Expert: AI-bedrägerier måste bekämpas med välvillig AI

David Jacoby, strategichef hos säkerhetsfirman Syndis, berättar i en intervju med för PC-tidningen att artificiell intelligens redan förändrar säkerheten online, både för angripare och försvarare. På den negativa sidan kan AI göra bedrägerier mycket mer övertygande. Jacoby säger dock även att AI kan användas för att förstärka skyddet. Artificiell intelligens används i allt högre grad för att upptäcka oegentligheter i nätverkstrafiken, avslöja bedrägliga transaktioner i realtid, upptäcka deepfake-innehåll och automatisera hanteringen av incidenter. Kapprustningen påskyndar kriminell innovation men även säkerhetssystemen anpassar sig, ofta med hjälp av samma underliggande teknik. Framtiden kommer att handla om hur snabbt defensiv AI kan ligga steget före offensiv AI. Kunskap, multifaktorautentisering och AI-driven hotdetektering i realtid kommer att spela en avgörande roll.

David Jacoby, strategichef, Syndis.

Foto: Skorzewiak/Shutterstock.com

DE STÖRSTA HOTEN MOT DIG OCH DIN DATOR

De stora hoten mot dig under 2026

Det nya året kommer att innebära flera utmaningar för din säkerhet. Nya hot växer sig allt starkare, och attackerna kommer att bli ännu svårare att upptäcka.

Journalist
Henning Rasmussen

Tidigt en söndagsmorgon ringer din mobil. Du känner genast igen rösten som ditt ena barnbarn, som förtvivlat berättar att han har varit med om en trafikolycka och fått näsan bruten och har fruktansvärt ont. I samband med olyckan har han gripits av polisen och att han behöver snabbt få några tusen kronor skickade till sig för att kunna köpa nödvändiga saker när han sitter i häktet.

Bluffar med AI på frammarsch

Det skulle kunna vara en mor- eller farföräldrars värsta mardröm, men i själva verket är det bara ett cyniskt bedrägeri. Barnbarnets röst skapas av artificiell intelligens, och i andra änden av samtalet sitter skickliga bedragare som bara är ute efter dina pengar. Exemplet med det fängslade barnbarnet kan låta som ren science fiction, men i själva verket är det precis vad som drabbade 73-åriga Ruth Card från Kanada.

Hennes historia publicerades i den välkända amerikanska tidningen The Washington Post, och Ruth Card hann ta ut motsvarande över 25 000 kronor åt bedragarna innan en bankanställd tog den äldre damen åt sidan och varnade henne för att en annan kund på banken nyligen hade blivit lurad av samma bedrägeri.

Artificiell intelligens har spridit sig till praktiskt taget alla tjänster och verktyg på rekordtid, och AI används nu i stor utsträckning av bedragare, som kan skapa större, billigare och mer övertygande bedrägerier. För att imitera röster från släktingar räcker det med röstprov på några meningar för att en artificiell intelligens ska kunna skapa en kopia. Röstprovet kan hämtas från en YouTube-video eller ett annat klipp från sociala medier som är fritt tillgängligt på internet. Det krävs inte heller någon speciell teknisk kunskap för att genomföra bedrägeriet, eftersom den artificiella intelligens som kan imitera röster är lätt tillgänglig online, tillsammans med en rad andra verktyg som kan missbrukas av brottslingar.

Tjänster som ElevenLabs används för dessa bedrägerier. ElevenLabs är en artificiell intelligens som kan generera falska röster och den har kritiserats för bland annat att ha fått Harry Potter-skådespelerskan Emma Watson att citera Adolf Hitlers bok ”Mein Kampf”.

Bedrägerierna blir allt bättre

Den stora utmaningen 2026 kommer att vara att det blir allt svårare att identifiera bedrägerier som begås med hjälp av artificiell intelligens, och att väldigt trovärdig kriminalitet kommer att sprida sig över alla plattformar. Du måste vara beredd på att bli lurad via telefonsamtal, sms och mejl, och du måste hela tiden vara kritisk när du använder elektroniska former av kommunikations eftersom bedrägerier kan dölja sig i appar, på webbplatser och i annonser på sociala medier. I den här artikeln kan du läsa om de största och farligaste hoten som väntar under 2026.

Bedragarna kan använda gratis onlineverktyg eller datorprogram som DeepFaceLab för att skapa falska videor som är så realistiska att de kan lura många offer att tro på vad personerna i videorna säger.

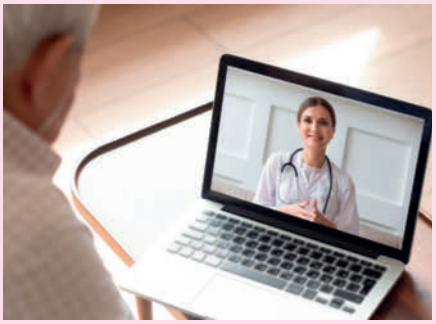
AI här ett hot mot dig och din dator

Hackare har sedan länge börjat använda artificiell intelligens för att skapa attacker som är mer trovärdiga. Det kräver nya vanor från din sida som potentiell offer.

Artificiell intelligens har verkligen hittat sin plats i hackarnas verktygslåda. Med hjälp av AI kan cyberbrottslingar skräddarsy bluffmejl som både är grammatiskt korrekta och anpassade till dig som mottagare. Enligt IBM:s X-Force-rapport från 2024 öppnas ända upp till 60 procent av dessa AI-genererade nätfiskemejl eftersom de är så svåra att skilja från äkta meddelanden. Ett annat växande hot är den utbredda användningen av så

SÅ SKYDDAR DU DIG

När du befinner dig i en situation där du får ett telefonsamtal eller ett meddelande från en familjemedlem i nöd kan det vara svårt att behålla lugnet – och givetvis ännu svårare att avslöja att det är ett bedrägeri. Därför rekommenderar de flesta experter att nära familjemedlemmar kommer överens om ett hemligt kodord eller en hemlig kodfras som ingen annan känner till. På så sätt kan du snabbt avgöra om personen som kontaktar dig är den riktiga familjemedlem eller en bedragare.



Tro inte på allt du ser eller läser på internet. De senaste åren har flera kända personer utnyttjats i bedrägerier som syftar till att övertyga offer att investera i till exempel falska kryptovalutor. Var försiktig om du blir kontaktad av din bank eller ditt sjukhus.

De flesta skulle bli oroliga och agera direkt om någon från deras bank eller en nära släkting ringde med dåliga nyheter. Men innan du agerar på samtalet måste du först försäkra dig om att personen i andra änden är den han eller hon utger sig för att vara.

Foto: fizkes, Prostock-studio, Tero Vesalainen, Tada Images, Arkhipenko Olga/Shutterstock.com

Falskt röst imiterade utrikesminister

Under sommarmånaderna 2025 skickade amerikanska utrikesdepartementet ut en varning till landets utländska diplomater. Bedragare hade använt sig av artificiell intelligens för att skapa falska röstmeddelanden av utrikesminister Marco Rubio. Dessa meddelanden använde man sedan för att kontakta tre utrikesministrar i andra länder, en amerikansk senator och en amerikansk guvernör.

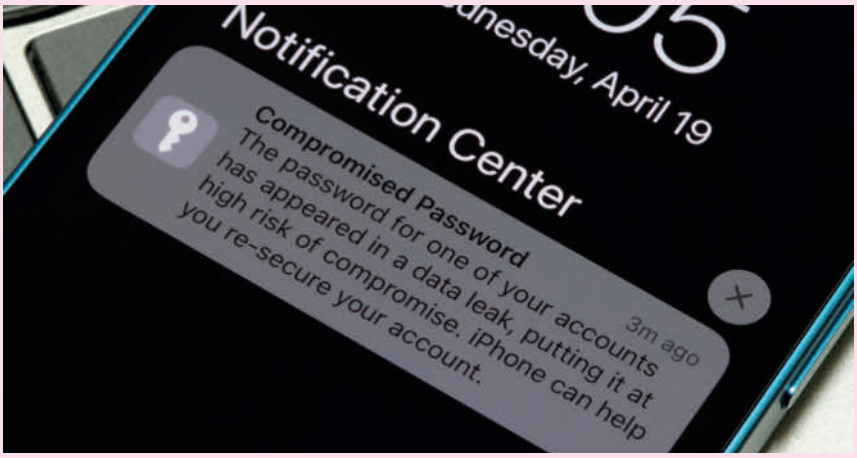
Med artificiell intelligens hade bedragarna lyckats kontakta de olika personerna via tjänsten Signal med textmeddelanden och röstmeddelanden med en röst som lät som Marco Rubios. Efter den händelsen har den amerikanska federala polisen (FBI) varnat för att den typen av AI-skapade bedrägerier bara ökar.

kallad deepfake-teknik, där både röster och videor kan imiteras in i minsta detalj.

I ett antal fall har bedragare med hjälp av klonade röster ringt företag och utgett sig för att vara chefen eller från ekonomiavdelningen. I ett exempel som publicerats av nyhetsbyrån AP News klonades rösten av en amerikansk politiker för att lura olika tjänstemän.

Samtidigt används AI för att hitta nya säkerhetshål i program och datorsystem – så kallade zero day-sårbarheter – mycket snabbare än tidigare. Enligt MIT:s laboratorium för datavetenskap och artificiell intelligens går det att automatisera hela attacken med språkmodeller, vilket gör att även oerfarna hackare kan orsaka betydande skador.

Därför måste dina säkerhetsvanor hålla jämna steg med utvecklingen.



På iPhone får du en varning om ett lösenord du använder har dykt upp i ett dataintrång. Du kan aktivera samma skydd på ditt Google-konto eller få det direkt på din dator med programmet HackCheck.

Dina tjänster blir hackade

Ett dataintrång innebär att dina lösenord, kortuppgifter och privata uppgifter kan hamna i händerna på brottslingar.

När en internettjänst där du har ett konto blir hackad kan din information hamna i en så kallad dataläcka. Det kan innebära att ditt användarnamn, lösenord och i värsta fall även dina betalningsuppgifter blir stulna och säljs vidare. Enligt analysföretaget Surfshark läckte över 300 miljoner konton ut bara under 2023.

Du kanske inte upptäcker något förrän pengar plötsligt dras från ditt konto eller någon plötsligt loggar in på ditt konto i ditt namn och börjar dela eller skicka saker där du står som avsändare. Enligt Stanford University sker de flesta identitetsstölder till följd av dataläckor, och du kan drabbas även om du inte har gjort något fel.

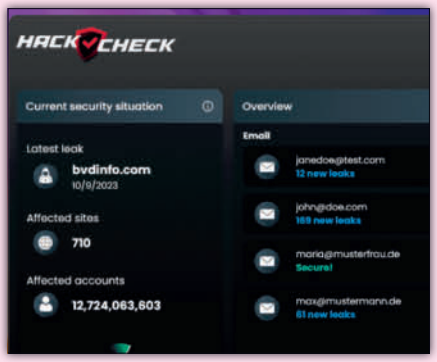
Din information kan stjälas via tjänster som du har använt i flera år, från onlinebutiker till mejlsystem, och den kan ofta missbrukas under lång tid innan det upptäcks.

Därför är det viktigt att använda unika lösenord för alla tjänster du använder och att aktivera tvåstegsverifiering där det går. Det gör det mycket svårare för en hackare att utnyttja informationen.

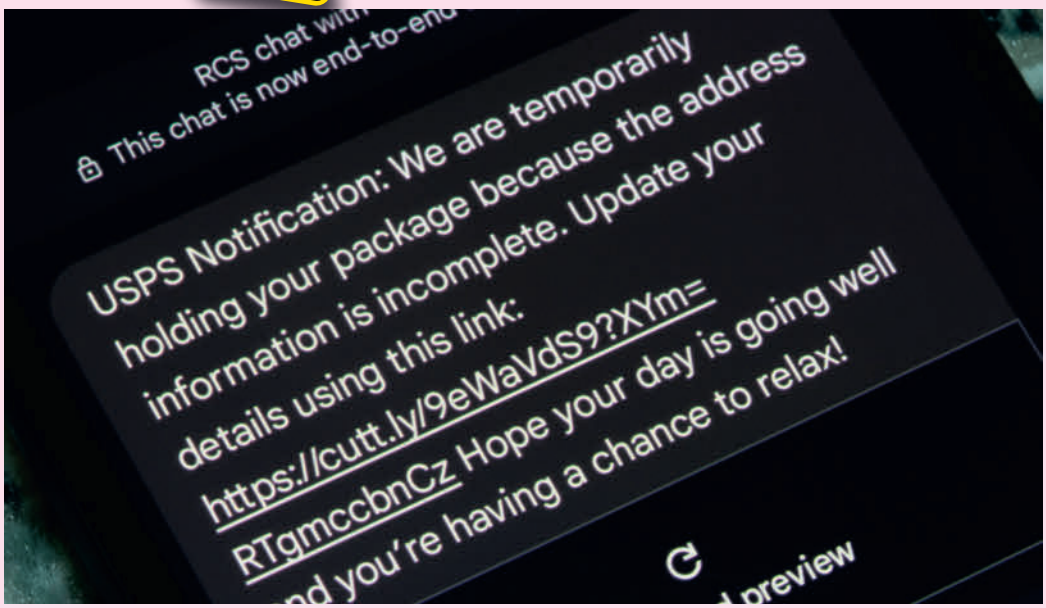
SÅ SKYDDAR DU DIG

Webbplatsen haveibeenpwned.com erbjuder möjligheten att du kan fylla i din mejladress och omedelbart få reda på om den har varit inblandad i ett dataintrång. Du kan också få automatiska aviseringar genom att installera programmet Abelssoft HackCheck på din dator. En varning visas på skrivbordet i Windows om ditt konto är i fara.

Hämta på **pctidningen.se/2520**



Abelssoft HackCheck, som du kan hämta på vår hemsida, ligger aktivt i bakgrunden på datorn och dyker upp med en varning om någon av dina mejladresser blivit inblandad i en dataläcka.



Du kan få ett falskt meddelande – på svenska eller engelska – om paket som inte kan levereras om du inte betalar en avgift.

Bedragare är extremt skickliga på att luras

Phishing och smishing är namn på moderna bedrägerier som försöker lura av dig information med trovärdiga meddelanden.

Brottslingar har blivit betydligt mer sofistikerade, och därför kan det vara svårt att skilja mellan äkta och falska meddelanden. Phishing, eller nätfiske, sker oftast via mejl, medan smishing, eller sms-fiske, sker via sms – båda med ett enda syfte: att få dig att klicka på en länk eller lämna ut dina personuppgifter. De farliga mejlen och meddelandena ser ut precis som ett meddelande från din bank, en budfirma eller en myndighet.

Om du klickar på länken kan du ge bedragarna tillgång till dina betalkort så att de kan ta ut pengar eller logga in på de tjänster du använder.

Enligt Europol blir den här typen av bedrägerier allt mer sofistikerade, och artificiell intelligens används nu rutinmässigt av brottslingar för att formulera perfekt svenska i sina bedrägerimeddelanden.

Det bästa försvaret är att alltid vara orubbligt kritisk. Klicka aldrig på länkar i oombedda mejl eller meddelanden – radera istället mejlet om du inte känner avsändaren.

SÅ SKYDDAR DU DIG

De falska meddelandena orsakar i sig ingen skada på din mobil eller dator. Skadan uppstår först när du följer de instruktionerna i meddelandena och till exempel följer en länk, eller anger dina uppgifter. Det bästa sättet att bekämpa bedrägerier är därför att helt enkelt radera de falska meddelandena och under inga omständigheter följa länkarna i dem.

När du får ett meddelande från en budfirma, din bank eller en myndighet och du är osäker på om det är falskt ska du aldrig svara på meddelandet. Ring istället det företag som påstås vara avsändaren.

Foto: Gorodenkoff, Tada Images, fizkes,/Shutterstock.com

Låt dig inte skrämmas av falska varningar

Popup-meddelanden och annonser får dig att agera i panik, men i många fall är dessa olycksbådande meddelanden bedrägerier.

Du kan stöta på falska varningar både på datorn och mobilen som påstår att enheten är infekterad med virus eller ransomware. Meddelandena ser äkta ut och använder ofta välkända logotyper för att öka sin trovärdighet, men syftet är förstås att få dig att klicka på en farlig länk eller betala för påstådd hjälp som du inte behöver.

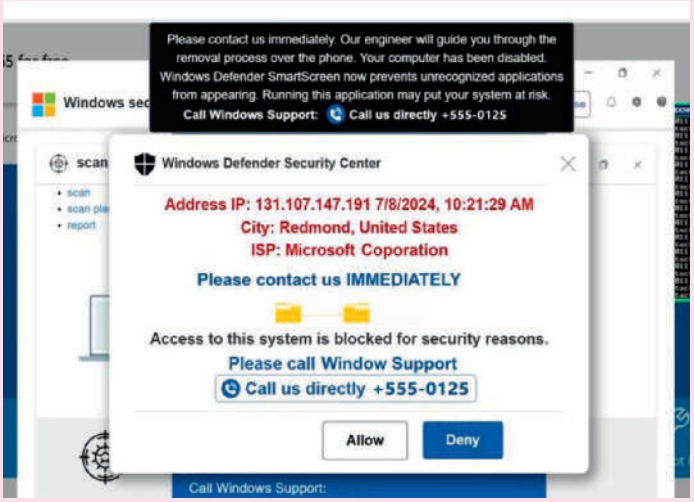
På datorn stöter du ofta på dessa falska meddelanden på specifika webbplatser eller från skadliga webbläsartillägg, men i vissa fall kan det också vara annonser utformade för att se ut som ett systemmeddelande från Windows eller från ett säkerhetsprogram. På mobilen kommer dessa varningar nästan uteslutande från tvivelaktiga appar som du själv har installerat eller webbläsarfönster som körs i bakgrunden.

Den europeiska polismyndigheten Europol varnar för att användningen av så kallad scareware har ökat. Scareware exploaterar människors rädsla för att förlora pengar och personlig data, och äldre människor drabbas särskilt hårt. När du stöter på ett varnande meddelande bör du omedelbart stänga fönstret utan att klicka på något. Se till att du har ett uppdaterat antivirusprogram på datorn och gärna också en effektiv säkerhetsapp på din mobil. Det hjälper dig att undvika att bli lurad.

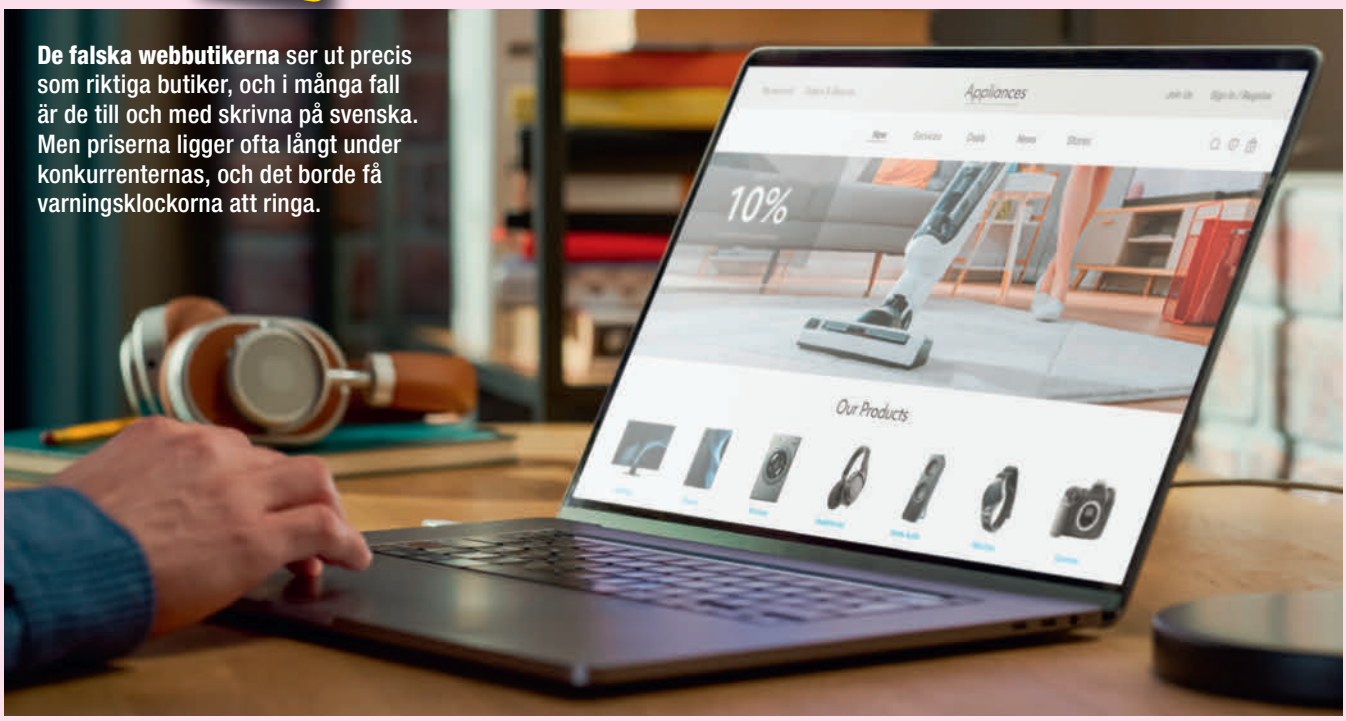
Du kan få oroväckande varningar om virus och andra hot på både din mobil och din dator. I många fall är dessa meddelanden falska, så det är viktigt att du inte klickar eller trycker på dem.

SÅ SKYDDAR DU DIG

Eftersom varningarna på skärmen är falska kan de inte skada din mobil eller dator. Skadan uppstår först om du följer instruktionerna i meddelandena och klickar eller trycker på länkar eller knappar. Dessa leder ofta till falska webbplatser som försöker stjäla din information eller dina pengar. Se därför till att stänga de irriterande fönstren så att du inte råkar klicka på dem.



Den falska varningen påstår sig komma från säkerhetsprogrammet Windows Defender, men är i själva verket bara ett öppet webbläsarfönster med en falsk varning. Du kan stänga varningen på ett säkert sätt genom att klicka på krysset i det övre högra hörnet eller trycka på Alt + F4 på tangentbordet.



De falska webbutikerna ser ut precis som riktiga butiker, och i många fall är de till och med skrivna på svenska. Men priserna ligger ofta långt under konkurrenternas, och det borde få varningsklockorna att ringa.

Falska butiker lurar dig i fällan

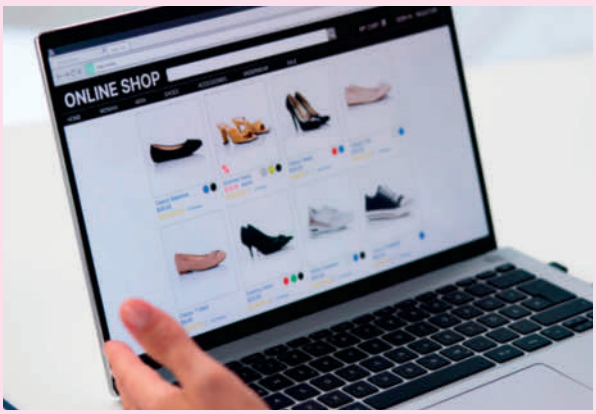
När du handlar på nätet bör du vara extra försiktig om du hamnar i en nätbutik där du inte har handlat tidigare – annars riskerar du att förlora både pengar och personuppgifter.

Antalet falska nätbutiker har ökat de senaste åren, och tyvärr är det inte osannolikt att du någon gång hamnar i klorna på kriminella säljare. Den här olyckliga trenden har underlättats av artificiell intelligens, som har gjort det enklare än någonsin för brottslingar att skapa realistiska och trovärdiga webbbutiker. De falska nätbutikerna ser helt äkta ut komplett med attraktiva bilder och detaljerade beskrivningar, ofta på engelska, och du kan till och med se dem bland de sponsrade butikerna i dina Google-sökresultat. Bakom den förtroendeingivande fasaden finns dock bara bedragare som är ute efter dina pengar – antingen utan att skicka några varor eller med varor av dålig kvalitet. Personerna bakom butikerna kan också stjäla dina betalningsuppgifter för att använda dem i bedrägerier.

Falska webbutiker brukar dyka upp med erbjudanden på populära varor eller märkesvaror till ovanligt låga priser. Om priset verkar vara för bra för att vara sant jämfört med vad du normalt skulle förvänta dig att varan kostar, då bör du vara extra försiktig och kontrollera webbutiken noggrant. Du kan bland annat titta närmare på webbplatsens

SÅ SKYDDAR DU DIG

Det bästa och mest effektiva skyddet mot falska webbutiker är att du är uppmärksam och tänker kritiskt. Brottslingar blir allt skickligare på att få butiker att se äkta ut, så du måste vara extra vaksam när du ser ett bra erbjudande eller erbjuds märkesvaror till priser som ligger långt under det normala. På **pctidningen.se/2520** kan du läsa om sju goda råd för att handla säkert på internet.



Om det dyker upp ett otroligt bra erbjudande i en webbshop är det klokt att vara extra kritisk. Det ska finnas ett organisationsnummer som du kan kolla upp i företagsregistret, och det är också en bra idé att kolla webbplatsen på trustpilot.com där du kan läsa recensioner av butiken.

Foto: aslysun, Gorodenkoff, Andrey_Popov, Maxim Elramsisy/Shutterstock.com

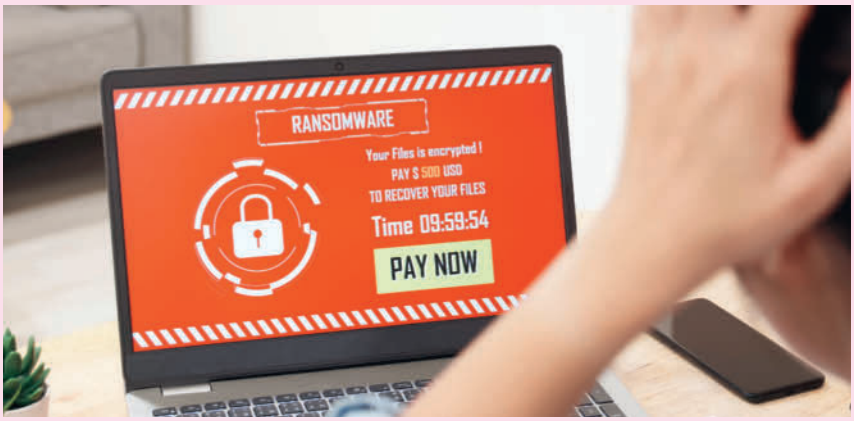
kontaktuppgifter, läsa recensioner på **trustpilot.com** och kontrollera att webbplatsen använder sig av en säker anslutning där adressen till hemsidan som börjar med https://.

Ett vanligtvis säkert tecken på en falsk butik är saknad eller ofullständig information om företaget bakom den. Om du inte hittar ett organisationsnummer, om hemsidan känns slarvigt eller dåligt utformad eller att villkoren är otydliga, då bör du stanna upp och begrunda situationen. Om du är osäker men ändå handlar i webbbutiken är det en bra idé att använda ett betalkort så att du kan bestrida köpet med din bank om det visar sig vara en bluff.

Designsandaler visade sig vara dåliga kopior

Om du trots allt skulle råka bli lurad av en falsk webbutik ska du snarast kontakta europeiska konsumentorganisationen Konsument Europa på adressen **konsumenteuropa.se**.

Det var precis vad Mathilde från Danmark gjorde, och du kan läsa hennes historia på organisationens webbplats. Hon berättar hur hon i en till synes dansk webbutik hittade ett par snygga Birkenstock-sandaler till halva priset, som hon beställde omedelbart. När hon senare fick ett bekräftelsemejl såg hon att sandalerna hade skickats från Kina och inte från Danmark. När sandalerna äntligen levererades till hennes adress i Danmark blev det snabbt klart att det handlade om förfalskade varor av dålig kvalitet. Mathilde lämnade in ett klagomål till sin bank och fick tillbaka sina pengar. Det är lätt att råka ut för den här typen av webbutiker med ett helt annat ursprung än vad de påstår, när man handlar från dem.



Ransomware, som krypterar dina filer och sedan kräver en lösensumma för att låsa upp dem, är bara en av många typer av skadlig programvara som kan infektera din dator och mobil om du inte är försiktig.

Datorn drabbas av malware

Om du har oturen att få skadlig programvara på din dator eller mobil riskerar du att den blir långsam och instabil, att du förlorar pengar, och att din personliga information blir stulen.

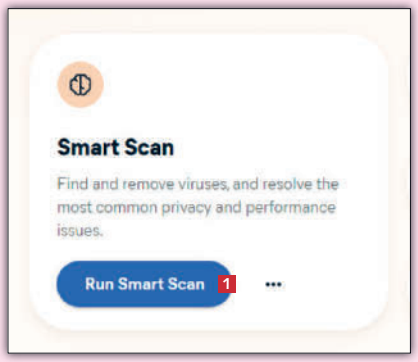
Malware är ett samlingsnamn på skadliga program som kan infektera datorer och mobiler. Dessa skadliga program kan ta sig in i din enhet på många olika sätt. De kan komma via farliga mejl, falska nedladdningar eller infekterade webbplatser.

När en enhet drabbas av malware kan programmen stjäla personlig information som användarnamn, lösenord och bankuppgifter, eller göra så att datorn eller mobilen blir långsammare och kan bli instabil med systemkrascher. Därför måste du vara försiktig vad du klickar på när du kollar din mejl eller besöker webbplatser, och bara ladda hem program från pålitliga källor som pctidningen.se. Se till att hålla både Windows och program uppdaterade så att utvecklarna kan täppa till kritiska säkerhetshål som kan göra din utrustning sårbar. Det är också viktigt att du har ett välfungerande och uppdaterat antivirusprogram installerat på datorn – till exempel Avast One Essential, som du kan hämta på **pctidningen.se/2520**.

SÅ SKYDDAR DU DIG

Det viktigaste skyddet mot skadlig programvara är att se till att din dator har ett grundläggande virusskydd, som Avast One Essential. Börja med att se till att ett antivirusprogram är installerat, uppdaterat och körs. Överväg att komplettera det med ytterligare program för att bekämpa skadlig programvara – till exempel Malwarebytes Antimalware, som du kan hämta från vår webbplats.

Hämta på **pctidningen.se/2520**



1 Hämta och installera Avast One Essential från vår webbplats. Starta programmet och klicka på **Run Smart Scan** 1 för att ge datorn en grundlig viruskoll.