Ekspert: AI-svindel skal bekæmpes med godsindet AI

David Jacoby, der er Chief Strategy Officer hos sikkerhedsfirmaet Syndis, fortæller til Komputer for alle, at kunstig intelligens allerede er ved at ændre sikkerheden på nettet, både for angribere og forsvarere. På den mørke side kan AI gøre svindelnumre langt mere overbevisende. David Jacoby fortæller dog også, at AI kan styrke forsvaret. Kunstig intelligens bruges i stigende grad til at opdage uregelmæssigheder i netværkstrafik, markere svigagtige transaktioner i realtid, spotte deepfake-indhold og automatisere håndtering af hændelser. Våbenkapløbet accelererer de kriminelles innovation, men sikkerhedssystemer tilpasser sig, ofte ved hjælp af den samme underliggende teknologi. Fremtiden vil afhænge af, hvor hurtigt defensiv AI kan holde sig foran offensiv AI. Uddannelse, multifaktorgodkendelse og AI-drevet trusselsdetektion i realtid vil være afgørende.

David Jacoby, Chief Strategy Officer, Syndis.

Foto: Skorzewiak/Shutterstock.com

DE STØRSTE TRUSLER MOD DIG OG DIN PC:

Sådan vil kriminelle ramme dig i 2026

Det kommende år byder på flere udfordringer af din sikkerhed. Nye trusler er på vej op i gear, og disse angreb bliver endnu sværere at afsløre.

Journalist
Henning Rasmussen

En tidlig søndag morgen ringer din telefon. Du genkender straks stemmen som dit barnebarn, der fortvivlet fortæller, at han har været involveret i en trafikulykke, der har resulteret i en brækket næse og ulidelige smerter. I forbindelsen med ulykken er dit barnebarn blevet arresteret af politiet, og har nu brug for en hurtig overførsel af nogle tusinde kroner til basale fornødenheder, mens han er i politiets varetægt.

Svindel med AI er i fremmarch

Det lyder nok som en bedsteforælders værste mareridt, men faktisk er det hele svindel. Barnebarnets stemme er genereret af kunstig intelligens, og i den anden ende af telefonforbindelsen sidder nogle dygtige svindlere, der kun er ude efter dine penge. Eksemplet med barnebarnet kunne måske lyde som fiktion, men faktisk var det præcis det, der skete for canadiske Ruth Card på 73 år.

Hendes historie er gengivet i den anerkendte amerikanske avis Washington Post, og Ruth Card nåede at hæve mere end 15.000 kroner til svindlerne, før en ansat i banken trak den ældre dame til side og advarede hende om, at en anden kunde i banken for kort tid siden var blevet narret af samme svindelnummer.

Kunstig intelligens har på rekordtid bredt sig til snart sagt alle tjenester og værktøjer, og AI bruges nu også i stor stil af svindlere, der kan lave større, billigere og mere overbevisende svindelkampagner. I tilfældet med at efterligne pårørendes stemmer, kræver det blot en stemmeprøve på nogle få sætninger for at den kunstige intelligens kan danne en kopi af en stemme. Stemmeprøven kan fx snuppes fra en YouTube-video eller et andet klip fra sociale medier, som ligger frit tilgængeligt på nettet. Det kræver heller ikke stor teknisk indsigt at lave svindlen, for den kunstige intelligens, der kan efterligne stemmer, er nemt tilgængelig på nettet sammen med en række andre værktøjer, der kan misbruges af kriminelle. Det er fx tjenester som ElevenLabs, der bruges til svindelnumrene. ElevenLabs er en kunstig intelligens, der kan generere falske stemmer, og den er tidligere blevet kritiseret for fx at få Harry Potter-skuespilleren Emma Watson til at citere fra Adolf Hitlers bog "Mein Kampf."

Svindlen bliver bedre og bedre

Den store udfordring i 2026 bliver, at det vil være sværere at identificere svindlen, som er lavet med den kunstige intelligens, og at den meget troværdige kriminalitet breder sig over alle platforme. Du skal således forberede dig på, at du kan blive narret både via telefonopkald, sms'er og e-mails, og at du altid skal være kritisk, når du bruger elektroniske kommunikationsformer, da der kan gemme sig svindel i både apps, på hjemmesider og i de reklamer, du ser på sociale medier. I denne artikel kan du læse meget mere om de største og mest faretruende trusler i 2026.

Svindlerne kan benytte sig af gratis værktøjer på nettet eller pc-programmer som DeepFaceLab til at lave falske videoer, der er så realistiske, at de kan narre mange ofre til at tro på det, personerne i videoerne fortæller dem.

Kunstig intelligens truer dig og din pc

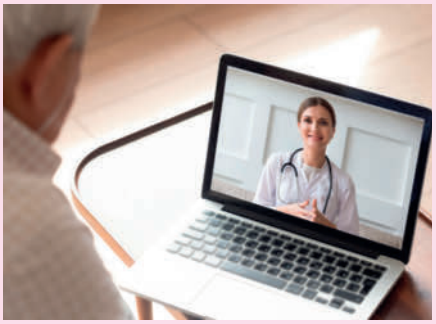
Hackere er for længst begyndt at bruge computerskabt intelligens til at lave mere troværdige angreb. Det kræver nye vaner fra dig som potentielt offer.

Kunstig intelligens har for alvor fundet vej ind i hackerens værktøjskasse. Med AI kan cyberkriminelle skræddersy svindelmails, der både er grammatisk korrekte og tilpasset dig som modtager.

Ifølge IBM's X-Force-rapport fra 2024 bliver op mod 60 procent af disse AI-genererede phishing-mails åbnet, fordi de er svære at skelne fra ægte henvendelser. En anden voksende trussel er den udbredte brug af så-

SÅDAN SIKRER DU DIG

Når man står i situationen og modtager et opkald eller en besked fra et nært familiemedlem i knibe, kan det være svært at holde hovedet koldt – og endnu sværere at afsløre det, hvis der er tale om svindel. Derfor anbefaler de fleste eksperter, at man internt i den tætte familie allerede nu bliver enige om et hemmeligt kodeord eller en hemmelig sætning, som ingen andre kender til. Dermed kan du hurtigt finde ud af, om de, der kontakter dig, er en del af familien eller nogle svindlere.



Du skal ikke tro på alt, hvad du ser eller læser på nettet. I de senere år er kendte personer blevet misbrugt i svindel, der fx skal overbevise dig om at investere i falsk kryptovaluta. Vær også på vagt, hvis du bliver kontaktet af banken eller sygehuset.

De fleste vil blive bekymrede og skride til handling, hvis en person fra banken eller en nær slægtning ringer med foruroligende nyt. Men før du agerer på opkaldet, skal du først sikre dig, at personen i den anden ende er den, han giver sig ud for at være.

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

Falsk stemme imiterede udenrigsminister

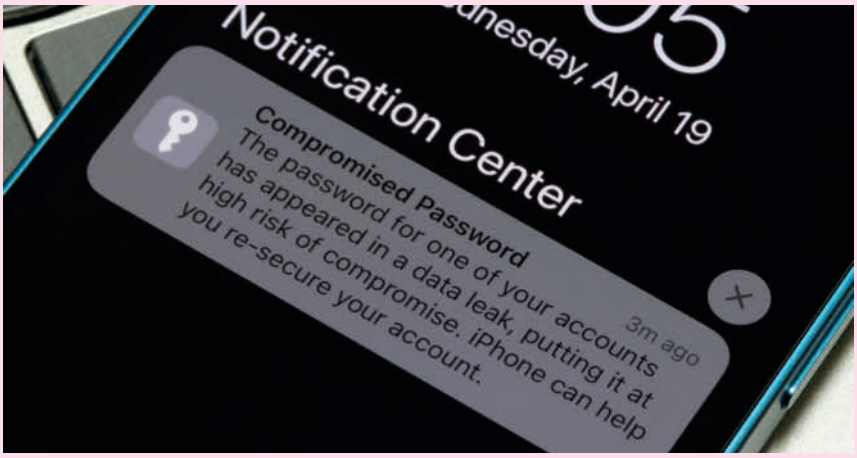
I sommermånederne i 2025 sendte det amerikanske udenrigsministerium, US Department of State, en advarsel til landets udenlandske diplomater. Svindlere havde brugt kunstig intelligens til at skabe falske stemmeoptagelser af udenrigsminister Marco Rubio, og disse optagelser havde de så brugt til at kontakte tre udenrigsministre i andre lande, en amerikansk senator og en amerikansk guvernør. Med kunstig intelligens havde svindlerne formået at kontakte de forskellige personer via tjenesten Signal med tekstbeskeder og talebeskeder med en stemme, der lød som Marco Rubios. Efterfølgende har det amerikanske forbundspoliti FBI advaret om, at denne type AI-genereret svindel er i kraftig stigning.

kaldt deepfake-teknologi, hvor stemmer og videoer kan efterlignes ned til mindste detalje.

En række tilfælde har vist, hvordan svindlere med klonede stemmer har ringet til virksomheder og udgivet sig for at være chefen eller lederen af regnskabsafdelingen. I et eksempel udgivet af nyhedsbureauet AP News blev en amerikansk politiker klonet for at narre embedsfolk.

Samtidig bruges AI til at finde nye sikkerhedshuller i programmer og systemer – såkaldte zero-day sårbarheder – langt hurtigere end før. Ifølge universitetet MIT's Computer Science and Artificial Intelligence Laboratory er det muligt at automatisere hele angrebsplanen med sprogmodeller, så selv uerfarne hackere kan gøre stor skade.

Derfor må dine sikkerhedsvaner følge med udviklingen.



På en iPhone bliver du advaret, hvis en kode, du anvender, er dukket op i et datalæk. Samme beskyttelse kan du aktivere på din Google-konto, eller få direkte på din pc med programmet HackCheck.

Dine tjenester bliver hacket

Et datalæk betyder, at dine kodeord, kortoplysninger og private data kan ende i hænderne på kriminelle.

Når en onlinetjeneste, som du er registreret hos, bliver hacket, kan dine oplysninger ende i et såkaldt datalæk. Det kan betyde, at brugernavn, adgangskode og nogle gange også dine betalingsoplysninger bliver lækket og solgt videre. Ifølge analysefirmaet Surfshark blev over 300 millioner konti lækket i 2023 alene.

Du opdager det måske først, når der pludselig trækkes penge på din konto, eller nogen logger ind på din konto i dit navn, og begynder at dele eller sende ting med dig som afsender. Ifølge Stanford University sker de fleste identitetstyverier som følge af netop datalæk, og det kan ramme dig, selv om du ikke umiddelbart har gjort noget forkert.

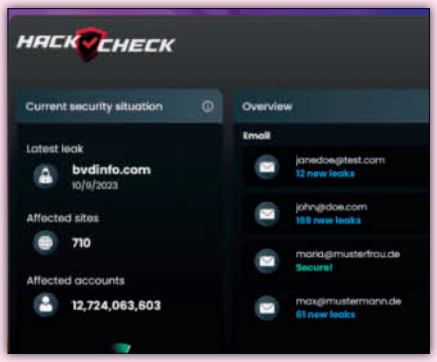
Dine oplysninger kan nemlig blive stjålet via tjenester, du har brugt i årevis fra netbutikker til mailsystemer, og de bliver ofte misbrugt længe, før det bliver opdaget.

Derfor er det vigtigt, at du bruger forskellige adgangskoder til alle de tjenester, du bruger, og slår totrinsbekræftelse til. Det gør det langt sværere for en hacker at udnytte dine data, hvis uheldet er ude.

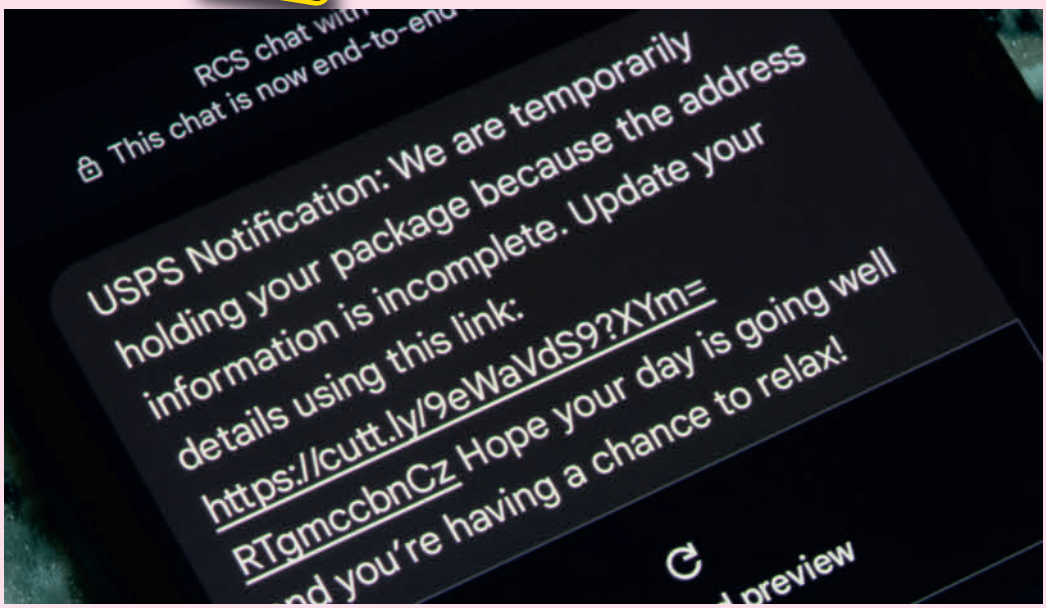
SÅDAN SIKRER DU DIG

På siden haveibeenpwned.com kan du indtaste din e-mailadresse og med det samme få svar på, om adressen er blevet misbrugt i et datalæk. Du kan også få besked automatisk, hvis du installerer programmet Abelssoft HackCheck på din pc. Så dukker der en advarsel op på Skrivebordet i Windows, hvis din konto er i fare.

Hent programmet på **komputer.dk/2520**



Abelssoft HackCheck, som du kan hente på vores hjemmeside, ligger i baggrunden på din pc, og dukker op med en advarsel, hvis en af dine mailadresser er blevet misbrugt i et datalæk.



Du kan risikere at modtage en falsk besked om en pakke, der først kan leveres efter betalingen af et lille gebyr – enten på dansk eller engelsk.

Svindlere er helt sublime til at snyde og narre dig

Phishing og smishing er navne på moderne fupnumre, der forsøger at lokke dine oplysninger ud af dig med troværdige beskeder.

De kriminelle er blevet langt mere snu, og det kan derfor være svært at skelne mellem ægte og falske beskeder. Phishing foregår typisk via e-mail, mens smishing lander på din telefon som sms'er – begge dele med ét eneste formål; at få dig til at klikke på et link eller afgive dine personlige oplysninger. De ondsindede mails og beskeder ligner til forveksling en besked fra din bank, en pakketjeneste eller en offentlig myndighed.

Klikker du på det indsatte link, kan du ende med at give svindlerne adgang til at hæve penge på dine betalingskort eller logge ind på de tjenester, du bruger.

Ifølge Europol bliver denne type svindel meget mere avanceret for hvert år, og kunstig intelligens bruges nu rutinemæssigt af de kriminelle til at formulere perfekt dansk i svindelbeskederne.

Dit bedste forsvar er sund skepsis. Klik aldrig på links i uopfordrede e-mails eller beskeder – slet i stedet mailen, hvis du ikke kender afsender.

SÅDAN SIKRER DU DIG

De falske beskeder gør ikke af sig selv nogen skade på hverken din telefon eller pc. Skaden sker først, hvis du følger de falske anvisninger i beskederne og fx klikker på et link eller indtaster dine oplysninger. Derfor er den bedste kur mod svindlen, at du blot sletter de falske beskeder, og under alle omstændigheder lader være med at følge de indsatte links.

Når du modtager en besked fra en pakketjeneste, din bank eller en myndighed, og du er i tvivl om den er falsk, skal du ikke reagere på beskeden. Ring i stedet for til det velkendte firma, der påstås at være afsender.

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

Lad dig ikke skræmme af de falske advarsler

Pop op-beskeder og reklamer lokker dig til at handle i panik, men i mange tilfælde er de ildevarslende beskeder ren svindel.

Både på din computer og mobiltelefon kan du møde falske advarsler, der påstår, at din pc eller telefon er inficeret med virus eller ransomware. Beskederne ser ægte ud, og de anvender ofte velkendte logoer, som øger troværdigheden, men formålet er naturligvis at få dig til at klikke på et farligt link eller betale for påstået hjælp, som du ikke har brug for.

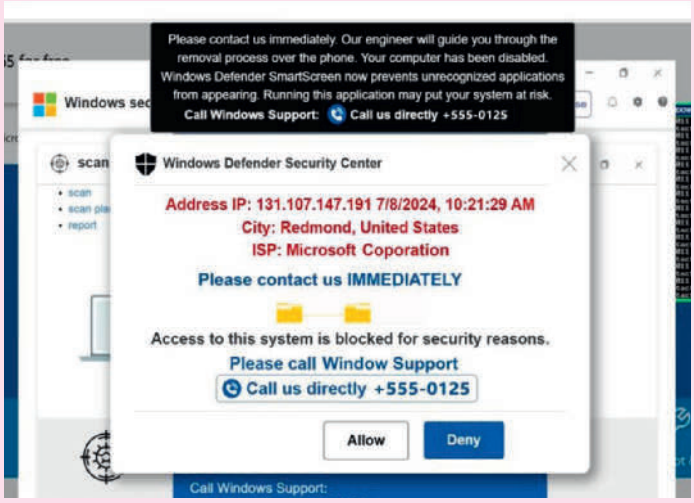
På pc'en vil du ofte møde disse falske beskeder på bestemte hjemmesider eller som skadelige browserudvidelser, men der kan også i nogle tilfælde være tale om bannerreklamer, som er designet til at ligne en systembesked fra Windows eller et sikkerhedsprogram. På telefonen er der næsten altid tale om beskeder fra tvivlsomme apps, du selv har installeret, eller browservinduer, der kører i baggrunden på telefonen.

Ifølge det europæiske politisamarbejde Europol er der sket en stigning i brugen af scareware (skræmme-software), som udnytter folks frygt for at miste data eller penge, og især ældre mennesker rammes hyppigt. Når du møder en alarmerende besked, bør du straks lukke vinduet uden at klikke på noget, og sørge for at have et opdateret antivirusprogram installeret på din pc og eventuelt også en effektiv sikkerhedsapp på telefonen. Så undgår du at blive snydt.

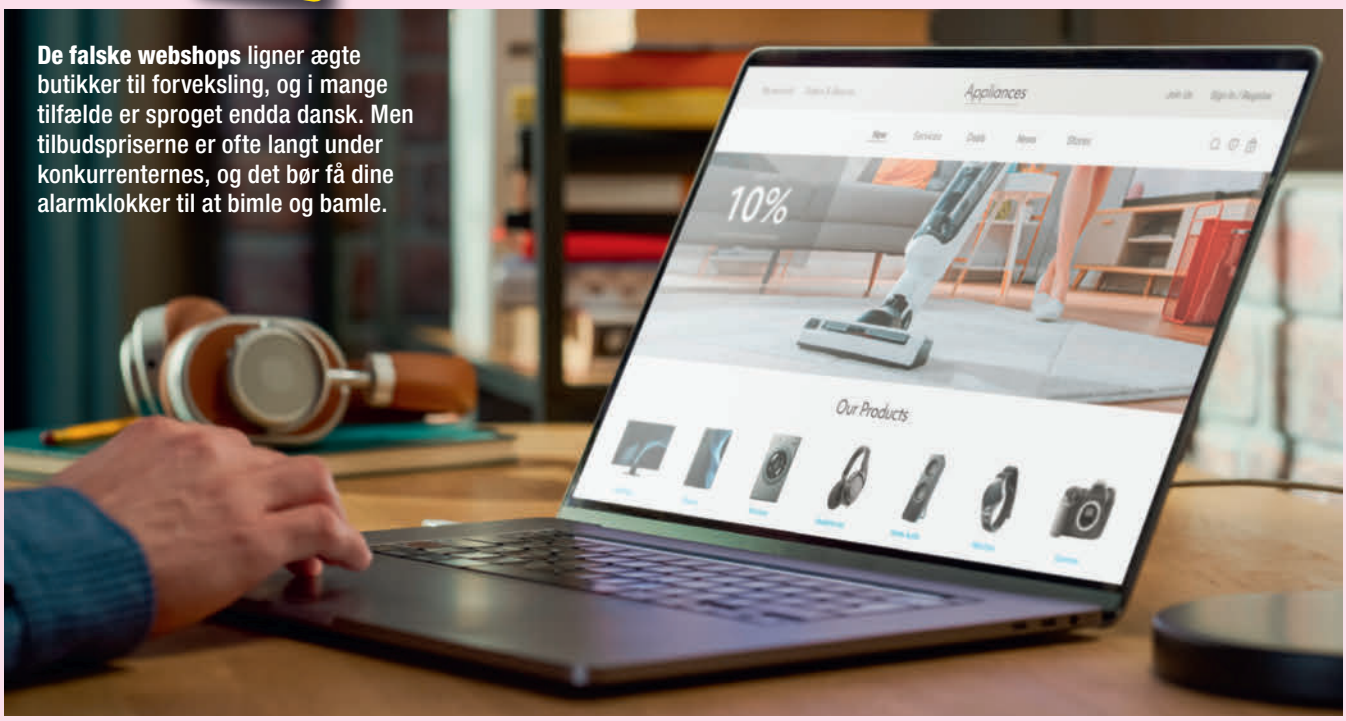
Du kan opleve at få bekymrende advarsler om virus og andre trusler på såvel din telefon som din computer. I mange tilfælde er beskederne falske, så det er vigtigt, at du ikke klikker eller trykker på dem.

SÅDAN SIKRER DU DIG

Fordi advarslerne på din skærm er falske, kan de heller ikke gøre skade på din telefon eller pc. Skaden sker først, hvis du følger beskedernes instruktioner og klikker på links eller knapper. Det vil nemlig ofte føre til falske sider, der forsøger at høste dine informationer eller penge. Derfor skal du blot sørge for at lukke for de irriterende vinduer, så du ikke ved et uheld kommer til at klikke på dem.



Den falske advarsel her påstår at komme fra Windows' sikkerhedsprogram Defender, men er i virkeligheden blot et åbnet browservindue med en falsk advarsel. Du kan i ro og mag lukke advarslen ved at klikke på krydset i toppen til højre eller trykke på Alt + F4 på dit tastatur.



De falske webshops ligner ægte butikker til forveksling, og i mange tilfælde er sproget endda dansk. Men tilbudspriserne er ofte langt under konkurrenternes, og det bør få dine alarmklokker til at bimle og bamle.

Falske sælgere narrer dig i fælden

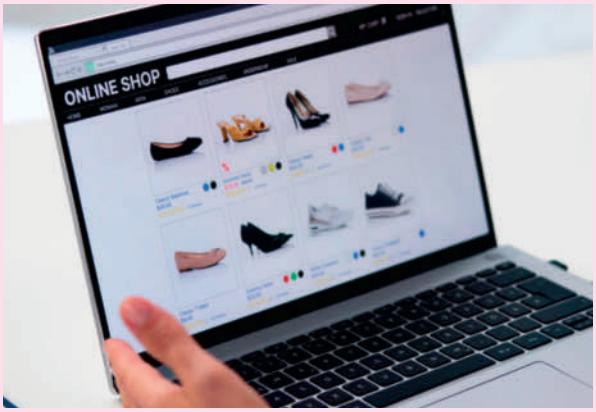
Når du køber ind på nettet, skal du være ekstra forsigtig, hvis du er endt på en webbutik, du ikke tidligere har handlet hos – ellers risikerer du at miste både penge og data.

Der er sket en stigning i antallet af falske webbutikker over den seneste årrække, og derfor er det desværre ikke usandsynligt, at du selv på et tidspunkt vil ende i kløerne på de kriminelle sælgere. Den kedelige tendens er hjulpet godt på vej af kunstig intelligens, som gør det nemmere end nogensinde for de kriminelle at skabe vellignende og troværdige butiksfacader på nettet. De falske webshops ser helt ægte ud med flotte billeder og fine beskrivelser, der ofte også er på dansk, og du kan også være uheldig at se dem blandt de sponsorerede butikker i din Google-søgning. Bag facaden gemmer sig svindlere, der vil have dine penge – enten uden at sende varer til dig eller med varer af dårlig kvalitet. Butikkernes bagmænd kan også stjæle dine betalingsoplysninger og bruge dem til svindel.

Ofte dukker de falske webshops op med populære tilbud eller mærkevarer til usædvanligt lave priser. Hvis prisen virker for god til at være sand i forhold til, hvad du normalt forventer, at varen skal koste, skal du være ekstra forsigtig og tjekke webshoppen grundigt efter i sømmene. Du kan blandt andet

SÅDAN SIKRER DU DIG

Den bedste og mest effektive beskyttelse mod de falske webshops er din opmærksomhed og kritiske sans. De kriminelle bliver hele tiden dygtigere og dygtigere til at få butikkerne til at se ægte ud, så du er også nødt til at være endnu mere på vagt, når du ser et godt tilbud eller får tilbudt mærkevarer til langt under normalprisen. På komputer.dk/2520 kan du læse syv gode råd til sikker onlineshopping.



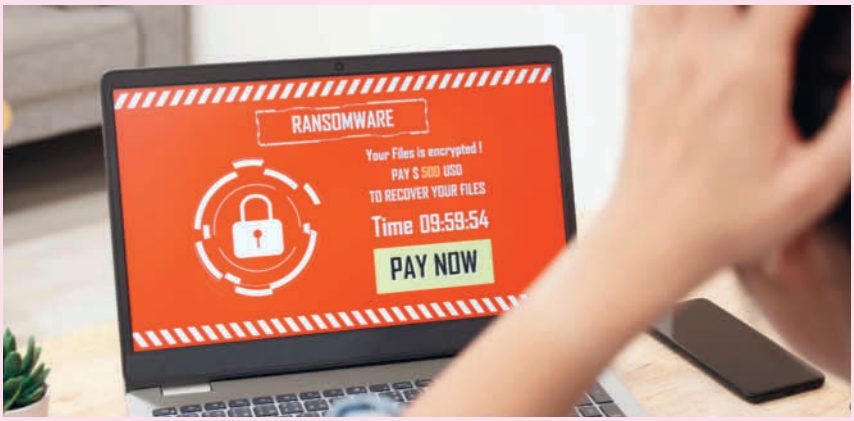
Hvis du finder et usandsynligt godt tilbud på en webshop, er det fornuftigt at være ekstra kritisk. Der bør fx være angivet et CVR-nummer, som du kan slå op i virksomhedsregistret, ligesom det er en god idé at tjekke hjemmesiden på trustpilot.com, hvor du kan læse andre anmeldelser af butikken.

kigge nærmere på hjemmesidens kontaktinformation, læse anmeldelser på **trustpilot.com**, og tjekke, om siden bruger en sikker forbindelse, hvor starter med https://.

Et sikkert tegn på en falsk butik er manglende eller ufuldstændige oplysninger om firmaet bag. Hvis du ikke kan finde butikkens CVR-nummer, du oplever at hjemmesiden er dårligt opbygget, eller der er utydelige handelsbetingelser, bør du stoppe op og overveje situationen. Er du i tvivl, men ender med at handle på webshoppen, er det en god idé at bruge et betalingskort, så du kan gøre indsigelse mod købet hos din bank, hvis det viser sig at være svindel.

Vellignende sandaler var dårlige kopier

Hvis du bliver snydt af en falsk webshop, kan du kontakte den europæiske forbrugerorganisation Forbruger Europa på siden **forbrugereuropa.dk**. Det har danske Mathilde gjort, og hendes beretning kan du læse på organisationens hjemmeside. Her fortæller hun, hvordan hun på en tilsyneladende dansk webshop fandt et par attraktive Birkenstock-sandaler til halv pris, som hun straks bestilte. Da hun senere modtog en bekræftelsesmail, kunne hun dog se, at sandalerne var afsendt fra Kina og ikke Danmark. Da sandalerne efter længere tid dukkede op på hendes adresse i Danmark, stod det desværre også hurtigt klart, at der var tale om kopivarer i dårlig kvalitet. Mathilde endte med at gøre indsigelse til sin bank og fik derved sine penge tilbage. Den type webshops, som har en anden oprindelse, end den giver sig ud for, kan du nemt støde på, når du shopper på nettet.



Ransomware, der krypterer dine filer og afkræver dig en løsesum, er blot én blandt mange typer af malware, der kan ramme din pc og telefon, hvis du ikke er forsigtig.

Pc'en inficeres med malware

Hvis du er uheldig at få malware på din pc eller telefon, risikerer du både langsomt og ustabilt udstyr, at miste penge og at få stjålet dine personlige oplysninger.

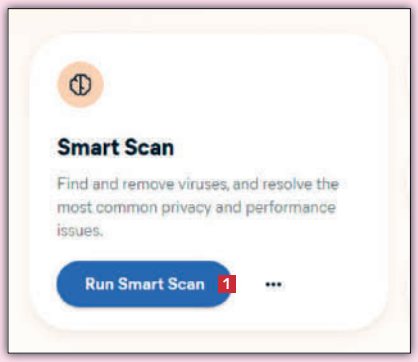
Malware er skadelige programmer, der kan inficere din computer og mobiltelefon. De ondsindede programmer har mange indgange til dit udstyr. De kan komme ind via farlige mails, falske downloads eller inficerede hjemmesider.

Når malware rammer din enhed, kan virussen blandt andet stjæle dine personlige oplysninger som brugernavne, koder og bankoplysninger, eller gøre din computer eller telefon langsommere og mindre stabil. Derfor skal du være opmærksom på, hvad du klikker på, når du tjekker dine mails eller besøger hjemmesider, og kun hente programmer fra troværdige kilder som komputer.dk. Sørg også for at holde både Windows og dine programmer opdaterede, så producenterne har mulighed for at få lukket kritiske sikkerhedshuller, som kan gøre dig og dit udstyr sårbare. Det er også vigtigt, at du har et velfungerende antivirusprogram installeret på pc'en – fx Avast One Essential, som du kan hente på **komputer.dk/2520**.

SÅDAN SIKRER DU DIG

Det vigtigste værn mod malware er, at du sikrer, at din pc's grundlæggende beskyttelse mod virus er på plads. Derfor bør du starte med at tjekke, at dit antivirusprogram er installeret og kører, og først derefter kan du overveje at supplere med yderligere programmer til bekæmpelse af malware – fx Malwarebytes Antimalware, som du kan hente på vores hjemmeside.

Hent programmerne på **komputer.dk/2520**



1 Hent Avast One Essential fra vores hjemmeside, og installér programmet. Start programmet, og klik på **Run Smart Scan** 1 for at give pc'en et grundigt virustjek.