så det inte kan missbrukas.

Om du använder Facebook är det en god idé att dölja din personliga information och dina bilder för personer du inte känner. Även om det kan verka oskyldigt kan information om var du bor, din äkta hälft och din utlandssemester lätt missbrukas av brottslingar. I värsta fall kan informationen användas för bedrägerier eller identitetsstöld, och kan locka en inbrottsjuv att slå till om han vet att du inte är hemma. I Facebooks inställningar kan du välja att bara dina vänner får se vad du delar så att främlingar inte kan komma åt ditt privatliv.



Därför är det viktigt

• Du drunknar i skräppost

Om du bara har en mejladress för allting kommer din inkorg snabbt att fyllas med nyhetsbrev och skräppost, så att du råkar missa viktiga mejl.

• Större risk för bedrägerier

Om din mejladress sprids kan den hamna i orätta händer och missbrukas för bedrägerier eller försök till identitetsstöld.

Skapa ett mejlkonto för det mindre viktiga

Det är en bra idé att komplettera din privata mejladress med en som du har skapat för annat. Din privata adress kan du ha för saker som internetbank, läkare och kontakt med släkt och vänner. Den andra adressen, som du kan skapa på [gmail.com](https://www.gmail.com), kan du använda till nyhetsbrev, tävlingar, webbutiker och ställen där du bara behöver

ange en mejladress för att komma vidare. På så sätt skyddar du dig från en reklam och oönskade mejl som snabbt skulle kunna fylla upp din inkorg. Samtidigt minimerar du risken för bedrägerier eftersom du inte sprider din privata mejladress. Om din "offentliga" mejl skulle svämma över av skräppost kan du radera den och skapa en ny.

Hämta Guardian Of Data på pctidningen.se/2516



Skydda dina filer med kryptering

På datorns hårddisk är alla dina filer vanligtvis helt oskyddade, så en tjuv eller annan obehörig kan läsa dina dokument eller se dina foton. Om du krypterar dina filer blir de däremot låsta med en digital nyckel så att bara du kan öppna och ta del av innehållet. Det är extra viktigt för känslig information som brev, kontouppgifter eller dina privata foton, som krypteringen gör helt oläsliga

för alla personer som du inte har godkänt. Om din dator är utrustad med Windows 11 Pro har den redan ett krypteringsprogram i form av BitLocker-funktionen, men för oss andra som inte har den kan filerna skyddas med det kostnadsfria programmet Guardian Of Data, som du kan ladda ner från vår webbplats. Krypteringen ser till att skydda dina filer och personlig information.



Därför är det viktigt

• Du kan drabbas av läckor

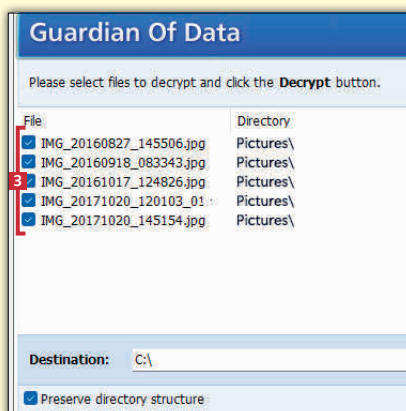
Om någon får tillgång till din dator kan de se dina dokument, foton och annan information.

• Identitetsstöld

Personliga uppgifter, som ditt personnummer, kan användas av bedragare för att utge sig för att vara du.



1 Ladda ner Guardian of Data från vår hemsida och installera det. När det klickar du på **Encrypt** **1** för att kryptera filer och **Decrypt** **2** för att låsa upp dem igen.



2 När du har valt **Decrypt** får du möjlighet att välja vilka filer **3** som ska låsas upp. Därmed behöver du inte dekryptera allt för att bara hämta en fil.



På vår webbplats kan du hämta en stor guide till programmet Guardian Of Data där du kan läsa om hur du använder programmet för att skydda dina filer.